kaspersky

Kaspersky Endpoint Security для Windows 14.3

© 2026 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Endpoint Security для Windows

- Что нового
- Исправленные ошибки
- Часто задаваемые вопросы

Kaspersky Endpoint Security для Windows

- Режимы работы приложения: Стандартный, EDR-агент, Легкий агент
- Комплект поставки
- Аппаратные и программные требования
- Сравнение функций приложения в зависимости от типа операционной системы
- Сравнение функций приложения в зависимости от инструментов управления
- Совместимость с другими приложениями

Установка и удаление приложения

- Развертывание через Kaspersky Security Center
  - Стандартная установка приложения
  - Создание инсталляционного пакета
  - Обновление баз в инсталляционном пакете
  - Создание задачи удаленной установки
- Локальная установка приложения с помощью мастера
- Удаленная установка приложения с помощью System Center Configuration Manager
- Описание параметров установки в файле setup.ini
- Процессы Kaspersky Endpoint Security для Windows
- Изменение состава компонентов приложения
- Обновление предыдущей версии приложения
  - Обновление приложения без перезагрузки
  - SMU-обновление приложения
- Удаление приложения

Лицензирование приложения

- О Лицензионном соглашении
- О лицензии
- О Лицензионном сертификате
- О подписке
- О лицензионном ключе
- О коде активации
- О файле ключа
- Сравнение функций приложения в зависимости от типа лицензии для рабочих станций
- Сравнение функций приложения в зависимости от типа лицензии для серверов
- Активация приложения
- Удаление лицензионного ключа
- Просмотр информации о лицензии
- Приобретение лицензии
- Продление подписки

Начало работы
- О плагине управления Kaspersky Endpoint Security для Windows
- Особенности работы с плагинами управления разных версий
- Особенности использования защищенных протоколов для взаимодействия с внешними службами
- Интерфейс приложения
  - Значок приложения в области уведомлений
  - Упрощенный интерфейс приложения
  - Настройка отображения интерфейса приложения
- Подготовка приложения к работе
- Управление политиками
  - Создание политики
  - Экспорт и импорт политики
  - Индикатор уровня защиты
- Управление задачами
- Настройка локальных параметров приложения
- Разделение доступа к функциям программы по пользовательским ролям
- Запуск и остановка Kaspersky Endpoint Security
- Приостановка и возобновление защиты и контроля компьютера
- Создание и использование конфигурационного файла
- Восстановление параметров приложения по умолчанию
- Производительность Kaspersky Endpoint Security и совместимость с другими приложениями
  - Включение и выключение режима энергосбережения
  - Включение и выключение режима передачи ресурсов другим приложениям
  - Лучшие практики по оптимизации производительности Kaspersky Endpoint Security

Поиск вредоносного ПО
- Проверка компьютера
- Проверка съемных дисков при подключении к компьютеру
- Фоновая проверка
- Проверка из контекстного меню
- Проверка целостности приложения
- Формирование области проверки
- Запуск проверки по расписанию
- Запуск проверки с правами другого пользователя
- Оптимизация проверки

Обновление баз и модулей приложения
- Схемы обновления баз и модулей приложения
  - Обновление с серверного хранилища
  - Обновление из папки общего доступа
  - Обновление с помощью Kaspersky Update Utility
  - Обновление в мобильном режиме
- Запуск и остановка задачи обновления
- Запуск задачи обновления с правами другого пользователя
- Выбор режима запуска для задачи обновления
- Добавление источника обновлений
- Обновление модулей приложения
- Использование прокси-сервера при обновлении
- Откат последнего обновления

Технология лечения активного заражения
Лечение активных угроз на рабочих станциях
Лечение активных угроз на серверах
Устранение необработанных угроз
Защита компьютера
Статус постоянной защиты
Защита от файловых угроз
Включение и выключение Защиты от файловых угроз
Автоматическая приостановка Защиты от файловых угроз
Изменение действия компонента Защита от файловых угроз над зараженными файлами
Формирование области защиты компонента Защита от файловых угроз
Использование методов проверки
Использование технологий проверки в работе компонента Защита от файловых угроз
Оптимизация проверки файлов
Проверка составных файлов
Изменение режима проверки файлов
Проверка контейнеров
Предотвращение вторжений
Включение и выключение Предотвращения вторжений
Работа с группами доверия приложений
Изменение группы доверия для приложения
Настройка прав группы доверия
Выбор группы доверия для приложений, запускаемых до Kaspersky Endpoint Security
Выбор группы доверия для неизвестных приложений
Выбор группы доверия для приложений с цифровой подписью
Работа с правами приложений
Защита ресурсов ОС и персональных данных
Удаление информации о неиспользуемых приложениях
Мониторинг работы Предотвращения вторжений
Защита доступа к аудио и видео
Защита от атак BadUSB
Включение и выключение Защиты от атак BadUSB
Использование экранной клавиатуры при авторизации USB-устройств
Авторизация сканеров штрихкода
AMSI-защита
Включение и выключение AMSI-защиты
Оптимизация проверки файлов AMSI-защитой
Защита от веб-угроз
Включение и выключение Защиты от веб-угроз
Настройка методов обнаружения вредоносных веб-адресов
Анти-Фишинг
Формирование списка доверенных веб-адресов
Экспорт и импорт списка доверенных веб-адресов
Защита от почтовых угроз
Включение и выключение Защиты от почтовых угроз
Изменение действия над зараженными сообщениями электронной почты
Формирование области защиты компонента Защита от почтовых угроз

- Проверка составных файлов, вложенных в сообщения электронной почты
- Фильтрация вложений в сообщениях электронной почты
- Экспорт и импорт списка расширений для фильтра вложений
- Проверка почты в Microsoft Office Outlook
- Проверка почты в Thunderbird, МойОфис, Р7-Офис

Защита от сетевых угроз
- Включение и выключение Защиты от сетевых угроз
- Блокирование атакующего компьютера
- Настройка адресов исключений из блокирования
- Экспорт и импорт списка исключений из блокирования
- Настройка Защиты от сетевых угроз по типам

Сетевой экран
- Включение и выключение Сетевого экрана
- Изменение типа сетевого соединения
- Работа с сетевыми пакетными правилами
  - Создание сетевого пакетного правила
  - Включение и выключение сетевого пакетного правила
  - Изменение действия Сетевого экрана для сетевого пакетного правила
  - Изменение приоритета сетевого пакетного правила
  - Экспорт и импорт сетевых пакетных правил
  - Описание сетевых пакетных правил в XML
- Работа с сетевыми правилами приложений
  - Создание сетевого правила приложения
  - Включение и выключение сетевого правила приложений
  - Изменение действия Сетевого экрана для сетевого правила приложений
  - Изменение приоритета сетевого правила приложений
- Мониторинг сети

Защита от эксплойтов
- Включение и выключение Защиты от эксплойтов
- Защита памяти системных процессов

Анализ поведения

Защита от шифрования
- Включение и выключение защиты папок общего доступа от внешнего шифрования
- Настройка периода блокировки недоверенного компьютера
- Формирование области защиты
- Добавление доверенных компьютеров для внешнего шифрования данных
- Экспорт и импорт списка исключений из защиты папок общего доступа от внешнего шифрования

Откат вредоносных действий

Kaspersky Security Network
- Включение и выключение использования Kaspersky Security Network
- Ограничения работы с Kaspersky Private Security Network
- Включение и выключение облачного режима для компонентов защиты
- Настройка KSN Proxy
- Проверка репутации файла в Kaspersky Security Network

Проверка защищенных соединений
- Включение проверки защищенных соединений
- Установка доверенных корневых сертификатов

- Проверка защищенных соединений с недоверенным сертификатом
- Исключение защищенных соединений из проверки
- Блокировка доступа к доменам с недоверенными сертификатами
- Удаление данных

Контроль компьютера

- Веб-Контроль
  - Добавление правила доступа к веб-ресурсам
  - Фильтр по адресам веб-ресурсов
  - Фильтр по содержанию веб-ресурсов
  - Проверка работы правил доступа к веб-ресурсам
  - Экспорт и импорт правил Веб-Контроля
  - Экспорт и импорт адресов веб-ресурсов правила Веб-Контроля
  - Мониторинг активности пользователей в интернете
  - Изменение шаблонов сообщений Веб-Контроля
  - Правила формирования масок адресов веб-ресурсов
  - Веб-Контроль для виртуальных машин
  - Переменные в шаблонах сообщений Веб-Контроля
- Контроль устройств
  - О правилах доступа
  - Получение данных об установленных устройствах
  - Контроль доступа к устройствам по типу
  - Контроль доступа к устройствам по шине подключения
  - Разграничение прав доступа пользователей к устройствам
  - Контроль доступа к мобильным устройствам
  - Контроль доступа к Bluetooth-устройствам
  - Контроль печати
  - Контроль подключения к Wi-Fi
  - Мониторинг использования съемных дисков
  - Изменение периода кеширования
  - Действия с доверенными устройствами
    - Добавление устройства в список доверенных
    - Экспорт и импорт списка доверенных устройств
  - Получение доступа к заблокированному устройству
    - Онлайн-режим предоставления доступа
    - Офлайн-режим предоставления доступа
  - Изменение шаблонов сообщений Контроля устройств
  - Анти-Бриджинг
    - Включение Анти-Бриджинга
    - Изменение статуса правила установки соединений
    - Изменение приоритета правила установки соединений
- Адаптивный контроль аномалий
  - Обучение Адаптивного контроля аномалий
  - Включение и выключение правила Адаптивного контроля аномалий
  - Изменение действия при срабатывании правила Адаптивного контроля аномалий
  - Создание исключения для правила Адаптивного контроля аномалий
  - Экспорт и импорт исключений для правил Адаптивного контроля аномалий
  - Применение обновлений для правил Адаптивного контроля аномалий

Изменение шаблонов сообщений Адаптивного контроля аномалий
Мониторинг работы Адаптивного контроля аномалий
Контроль приложений
Ограничения функциональности Контроля приложений
Получение данных об установленных приложениях
Включение режима блокирования только запрещенных приложений
Контроль приложений на основе эталонного компьютера
Управление правилами Контроля приложений
Добавление условия срабатывания правила Контроля приложений
Добавление в категорию приложений исполняемых файлов из папки Исполняемые файлы
Добавление в категорию приложений исполняемых файлов, связанных с событиями
Добавление правила Контроля приложений
Изменение статуса правила Контроля приложений с помощью Kaspersky Security Center
Экспорт и импорт правил Контроля приложений
Просмотр событий по результатам работы компонента Контроль приложений
Просмотр отчета о запрещенных приложениях
Тестирование правил Контроля приложений
Включение и выключение тестирования правил Контроля приложений
Просмотр отчета о запрещенных приложениях в тестовом режиме
Просмотр событий по результатам тестовой работы компонента Контроля приложений
Мониторинг активности приложений
Правила формирования масок имен файлов или папок
Изменение шаблонов сообщений Контроля приложений
Переменные в шаблонах сообщений Контроля приложений
Лучшие практики инвентаризации исполняемых файлов
Лучшие практики по внедрению режима списка разрешенных приложений
Настройка режима списка разрешенных приложений
Тестирование режима списка разрешенных приложений
Поддержка режима списка разрешенных приложений
Контроль сетевых портов
Включение контроля всех сетевых портов
Формирование списка контролируемых сетевых портов
Формирование списка приложений, для которых контролируются все сетевые порты
Экспорт и импорт списков контролируемых портов
Анализ журналов
Настройка предустановленных правил
Добавление пользовательских правил
Контроль целостности системы
О правилах Контроля целостности системы
Контроль целостности системы в режиме реального времени
Проверка целостности системы по запросу
Экспорт и импорт правил Контроля целостности системы
Просмотр отчетов о работе Контроля целостности системы
Сброс статуса целостности системы
Cloud Discovery

Доверенная зона
- Создание исключения из проверки
- Создание исключения по типу обнаруживаемых объектов
- Формирование списка доверенных приложений
- Создание локальной доверенной зоны
- Экспорт и импорт доверенной зоны
- Работа с приложениями, подписанными доверенной цифровой подписью
- Приложение. Предустановленные исключения из проверки и доверенные приложения
  - Microsoft SQL Server
  - Microsoft Exchange Server
  - Microsoft System Center Configuration Manager
  - Citrix
  - VMware
  - Дедупликация данных в Microsoft Windows Server

Работа с резервным хранилищем
- Настройка максимального срока хранения файлов в резервном хранилище
- Настройка максимального размера резервного хранилища
- Восстановление файлов из резервного хранилища
- Удаление резервных копий файлов из резервного хранилища

Служба уведомлений
- Настройка параметров журналов событий
- Настройка отображения и доставки уведомлений
- Настройка отображения предупреждений о состоянии приложения в области уведомлений
- Обмен сообщениями между пользователем и администратором

Работа с отчетами
- Просмотр отчетов
- Настройка максимального срока хранения отчетов
- Настройка максимального размера файла отчета
- Сохранение отчета в файл
- Удаление информации из отчетов

Самозащита Kaspersky Endpoint Security
- Включение и выключение механизма самозащиты
- Включение и выключение поддержки AM-PPL
- Защита служб приложения от внешнего управления
- Обеспечение работы приложений удаленного администрирования
- Защита паролем
  - Включение Защиты паролем
  - Предоставление разрешений для отдельных пользователей или групп
  - Использование временного пароля для предоставления разрешений
  - Отзыв временного пароля
  - Особенности разрешений Защиты паролем
  - Сброс пароля KLAdmin
- Защита подключения к Серверу администрирования

Шифрование данных
- Ограничения функциональности шифрования
- Смена длины ключа шифрования (AES56 / AES256)

Шифрование диска Kaspersky
- Особенности шифрования SSD-дисков
- Запуск шифрования диска Kaspersky
- Формирование списка жестких дисков для исключения из шифрования
- Экспорт и импорт списка жестких дисков для исключения из шифрования
- Включение использования технологии единого входа (SSO)
- Управление учетными записями Агента аутентификации
- Использование токена и смарт-карты при работе с Агентом аутентификации
- Расшифровка жестких дисков
- Восстановление доступа к диску, защищенному технологией Шифрование диска Kaspersky
- Вход под служебной учетной записью Агента аутентификации
- Обновление операционной системы
- Устранение ошибок при обновлении функциональности шифрования
- Трассировка работы Агента аутентификации
- Изменение справочных текстов Агента аутентификации
- Удаление объектов и данных, оставшихся после тестовой работы Агента аутентификации

Управление BitLocker
- Запуск шифрования диска BitLocker
- Расшифровка жесткого диска, защищенного BitLocker
- Восстановление доступа к диску, защищенному BitLocker
- Приостановка защиты BitLocker для обновления программного обеспечения

Шифрование файлов на локальных дисках компьютера
- Запуск шифрования файлов на локальных дисках компьютера
- Формирование правил доступа приложений к зашифрованным файлам
- Шифрование файлов, создаваемых и изменяемых отдельными приложениями
- Формирование правила расшифровки
- Расшифровка файлов на локальных дисках компьютера
- Создание зашифрованных архивов
- Восстановление доступа к зашифрованным файлам
- Восстановление доступа к зашифрованным данным в случае выхода из строя операционной системы
- Изменение шаблонов сообщений для получения доступа к зашифрованным файлам

Шифрование съемных дисков
- Запуск шифрования съемных дисков
- Добавление правила шифрования для съемных дисков
- Экспорт и импорт списка правил шифрования для съемных дисков
- Портативный режим для работы с зашифрованными файлами на съемных дисках
- Расшифровка съемных дисков

Просмотр информации о шифровании данных
- Просмотр статусов шифрования
- Просмотр статистики шифрования на информационных панелях Kaspersky Security Center
- Просмотр ошибок шифрования файлов на локальных дисках компьютера
- Просмотр отчета о шифровании данных

Работа с зашифрованными устройствами при отсутствии доступа к ним
- Восстановление данных с помощью утилиты восстановления FDERT
- Создание диска аварийного восстановления операционной системы

Защита от сложных и целевых атак (встроенные агенты)
- Лицензирование MDR и EDR Optimum
- Совместимость со сторонними EDR-решениями
- Kaspersky Endpoint Agent
  - Миграция конфигурации [KES+KEA] на [KES+встроенный агент]
  - Миграция политик и задач Kaspersky Endpoint Agent
- Endpoint Detection and Response агент (EDR-агент)
  - Установка EDR-агента
  - Интеграция EDR-агента с MDR
  - Интеграция EDR-агента с EDR (KATA)
  - Интеграция EDR-агента с NDR (KATA)
  - Интеграция EDR-агента с EDR Expert (on-premises)
  - Совместимость со сторонними EPP-приложениями
- Managed Detection and Response
  - Интеграция встроенного агента с MDR
  - Руководство по миграции с KEA на KES для MDR
- Endpoint Detection and Response Expert (on-premises)
  - Интеграция встроенного агента с EDR Expert (on-premises)
  - Настройка отправки телеметрии EDR Expert (on-premises)
  - Фильтрация событий телеметрии EDR Expert (on-premises)
  - Экспорт и импорт фильтров событий EDR Expert (on-premises)
  - Особенности использования профилей политик для настройки интеграции с EDR Expert (on-premises) и EDR (KATA)
- Endpoint Detection and Response Expert (cloud)
  - Интеграция встроенного агента с EDR Expert (cloud)
  - Настройка отправки телеметрии EDR Expert (cloud)
  - Исключения из телеметрии EDR Expert (cloud)
  - Как экспортировать / импортировать фильтры событий EDR Expert (cloud)
- Endpoint Detection and Response Optimum / Expert
  - Интеграция встроенного агента с EDR Optimum / EDR Expert
  - Поиск индикаторов компрометации (стандартная задача)
  - Расширенный сбор телеметрии для поиска IOC
  - Помещение файла на карантин
  - Получение файла
  - Удаление файла
  - Запуск процесса
  - Завершение процесса
  - Запрет запуска объектов
    - Управление Запретом запуска объектов
    - Создание CSV-файла с правилами запрета
  - Сетевая изоляция компьютера
  - Cloud Sandbox
  - Руководство по миграции с KEA на KES для EDR Optimum
- Kaspersky Anti Targeted Attack Platform
  - Интеграция встроенного агента с EDR (KATA)
  - Интеграция встроенного агента с NDR (KATA)
  - Настройка отправки телеметрии EDR (KATA)

Исключения из телеметрии EDR (KATA)
Пример 1. Исключенные процессы
Пример 2. Исключенные сетевые коммуникации
Пример 3. Исключенные операции с файлами
Пример 4. Исключенные изменения реестра
KATA Sandbox
Интеграция встроенного агента с KATA Sandbox
Настройка действий по реагированию на угрозы
Руководство по миграции с KEA на KES для EDR (KATA)
Kaspersky Sandbox
Интеграция встроенного агента с Kaspersky Sandbox
Поиск индикаторов компрометации (автономная задача)
Руководство по миграции с KEA на KES для Kaspersky Sandbox
Работа с карантином
Настройка максимального размера карантина
Передача данных о файлах на карантине в Kaspersky Security Center
Восстановление файлов из карантина
Реагирование на IOA
Мониторинг EDR-действий
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Интеграция Kaspersky Endpoint Security с KUMA
Подготовка к интеграции KES с KUMA
Подключение KES к KUMA
Добавление коннектора агентов KUMA
Коннектор, тип file
Коннектор, тип tcp
Коннектор, тип udp
Коннектор, тип http
Коннектор, тип wec
Коннектор, тип etw
Добавление точки назначения
Настройка прокси для агентов KUMA
Фильтрация событий для отправки в KUMA
Экспорт и импорт фильтров событий KUMA
Руководство по миграции с KSWS на KES
Соответствие компонентов KSWS и KES
Соответствие параметров KSWS и KES
Миграция компонентов KSWS
Миграция политик и задач KSWS
Миграция доверенной зоны KSWS
Миграция правил Контроля запуска программ KSWS
Установка KES вместо KSWS
Миграция конфигурации [KSWS+KEA] на [KES+встроенный агент]
Проверка удаления приложения Kaspersky Security для Windows Server
Активация KES ключом KSWS
Особенности миграции на высоконагруженных серверах

- Управление приложением на сервере в режиме Server Core
- Пример миграции с [KSWS+KEA] на [KES+встроенный агент]

Режим Легкого агента для защиты виртуальных машин

- Особенности работы приложения в режиме Легкого агента
- Предварительная настройка виртуальной машины
  - Совместимость с технологией Citrix App Layering
  - Совместимость с технологией Citrix Provisioning (Citrix Provisioning Services)
  - Совместимость с технологией Omnissa App Volumes
- Установка Легкого агента
- Подключение Легкого агента к SVM
  - Обнаружение SVM
  - Настройка алгоритма выбора SVM для Легкого агента
  - Распределение подключений Легких агентов к SVM (теги)
  - Защита соединения между Легким агентом и SVM
- Активация Легкого агента
- Руководство по миграции с Легкого агента KSVLA на Легкий агент KES
  - Установка Легкого агента KES вместо Легкого агента KSVLA
  - Соответствие компонентов Легкого агента KSVLA и Легкого агента KES
  - Миграция политик и задач Легкий агент KSVLA
  - Миграция конфигурации [Легкий агент KSVLA+KEA] на [Легкий агент KES+встроенный агент]

Управление приложением из командной строки

- Setup. Установка приложения
- Setup /x. Удаление приложения
- msiexec /i. Восстановление приложения
- Команды AVP
  - SCAN. Поиск вредоносного ПО
  - UPDATE. Обновление баз и модулей приложения
  - ROLLBACK. Откат последнего обновления
  - TRACES. Трассировка
  - START. Запуск профиля
  - STOP. Остановка профиля
  - STATUS. Статус профиля
  - STATISTICS. Статистика выполнения профиля
  - RESTORE. Восстановление файлов из резервного хранилища
  - EXPORT. Экспорт параметров приложения
  - IMPORT. Импорт параметров приложения
  - ADDKEY. Применение файла ключа
  - LICENSE. Лицензирование
  - RENEW. Приобретение лицензии
  - PBATESTRESET. Сброс результатов проверки перед шифрованием диска
  - EXIT. Завершение работы приложения
  - EXITPOLICY. Выключение политики
  - STARTPOLICY. Включение политики
  - DISABLE. Выключение защиты
  - SPYWARE. Обнаружение шпионского ПО
  - KSN. Переключение KSN / KPSN

SERVERBINDINGDISABLE. Выключение защиты подключения к серверу
ZTNA. Удаленный доступ
Команды KESCLI
Scan. Поиск вредоносного ПО
GetScanState. Статус выполнения проверки
GetLastScanTime. Определения времени выполнения проверки
GetThreats. Получение данных об обнаруженных угрозах
UpdateDefinitions. Обновление баз и модулей приложения
GetDefinitionState. Определение даты и времени последнего обновления баз
EnableRTP. Включение защиты
GetRealTimeProtectionState. Статус Защиты от файловых угроз
GetEncryptionState. Статус шифрования диска
Version. Определение версии приложения
Команды управления Detection and Response
SANDBOX. Управление Sandbox
PREVENTION. Управление Запретом запуска объектов
ISOLATION. Управление Сетевой изоляцией
RESTORE. Восстановление файлов из карантина
IOCSCAN. Поиск индикаторов компрометации (IOC)
MDRLICENSE. Активация MDR
EDRKATA. Интеграция с EDR (KATA)
EDRExpertOnPrem. Интеграция с EDR Expert (on-premises)
KUMA. Интеграция с KUMA
YARA. Запуск YARA-проверки
TELEMETRYFILTERS. Фильтрация событий для отправки в KUMA
Команды управления Легким агентом
KSVLAINFO. Определение режима работы Легкого агента
VIISINFO. Статус подключения Легкого агента к Серверу интеграции
SVMINFO. Статус подключения Легкого агента к Серверу защиты
Коды ошибок
Приложение. Профили приложения
Управление приложением через REST API
Установка приложения с REST API
Работа с API
Источники информации о приложении
Обращение в Службу технической поддержки
О составе и хранении файлов трассировки
Трассировка работы приложения
Трассировка производительности приложения
Запись дампов
Защита файлов дампов и трассировок
Получение данных об ОС (Kaspersky Get System Info)
Ограничения и предупреждения
Глоссарий
Cloud discovery
IOC
IOC-файл

Kerberos-аутентификация
OLE-объект
OpenIOC
SVM
Агент администрирования
Агент аутентификации
Активный ключ
Антивирусные базы
Архив
База вредоносных веб-адресов
База фишинговых веб-адресов
Группа администрирования
Доверенный платформенный модуль
Задача
Зараженный файл
Издатель сертификата
Легкий агент
Лечение объектов
Лицензионный сертификат
Ложное срабатывание
Маска
Нормализованная форма адреса веб-ресурса
Область защиты
Область проверки
Портативный файловый менеджер
Потенциально заражаемый файл
Сервер интеграции
Приложения
Приложение 1. Параметры приложения
Защита от файловых угроз
Защита от веб-угроз
Защита от почтовых угроз
Защита от сетевых угроз
Сетевой экран
Защита от атак BadUSB
AMSI-защита
Защита от эксплойтов
Анализ поведения
Предотвращение вторжений
Откат вредоносных действий
Kaspersky Security Network
Анализ журналов
Защита от шифрования
Веб-Контроль
Контроль устройств
Контроль приложений
Адаптивный контроль аномалий

Контроль целостности системы
Endpoint Sensor
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert (on-premises)
Network Detection and Response (KATA)
Интеграция с KUMA
Полнодисковое шифрование
Шифрование файлов
Шифрование съемных дисков
Шаблоны (шифрование данных)
Исключения
Настройки приложения
Отчеты и хранилище
Настройки сети
Интерфейс
Управление настройками
Обновление баз и модулей приложения
Удаленный доступ
Приложение 2. Группы доверия приложений
Приложение 3. Расширения файлов для быстрой проверки съемных дисков
Приложение 4. Типы файлов для фильтра вложений Защиты от почтовых угроз
Приложение 5. Сетевые параметры для взаимодействия с внешними службами
Приложение 6. События приложения
Критическое
Отказ функционирования
Предупреждение
Информационное сообщение
Приложение 7. Поддерживаемые расширения файлов для Запрета запуска объектов
Приложение 8. Поддерживаемые интерпретаторы скриптов для Запрета запуска объектов
Приложение 9. Область поиска IOC в реестре (RegistryItem)
Приложение 10. Требования к IOC-файлам
Приложение 11. API для реагирования на угрозы EDR
Приложение 12. Учетные записи пользователей в правилах компонентов приложения
Юридическая информация
Предоставление данных
Предоставление данных в рамках Лицензионного соглашения
Предоставление данных при использовании Kaspersky Security Network
Предоставление данных при использовании решений Detection and Response
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
Интеграция с Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Соответствие законодательству Европейского союза (GDPR)

Уведомления о товарных знаках

Информация о стороннем коде

Справка Kaspersky Endpoint Security для Windows

Новые функции в версии 14.3

Добавлена поддержка аутентификации по токену для Защиты паролем

Что нового в каждой версии Kaspersky Endpoint Security для Windows

Начало работы

Развертывание Kaspersky Endpoint Security для Windows

Первоначальная настройка Kaspersky Endpoint Security для Windows

Лицензирование Kaspersky Endpoint Security для Windows

Предоставление данных

В рамках Лицензионного соглашения

При использовании KSN

GDPR

Устранение угроз

На рабочих станциях

На серверах

Реагирование на обнаружение индикатора компрометации (Сетевая изоляция → Карантин → Запрет запуска объектов)

Лучшие практики

Оптимизация производительности приложения

Внедрение режима Контроля приложений "По умолчанию запрещено"

Миграция KEA на KES со встроенным агентом

Использование KES в составе других решений

Kaspersky EDR

Kaspersky Sandbox

Kaspersky MDR

Что нового

Обновление 14.3

В Kaspersky Endpoint Security для Windows 14.3 появились следующие возможности и улучшения:

1. В компонент Интеграция с KUMA добавлена поддержка функциональности агентов KUMA. Теперь вы можете настроить получение и пересылку событий безопасности с устройства без необходимости выполнения отдельной установки агентов KUMA.

2. Для пользователей Endpoint Detection and Response Expert (on-premises) добавлена поддержка GZIP-сжатия телеметрии при использовании протоколов TCP и TCP/TLS.

3. Для компонента Контроль приложений добавлена поддержка новой KL-категории – *Инструменты ИИ*. Данная KL-категория включает в себя приложения от Anthropic, OpenAI и других поставщиков. Теперь вы можете настроить правила доступа к приложениям, входящим в KL-категорию Инструменты ИИ.

4. Добавлена поддержка интерфейса IOAV (IOfficeAntivirus) от Microsoft. Интерфейс IOAV, как и интерфейс AMSI, позволяет выполнять дополнительную проверку офисных документов и макросов. Таким образом, поддержка интерфейса IOAV позволяет улучшить защиту от атак, осуществляемых через офисные приложения.

Обновление 14.2

В Kaspersky Endpoint Security для Windows 14.2 появились следующие возможности и улучшения:

1. Изменен набор компонентов приложения, устанавливаемых по умолчанию. В конфигурацию приложения по умолчанию добавлены компоненты: Защита от атак BadUSB, управление BitLocker, встроенный агент EDR Optimum.

2. Добавлена поддержка аутентификации по токену (Защита паролем). Теперь для доступа к приложению вы можете использовать не только имя пользователя / пароль или временный пароль, выданный администратором, но и токен. Аутентификацию по токену можно использовать, например, для сервисных учетных записей без предоставления пароля.

3. Добавлен новый критерий надежности пароля для BitLocker – проверка истории паролей. Приложение не позволит задать пароль, который пользователь использовал ранее.

4. Добавлена возможность изменить язык интерфейса Kaspersky Endpoint Security при обновлении версии приложения с помощью задачи *Удаленная установка приложения*. Теперь вам не нужно переустанавливать приложение, если вы неверно выбрали язык интерфейса приложения.

5. Для пользователей решений Endpoint Detection and Response от "Лаборатории Касперского" добавлены новые события телеметрии: GPO Change, SCCM Local Config Mismatch, SCCM Config Change, SCCM Deployment Task, Smb Connection Open. Новые события повышают качество обнаружения угроз EDR-решений.

6. Для пользователей Kaspersky Endpoint Detection and Response Expert (on-premises) добавлена поддержка нового действия по реагированию на угрозы – *Поместить файл*. Эта задача позволяет доставлять на компьютеры конфигурационные файлы, скрипты для реагирования на угрозы, утилиты для устранения последствий атак и т.д. Задача *Поместить файл* доступна в OSMP-консоли с развернутым решением Kaspersky EDR Expert (on-premises) версии 9.0.

7. Для пользователей Kaspersky Endpoint Detection and Response Optimum улучшена работа действий по реагированию на угрозы. Теперь перед выполнением действия (*Удаление файла*, *Помещение файла на карантин* или *Запрет запуска объектов*) приложение проверяет, является ли объект критически важным для системы (англ. System Critical Object, SCO), и предупреждает о возможном влиянии на стабильность системы. Применять действия к файлам, относящимся к SCO, не рекомендуется.

8. Для пользователей Kaspersky Security для виртуальных сред Легкий агент добавлена поддержка работы приложения в составе отказоустойчивого кластера Серверов интеграции. Отказоустойчивый кластер Серверов интеграции обеспечивает непрерывную защиту виртуальной среды за счет переключения SVM и Легких агентов на резервный Сервер интеграции при отказе главного Сервера интеграции.

9. Поддержка операционной системы Windows 11 26H2.

10. При разработке этой версии Kaspersky Endpoint Security мы учли изменения, которые вошли в следующие приватные патчи: PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF22065, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF23095, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF24037, PF24043, PF24048, PF25013, PF25016, PF25019, PF25030.

Обновление 14.1

В Kaspersky Endpoint Security для Windows 14.1 появились следующие возможности и улучшения:

1. Добавлена поддержка операционной системы Windows Server 2025.

2. Увеличен лимит на количество правил фильтрации событий телеметрии Endpoint Detection and Response Expert (on-premises) и Kaspersky Endpoint Detection and Response Expert (cloud). Теперь Kaspersky Endpoint Security поддерживает до 10 000 включающих и исключающих правил фильтрации в совокупности.

3. Теперь вы можете настроить запуск задач только в указанные дни недели, с заданным интервалом в неделях. Расписание доступно в Kaspersky Security Center версии 16.1 и выше.

4. Для задачи *Поиск вредоносного ПО* теперь можно указать интервал, в течение которого выполнение задачи будет приостановлено, например, для минимизации влияния на производительность компьютера в периоды повышенных нагрузок.

5. Оптимизирована работа с дисковой подсистемой защищаемого компьютера за счет сокращения количества операций ввода-вывода (I/O).

6. При разработке этой версии Kaspersky Endpoint Security мы учли изменения, которые вошли в следующие приватные патчи: PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF14071, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF25013, PF25016, PF25019.

Обновление 14.0

В Kaspersky Endpoint Security для Windows 14.0 появились следующие возможности и улучшения:

1. Добавлена поддержка компьютеров с Arm-архитектурой. Вы можете установить приложение как в стандартном режиме, так и в режиме EDR-агента. При этом приложение имеет ряд ограничений (например, из технологий шифрования данных приложение поддерживает только BitLocker).

2. Поддержка расширенного аудита политик в Kaspersky Security Center Web Console версий 15.0 и выше. Теперь вы можете просматривать ревизии политик и сохранять ревизии политик в файл. *Ревизия* – набор измененных параметров, сохраненные пользователем. С помощью ревизий вы можете сравнивать и откатывать изменения параметров политики.

3. Для пользователей решений Endpoint Detection and Response добавлены новые события телеметрии. Новые события повышают качество обнаружения угроз с помощью EDR-решений от "Лаборатории Касперского".

4. При разработке этой версии Kaspersky Endpoint Security для Windows мы учли изменения, которые вошли в следующие приватные патчи: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Обновление 12.12

В Kaspersky Endpoint Security для Windows 12.12 появились следующие возможности и улучшения:

1. Функция защиты папок общего доступа от внешнего шифрования, которая входила в состав компонента Анализ поведения, выделена в отдельный компонент Защита от шифрования.

2. Добавлена поддержка протокола Kerberos для аутентификации приложения через прокси-сервер для доступа в интернет.

3. Добавлена возможность указывать хеш файла для доверенного приложения, а не только полный путь.

4. Для пользователей решений Endpoint Detection and Response (EDR) расширены возможности задачи *Поиск IOC*. Добавлена функция ретроспективного поиска IOC. *Ретроспективный поиск IOC* – это режим работы задачи *Поиск IOC*, при котором Kaspersky Endpoint Security выполняет поиск индикаторов компрометации по данным, полученным за определенный интервал времени. Режим предназначен для поиска индикаторов компрометации по данным сетевой активности компьютера. Kaspersky Endpoint Security анализирует данные в журналах операционной системы и браузеров на компьютере.

5. Для пользователей решений Endpoint Detection and Response (EDR) добавлена возможность снять ограничение на размер карантина. Это может понадобится при YARA-проверке, так как приложение может сохранять дамп памяти большого размера. Теперь вы можете использовать все свободное пространства диска для карантина.

6. Добавлена поддержка HTTPS-сжатия для оптимизации отправки событий в Kaspersky Unified Monitoring and Analysis Platform (KUMA). Это позволит уменьшить исходящий трафик.

7. При разработке этой версии Kaspersky Endpoint Security для Windows мы учли изменения, которые вошли в следующие приватные патчи: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Обновление 12.11

В Kaspersky Endpoint Security для Windows 12.11 появились следующие возможности и улучшения:

1. Добавлена проверка настройки компонентов контроля перед сохранением параметров. Проверка добавлена для компонентов Контроль приложений, Контроль устройств, Контроль целостности системы. Теперь приложение показывает предупреждение пользователю, если текущие настройки компонента контроля могут привести к повышенной нагрузке на компьютер или сбоям в работе системы. Например, если для Контроля приложений вы выбрали режим блокировки всех приложений, кроме разрешенных, и не добавили ни одного разрешающего правила, то приложение покажет предупреждение, так как это может привести к сбоям в работе системы.

2. Добавлена возможность автоматической отправки файлов на проверку в KATA Sandbox. *KATA Sandbox* – компонент Kaspersky Anti Targeted Attack Platform, который запускает файлы на виртуальных образах операционных систем. Sandbox анализирует поведение объектов для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации. Sandbox выполняет анализ и проверку объектов на специальных серверах с развернутыми виртуальными образами операционных систем Microsoft Windows (серверы Sandbox). Для работы KATA Sandbox в автоматическом режим должно быть развернуто решение Kaspersky Anti Targeted Attack Platform версии 8.0 или выше.

3. Оптимизировали отправку EDR-телеметрии. Теперь вы можете задавать максимальную длину пакетов.

4. Улучшена диагностика подключения к Kaspersky Security Network. Детализировали ошибки подключения к Kaspersky Security Network для устранения возможных проблем.

5. Добавлена возможность настраивать списки событий для отправки в Kaspersky Unified Monitoring and Analysis Platform (KUMA). Теперь кроме предустановленных списков событий в KUMA вы можете вручную добавлять события в телеметрию или исключать события по идентификатору в журнале событий Windows.

6. Обновлен интерфейс политик в Web Console. Изменилась структура разделов в политике, чтобы быстрее находить нужные функции.

7. Поддержка операционной системы Windows 11 25H2.

8. При разработке этой версии Kaspersky Endpoint Security для Windows мы учли изменения, которые вошли в следующие приватные патчи: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

Обновление 12.10

В Kaspersky Endpoint Security для Windows 12.10 появились следующие возможности и улучшения:

1. Для компонента Защита от атак BadUSB добавлена возможность пройти авторизацию сканеров штрихкодов, считав штрихкод с экрана. Теперь вам не нужно вводить код с помощью экранной клавиатуры для авторизации сканеров штрихкодов.

2. Для пользователей решений Endpoint Detection and Response (EDR) от "Лаборатории Касперского" появились следующие возможности и улучшения:

   - Добавлена возможность управлять Сетевой изоляцией компьютера в деталях алерта. Также в деталях алерта вы можете задавать срок Сетевой изоляции компьютера и добавлять исключения.

   - Наполнение деталей алерта новыми данными. Теперь детали алерта содержат больше информации об угрозе, включая действия приложения при реагировании на угрозы EDR.

   - Улучшено взаимодействие с IOC-файлами. Теперь вы можете просматривать содержимое IOC-файлов в интерфейсе Kaspersky Security Center Web Console и редактировать содержание. После загрузки IOC-файла приложение показывает отчет о применении IOC-терминов.

   - Улучшено реагирование на обнаруженные IOC. Теперь вы можете помещать файлы на карантин, обнаруженные при выполнении задачи *Поиск IOC*, прямо в результатах обнаружения IOC в свойствах задачи. Также в свойствах задачи вы можете изолировать компьютеры от сети.

   - Добавлена возможность создавать IOC-файлы прямо в свойствах задачи *Поиск IOC* на основе сформированных в TXT-файле списков хешей файлов, IP-адресов или DNS-имен.

   - Расширена область поиска для задачи *Поиск IOC*. Теперь вы можете формировать область поиска IOC в реестре (**Реестр Windows - RegistryItem**). В предыдущих версиях приложения вы могли использовать только предустановленную область поиска IOC в реестре.

3. Добавлено новое разрешение Защиты паролем – *Экспорт настроек*. По умолчанию только пользователь KLAdmin может создавать конфигурационный файл с параметрами Kaspersky Endpoint Security в интерфейсе приложения. Для доступа других пользователей вам нужно предоставить соответствующее разрешение.

4. При разработке этой версии Kaspersky Endpoint Security для Windows мы учли изменения, которые вошли в следующие приватные патчи: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

Обновление 12.9

В Kaspersky Endpoint Security для Windows 12.9 появились следующие возможности и улучшения:

1. Добавлен новый инструмент – *Мониторинг временных паролей*. Временный пароль позволяет предоставить доступ к приложению Kaspersky Endpoint Security с включенной Защитой паролем для отдельного компьютера. Мониторинг временных паролей позволяет сохранять историю паролей (до 30 дней), контролировать статус временного пароля (*Активен*, *Истек*, *Отозван*) и отзывать временные пароли.

2. Добавлена возможность разрывать подключение к веб-ресурсам, запрещенные правилами Веб-Контроля, сразу после применения политики. В предыдущих версиях приложения Веб-Контроль ограничивал только новые подключения к запрещенным веб-ресурсам.

3. Для пользователей Kaspersky Anti Targeted Attack Platform добавлена возможность запускать YARA-проверку локально на компьютере. Для этого вам нужно загрузить файл с YARA-правилами и выполнить команду в CMD.

4. Исправлено поведение приложения при включении BitLocker на компьютерах, на которых диски уже защищены BitLocker с помощью сторонних инструментов. Kaspersky Endpoint Security запускает процедуру восстановления для передачи ключа восстановления в Kaspersky Security Center. Таким образом, управление BitLocker переходит в консоль Kaspersky Security Center.

5. Для пользователей решений Detection and Response от "Лаборатории Касперского" добавлен новый раздел **История реагирования**. Этот раздел содержит информацию о выполненных на компьютере действиях по реагированию на угрозы. К таким действиям относятся, например, запуск задачи *Завершение процесса* или сетевая изоляция компьютера. История реагирования доступна для пользователей следующих решений от "Лаборатории Касперского: MDR, EDR, KATA.

6. Для пользователей Kaspersky Unified Monitoring and Analysis Platform добавлена поддержка действий по реагированию на угрозы EDR. При реагировании на угрозы KUMA запускает скрипты, которые создают соответствующие EDR-задачи. Для выполнения EDR-задач вам нужно создать правило реагирования для пользовательского скрипта в консоли KUMA и выбрать события.

7. При разработке этой версии Kaspersky Endpoint Security для Windows мы учли изменения, которые вошли в следующие приватные патчи: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

Обновление 12.8

В Kaspersky Endpoint Security для Windows 12.8 появились следующие возможности и улучшения:

1. Добавлена поддержка работы приложения в режиме Легкого агента для защиты виртуальных сред. Теперь вы можете развернуть приложение в роли Легкого агента в составе решения Kaspersky Security для виртуальных сред 6.2 Легкий агент.

2. Добавлена возможность перехватывать файловые операции в Docker-контейнерах на серверах. *Контейнер* – это изолированная среда, где приложение может работать без прямого взаимодействия с операционной системой. Kaspersky Endpoint Security проверяет файлы внутри контейнеров, к которым обращается пользователь. При обнаружении угрозы, приложение блокирует вредоносную активность и пытается вылечить файл в контейнере. Если вылечить файл не удалось, приложение останавливает контейнер.

3. Добавлена возможность сформировать область защиты для функции защиты папок общего доступа от внешнего шифрования (компонент Анализ поведения). Теперь вы можете указывать папки общего доступа, файловую активность в которых будет отслеживать приложение. Также вы можете исключать файлы из области защиты. В предыдущих версиях приложения компонент Анализ поведения отслеживал файловую активность во всех папках общего доступа.

4. Добавлена возможность настраивать разные наборы компонентов для разных типов операционных систем в инсталляционном пакете. То есть вы можете разворачивать приложение на рабочие станции и серверы с помощью одного инсталляционного пакета. Компоненты, которые недоступны для типа операционной системы, автоматически исключены в свойствах инсталляционного пакета.

5. Добавлена возможность выбирать предустановленные исключения из проверки и доверенные приложения. Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки доверенной зоны для работы приложения в виртуальной среде (Citrix, VMware). К таким исключениям относятся, например, файлы виртуальных машин VHD и VHDX. Вы можете добавить исключения при создании инсталляционного пакета приложения, создании политики или при установке Kaspersky Endpoint Security.

6. В EDR-телеметрию добавлены события операций с устройствами, подключенных по USB. Также вы можете добавить эти события в исключения из EDR-телеметрии.

7. Добавлена возможность блокировать сетевые соединения по устаревшему протоколу TLS 1.0. Протокол TLS 1.0 имеет низкий уровень безопасности, поэтому рекомендуется отключить этот протокол и использовать более новые версии TLS 1.2 или TLS 1.3. По умолчанию Kaspersky Endpoint Security блокирует соединение по протоколу TLS 1.0. После обновления версии приложения работа сторонних сервисов, которые используют протокол TLS 1.0, может быть нарушена. Чтобы избежать сбоев в работе сторонних сервисов перед обновлением версии приложения вы можете разрешить использование протокола TLS 1.0 в групповой политике.

8. При разработке этой версии Kaspersky Endpoint Security для Windows мы учли изменения, которые вошли в следующие приватные патчи: PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

Обновление 12.7

В Kaspersky Endpoint Security для Windows 12.7 появились следующие возможности и улучшения:

1. Добавлена возможность ограничить потребление ресурсов процессора для задач *Поиск вредоносного ПО*. Для этого вам нужно в параметрах приложения установить максимальное значение нагрузки на все ядра процессора при проверке компьютера в процентах.

2. Добавлена возможность вручную отправлять файлы на проверку в KATA Sandbox. *KATA Sandbox* – компонент Kaspersky Anti Targeted Attack Platform, который запускает файлы на виртуальных образах операционных систем. Sandbox анализирует поведение объектов для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации. Sandbox выполняет анализ и проверку объектов на специальных серверах с развернутыми виртуальными образами операционных систем Microsoft Windows (серверы Sandbox). Для отправки файла на проверку в KATA Sandbox пользователю нужно выбрать соответствующий пункт в контекстном меню файла.

3. Добавлена возможность интеграции с решением, обеспечивающим защиту внутренней сети предприятия, – *Kaspersky Network Detection and Response*. Kaspersky Network Detection and Response (NDR) входит в состав Kaspersky Anti Targeted Attack Platform. Вы можете настроить взаимодействие с NDR как в стандартном режиме установки приложения, так и в режиме EDR-агента.

4. Поддержка почтового клиента Microsoft Office Outlook версии 2021 для расширения компонента Защита от почтовых угроз. Расширение предназначено для проверки сообщений на уровне почтового клиента, а не протокола. Расширение позволяет проверять в почтовом клиенте не только сообщения, но и объекты полученные через интерфейс MAPI из хранилищ Microsoft Exchange (например, объекты в Календаре).

5. При разработке этой версии Kaspersky Endpoint Security для Windows мы учли изменения, которые вошли в следующие приватные патчи: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Обновление 12.6

В Kaspersky Endpoint Security для Windows 12.6 появились следующие возможности и улучшения:

1. Добавлена возможность интеграции с SIEM-решением от "Лаборатории Касперского" – *Kaspersky Unified Monitoring and Analysis Platform (KUMA)*. Теперь у вас есть возможность отправлять события из журналов Windows в KUMA. Это позволяет получать в KUMA события из журналов Windows (поддерживается ограниченный набор EventID) со всех компьютеров, на которых установлено приложение Kaspersky Endpoint Security, без установки агентов KUMA на эти компьютеры.

2. Вместо компонента Мониторинга файловых операций добавлен новый компонент *Контроль целостности системы*. Контроль целостности системы включает в себя все функции Мониторинга файловых операций, а также позволяет контролировать изменения в реестре и подключение внешних устройств. Контроль целостности системы отслеживает изменения в операционной системе, которые могут указывать на нарушения безопасности компьютера. Обнаружив такие изменения, Kaspersky Endpoint Security формирует соответствующие события и предупреждает администратора. Мониторинг файловых операций удален из приложения. Параметры Мониторинга файловых операций мигрируют в Контроль целостности системы автоматически при обновлении приложения. Для корректной работы Контроля целостности системы нужно обновить не только приложение Kaspersky Endpoint Security, но и плагин управления до версии 12.6.

3. Добавлен статус установленного встроенного агента EDR (KATA) в свойствах компьютера в консоли Kaspersky Security Center. Теперь, если у вас установлен встроенный агент EDR (KATA), в графе **Статус Endpoint Sensor** отображается текущий статус работы компонента (например, *Выполняется*, *Остановлен*, *Не поддерживается лицензией* и так далее).

4. Добавлена возможность выбрать предустановленные исключения из проверки и доверенные приложения. Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки доверенной зоны для работы приложения на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. К таким исключениям относятся, например, файлы баз данных MDF и LDF. Вы можете добавить исключения при создании новой политики, изменении текущей политики или при установке Kaspersky Endpoint Security.

5. Отображение деталей алерта для Kaspersky Endpoint Detection and Response Optimum перенесены из плагина управления Kaspersky Endpoint Security в отдельный плагин управления Kaspersky Endpoint Detection and Response. Плагин управления EDR является единым плагином для работы с агентами на операционных системах Windows, Mac и Linux. Теперь для работы с EDR Optimum вам нужен плагин управления Kaspersky Endpoint Security для создания задач реагирования на угрозы и плагин управления EDR для просмотра деталей алерта.

6. Поддержка операционной системы Windows 11 24H2.

7. При разработке этой версии Kaspersky Endpoint Security для Windows мы учли изменения, которые вошли в следующие приватные патчи: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

Обновление 12.5

В Kaspersky Endpoint Security для Windows 12.5 появились следующие возможности и улучшения:

1. Добавлена возможность управлять исключениями для телеметрии. *Телеметрия* – список событий, которые произошли на защищаемом компьютере. Данные телеметрии использует Kaspersky Anti Targeted Attack Platform (EDR) для анализа и защиты IT-инфраструктуры организации. Исключения позволяют повысить производительность компьютера и оптимизировать отправку данных на Сервер сбора телеметрии.

2. Улучшен интерфейс доверенной зоны приложения. Теперь Kaspersky Endpoint Security скрывает от пользователя объекты из доверенной зоны, если администратор запретил пользователю добавлять собственные (локальные) исключения из проверки и доверенные приложения. Это предотвращает несанкционированный доступ злоумышленника к доверенной зоне, повышая уровень безопасности компьютера.

3. Добавлена проверка трафика для почтовых клиентов МойОфис Почта и Органайзер Р7-Офис. Теперь компонент Защита от почтовых угроз проверяет не только вложения сообщений при загрузке, но и получаемые и отправляемые сообщения.

4. Добавлена веб-категория *Инструменты генеративного ИИ*. Вы можете настроить доступ к веб-сайтам из новой категории с помощью Веб-Контроля.

5. Добавлена возможность выбрать расположение сетевого пакетного правила в списке Сетевого экрана. Расположение сетевого пакетного правила в списке определяет его приоритет. В предыдущих версиях приложения новое правило можно было добавить только в конец списка, после чего требовалось вручную переместить правило по списку для задания приоритета. Теперь при добавлении правила вы можете выбирать расположение правила в списке: в начале, в конце списка или рядом с выбранным правилом.

6. В правилах компонентов Kaspersky Endpoint Security добавлена возможность выбирать пользователей не только из Active Directory, но и из списка пользователей в Kaspersky Security Center или вы можете ввести данные локальной учетной записи вручную. Такая возможность добавлена для правил следующих компонентов: Контроль приложений, Контроль устройств, Веб-Контроль, Адаптивный контроль аномалий и Анализ журналов.

7. В отчет об обнаружении сетевой атаки добавлена графа с MAC-адресом атакующего компьютера (компонент Защита от сетевых угроз). Теперь вы можете посмотреть в отчете не только IP-адрес атакующего компьютера, но и MAC-адрес. Это поможет в расследовании инцидентов. Также отчеты с MAC-адресом атакующего компьютера будут доступны в консоли Kaspersky Security Center Linux версии 15.1 и выше.

8. Повышен уровень требований к защите компьютера. Теперь для обеспечения высокого уровня защиты обязательно должна быть включена Защита служб приложения от внешнего управления. Проверьте индикатор уровня защиты, который отображается в верхней части окна политики. Если у вас средний или низкий уровень защиты, вы можете включить Защиту служб приложения от внешнего управления в окне с рекомендациями индикатора уровня защиты.

9. Добавлена поддержка новых событий обнаружения объектов при работе приложения в конфигурации Endpoint Detection and Response Agent (EDR Agent). В конфигурации [KES+встроенный агент] эти события уже формируются.

10. При разработке этой версии Kaspersky Endpoint Security для Windows мы учли изменения, которые вошли в следующие приватные патчи: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

Обновление 12.4

В Kaspersky Endpoint Security для Windows 12.4 появились следующие возможности и улучшения:

1. Добавлена новая функция для защиты подключения компьютера к Kaspersky Security Center. Новая задача *Защита подключения к Серверу администрирования* позволяет задать пароль для подключения к доверенному серверу. Таким образом, переподключить компьютер и выполнить команды с другого сервера без этого пароля невозможно.

2. Для компонента Защита паролем добавлена возможность выбирать пользователей вручную, а не только из Active Directory. То есть вы можете вручную задать имя пользователя и пароль и назначить права доступа к Kaspersky Endpoint Security для этой учетной записи. Таким образом, вам не нужно делиться паролем от KLAdmin с другими пользователями или создавать новые учетные записи Active Directory для контроля доступа к приложению.

3. Поддержка операционной системы Windows 11 23H2.

Обновление 12.3

В Kaspersky Endpoint Security для Windows 12.3 появились следующие возможности и улучшения:

1. Добавлена возможность установить приложение в конфигурации Endpoint Detection and Response Agent. Эта конфигурация позволяет установить приложение с набором компонентов, необходимым для работы решений Detection and Response от "Лаборатории Касперского": Kaspersky Managed Detection and Response и Kaspersky Anti Targeted Attack Platform (EDR). Вы можете установить приложение в этой конфигурации вместе с решениями от сторонних поставщиков (например, Dr.Web, Dallas Lock, ESET). Таким образом, теперь у вас есть возможность использовать средства защиты инфраструктуры от сторонних поставщиков совместно с решениями Detection and Response от "Лаборатории Касперского".

2. Улучшена работа Kaspersky Endpoint Security с Bluetooth-устройствами. Теперь вы можете настроить исключения и ограничить доступ ко всем Bluetooth-устройствам кроме устройств ввода (беспроводные клавиатуры, мыши и т.п.).

3. Оптимизирована работа Контроля приложений с базой данных исполняемых файлов. Теперь Kaspersky Endpoint Security автоматически удаляет информацию о файлах из базы данных, если файл удален с компьютера. Это позволяет поддерживать базу данных в актуальном состоянии и экономить ресурсы Kaspersky Security Center.

4. Повышен уровень требований к защите компьютера. Теперь для обеспечения высокого уровня защиты обязательно должна быть включена Защита паролем. Проверьте индикатор уровня защиты, который отображается в верхней части окна политики. Если у вас средний или низкий уровень защиты, вы можете включить Защиту паролем в окне с рекомендациями индикатора уровня защиты.

5. Добавлена поддержка протокола HTTPS для работы приложения с Kaspersky Security Network. Включите использование HTTPS в свойствах Сервера администрирования в параметрах прокси-сервера KSN.

Обновление 12.2

В Kaspersky Endpoint Security для Windows 12.2 появились следующие возможности и улучшения:

1. Добавлена поддержка протокола WPA3 для контроля подключения к сетям Wi-Fi (Контроль устройств). Теперь вы можете выбрать WPA3 в настройках доверенной сети Wi-Fi и запретить подключение к сети по менее безопасному протоколу.

2. Добавлена возможность выбирать протокол и порты для исключений Защиты от сетевых угроз. Теперь вы можете указать не только IP-адреса доверенных устройств, но и выбрать порт и протокол. Это позволяет исключить определенные потоки данных и предотвратить сетевые атаки с доверенных IP-адресов.

3. Изменен порядок источников обновлений для локальной задачи *Обновление баз и модулей приложения*, если к компьютеру применена политика. Теперь приложение по умолчанию использует сервер Kaspersky Security Center в качестве первого источника обновлений, а не серверы "Лаборатории Касперского". Это позволит уменьшить расход трафика при запуске локальной задачи *Обновление баз и модулей приложения* пользователем.

Обновление 12.1

В Kaspersky Endpoint Security для Windows 12.1 появились следующие возможности и улучшения:

1. Добавлен встроенный агент для работы с решением Kaspersky Anti Targeted Attack Platform. Теперь вам не нужен Kaspersky Endpoint Agent для работы EDR (KATA). Все функции Kaspersky Endpoint Agent будет выполнять Kaspersky Endpoint Security. Для переноса политик Kaspersky Endpoint Agent воспользуйтесь мастером миграции. После обновления приложения Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent. Kaspersky Endpoint Agent добавлен в список несовместимого ПО. Так как в Kaspersky Endpoint Security добавлены встроенные агенты для работы всех решений Detection and Response, устанавливать Kaspersky Endpoint Agent для интеграции с этими решениями больше не требуется.

2. Добавлен режим совместимости с Azure WVD. Функция позволяет корректно показывать состояние виртуальной машины Azure в консоли Kaspersky Anti Targeted Attack Platform. Режим совместимости с Azure WVD позволяет назначать постоянный уникальный Sensor ID для этих виртуальных машин.

3. Добавлена возможность настроить доступ пользователей к мобильным устройствам в приложении iTunes или приложениях аналогах. То есть, вы можете, например, разрешить использовать мобильное устройство только в приложении iTunes и запретить использовать мобильное устройство в качестве съемного носителя. Также приложение поддерживает эти правила для приложения Android Debug Bridge (ADB).

4. Прекращена поддержка Kaspersky Security Center версии 11. Обновите Kaspersky Security Center до последней версии.

Исправленные ошибки

В таблице ниже перечислены все ошибки, обнаруженные в предыдущих версиях Kaspersky Endpoint Security и исправленные в текущей версии.

Список ошибок, исправленных в версии 14.2

Идентификатор	Описание
10110351	Контроль устройств разрешает доступ к MTD-устройству (SD-карта) при выбранном действии **Запрещать** для типа устройств **Съемные диски**.
10068496	На защищаемом устройстве есть возможность выбирать режим защиты от MAC-спуфинга, когда в родительской политике заблокированы настройки Защиты от сетевых угроз.
10095087	При включенной проверке защищенных соединений открытие любого веб-сайта через межсетевой экран нового поколения (NGFW) с отозванным сертификатом сопровождается уведомлением о переходе на домен с недоверенным сертификатом.
10140912	При установленном приложении компьютер не обнаруживает устройство BHT1100B PDA под управлением Windows Mobile.
10141009	При установленном компоненте Шифрование файлов приложение Anthropic Claude может не запускаться.

Идентификатор	Описание
10610853	После обновления приложения до новой версии не удается открыть политику, так как в настройках Контроля устройств новой версии присутствуют устройства, не поддерживаемые в предыдущей версии.
10720516	Вложения в файлах офисных форматов могут не открываться при установленном приложении.
10421967	Не удается авторизоваться в общем почтовом ящике, если он добавлен как отдельная учетная запись.

Список ошибок, исправленных в веб-плагине 14.2.0.8289

Идентификатор	Описание
9946286	В правило Веб-Контроля не удается добавить адрес сайта по маске, в которой отсутствует точка между доменом и доменной зоной.
10054657 10507166	После миграции на новую версию не удается управлять настройками некоторых компонентов через политику (например, Контроль устройств и Контроль приложений).
10084390	В настройках компонента Контроль устройств дублируется тип устройства **Жесткий диск**, что приводит к блокировке жестких дисков пользователей.
10113718	В некоторых случаях не отображаются пользовательские правила Сетевого экрана.
10311613	В настройках компонента Предотвращение вторжений не удается добавить защищаемый ресурс по маске с использованием символа `*`.
10391923	В Контроле приложений при создании категории приложений на основе MD5-хеша файла не отображается предупреждение о том, что такая категория невалидна и не будет работать.
10571790	Для компонента Контроль приложений исправлен заголовок списка запрещающих правил в режиме **Разрешать все, не указанное в списке правил**.
10592891 10689065	В Доверенной зоне для исключений в разделе **Исключения из Поиска вредоносного ПО** не отображается поле **Комментарий**.
10613015 10689049 10592534	В компоненте Контроль устройств для доверенных устройств не отображается поле **Комментарий**.
10645068 10689057	Задача *Удаление ключа* не запускается, если выбран файл лицензионного ключа в формате KEY.
10685370 10685422	В компоненте Контроль устройств не удается добавить новое устройство в список доверенных, если в нем уже есть устройство с таким именем.
10721136	Не удается сохранить групповую задачу, если в настройках расписания не указана дата его завершения.
10753509	При изменении списка пользователей и групп для доверенных устройств компонента Контроль устройств может изменяться тип записей, в результате чего настройки перестают применяться на устройстве.
10773402	В некоторых случаях могут не сохраняться изменения в настройках политики из-за повреждения профилей.
10822620	В политике не отображаются настройки компонента Защита от шифрования, а также не сохраняются изменения настроек уведомлений.
10817035	В дочерней политике доступно добавление доверенного устройства, даже если эта настройка заблокирована в родительской политике ("замок" закрыт). При этом добавленное устройство не сохраняется.
10678009	В веб-плагине Kaspersky Endpoint Security не удается добавить новое правило Сетевого экрана в политику, если ранее было создано правило с использованием диапазона IP-адресов.

Список ошибок, исправленных в версии 14.1

Идентификатор	Описание
10140523	Включение Native NVMe в Windows 11 может приводить к нестабильной работе приложения.
9340076	На устройстве, где установлено приложение с включенным компонентом Шифрование файлов, Windows Explorer автоматически не обновляет отображение содержимого сетевой папки при ее изменении на другом устройстве.
9722863	В отчете компонента Контроль устройств не отображается событие отключения USB-токена.
10006481	После применения правила, запрещающего входящий трафик, активные TCP-соединения с внешними сервисами могут преждевременно разрываться из-за некорректного расчета таймаута.
10140912	Приложение не распознает устройство BHT1100B PDA.
10157563	На рабочих VDI-станциях после перезагрузки может не работать перенаправление папок (Folder Redirection).
10158494	Компонент Контроль устройств регистрирует множественные события подключения / отключения съемного устройства без его физического переподключения.

Часто задаваемые вопросы



ОБЩЕЕ

На каких компьютерах работает Kaspersky Endpoint Security?

Что изменилось с последней версии?

С какими другими приложениями "Лаборатории Касперского" может работать Kaspersky Endpoint Security?

Как сэкономить ресурсы компьютера при работе Kaspersky Endpoint Security?



РАЗВЕРТЫВАНИЕ

Как установить Kaspersky Endpoint Security на все компьютеры организации?

Какие параметры установки можно настроить в командной строке?

Как дистанционно удалить Kaspersky Endpoint Security?



ОБНОВЛЕНИЕ

Какие есть способы обновления баз?

Что делать, если после обновления появились проблемы?

Как обновить базы вне сети организации?

Возможно ли использование прокси-сервера для обновления?



БЕЗОПАСНОСТЬ

Каким образом Kaspersky Endpoint Security проверяет почту?

Как исключить доверенный файл из проверки?

Как защитить компьютер от вирусов на флешках?

Как выполнить поиск вредоносного ПО незаметно для пользователя?

Как приостановить защиту Kaspersky Endpoint Security на время?

Как восстановить файл, который Kaspersky Endpoint Security ошибочно удалил?

Как защитить Kaspersky Endpoint Security от удаления пользователем?



ИНТЕРНЕТ

Проверяет ли Kaspersky Endpoint Security защищенные соединения (HTTPS)?

Как разрешить пользователям подключаться только к доверенным сетям Wi-Fi?

Как заблокировать социальные сети?



ПРИЛОЖЕНИЯ

Как узнать, какие приложения установлены на компьютере пользователя (инвентаризация)?

Как предотвратить запуск компьютерных игр?

Как проверить, что Контроль приложений настроен верно?

Как добавить приложение в список доверенных?



УСТРОЙСТВА

Как запретить использовать флешки?

Как добавить устройство в список доверенных?

Можно ли получить доступ к заблокированному устройству?



ШИФРОВАНИЕ

При каких условиях шифрование невозможно?

Как ограничить доступ к архиву с помощью пароля?

Возможно ли использование смарт-карт и токенов при шифровании?

Можно ли получить доступ к зашифрованным данным, если нет связи с Kaspersky Security Center?

Что делать, если на компьютере вышла из строя ОС, а данные остались зашифрованы?



ПОДДЕРЖКА

Где лежит файл с отчетами?

Как создать файл трассировки?

Как включить запись дампов?

Kaspersky Endpoint Security для Windows

Kaspersky Endpoint Security для Windows (далее также Kaspersky Endpoint Security) обеспечивает комплексную защиту компьютера от различного вида угроз, сетевых и мошеннических атак.

Приложение не предназначено для использования в технологических процессах, в которых применяются автоматизированные системы управления. Для защиты устройств в таких системах рекомендуется использовать приложение Kaspersky Industrial CyberSecurity for Nodes.

Технологии обнаружения угроз

Машинное обучение

Kaspersky Endpoint Security использует модель на основе машинного обучения. Модель разработана специалистами "Лаборатории Касперского". Далее модель постоянно получает данные об угрозах из KSN (обучение модели).

Облачный анализ

Kaspersky Endpoint Security получает данные об угрозах из Kaspersky Security Network. *Kaspersky Security Network (KSN)* – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения.

Экспертный анализ

Kaspersky Endpoint Security использует данные об угрозах, добавленные вирусными аналитиками "Лаборатории Касперского". Вирусные аналитики проверяют объекты, если определить репутацию объекта автоматически не удалось.

Поведенческий анализ

Kaspersky Endpoint Security анализирует активность объекта в режиме реального времени.

Автоматический анализ

Kaspersky Endpoint Security получает данные от системы автоматического анализа объектов. Система обрабатывает все объекты, которые поступают в "Лабораторию Касперского". Далее система определяет репутацию объекта и добавляет данные в антивирусные базы. Если системе не удалось определить репутацию объекта, система отправляет запрос вирусным аналитикам "Лаборатории Касперского".

Sandbox

Kaspersky Endpoint Security проверяет объект на виртуальной машине. Kaspersky Sandbox анализирует поведение объекта и принимает решение о его репутации. Технология доступна, только если вы используете решение Kaspersky Sandbox.

Cloud Sandbox

Kaspersky Endpoint Security проверяет объекты в изолированной среде, которую предоставляет "Лаборатория Касперского". Технология Cloud Sandbox включена постоянно и доступна всем пользователям Kaspersky Security Network независимо от типа лицензии, которую вы используете. Если у вас развернуто решение Endpoint Detection and Response, вы можете включить отдельный счетчик для угроз, обнаруженных с помощью Cloud Sandbox.

Компоненты приложения

Каждый тип угроз обрабатывается отдельным компонентом. Можно включать и выключать компоненты независимо друг от друга, а также настраивать параметры их работы.

Раздел	Компонент
Базовая защита 	**Защита от файловых угроз** Компонент Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. По умолчанию компонент Защита от файловых угроз постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы в режиме реального времени. Компонент проверяет файлы на всех дисках компьютера, а также на подключенных дисках. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа. **Защита от веб-угроз** Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует соединение с вредоносными и фишинговыми веб-сайтами. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа. **Защита от почтовых угроз** Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других приложений, представляющих угрозу. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа. Защита от почтовых угроз может проверять и получаемые, и отправляемые сообщения. Приложение поддерживает протоколы POP3, SMTP, IMAP, NNTP в следующих почтовых клиентах: • Microsoft Office Outlook; • Mozilla Thunderbird; • Windows Mail; • МойОфис Почта; • Органайзер Р7-Офис. Для проверки защищенного трафика в почтовых клиентах Mozilla Thunderbird, МойОфис Почта и Органайзер Р7-Офис вам нужно включить использование хранилища сертификатов Windows для приложений на основе технологий Mozilla. Другие протоколы и почтовые клиенты Защита от почтовых угроз не поддерживает. Защита от почтовых угроз не всегда может получить доступ к сообщениям на *уровне протокола* (например, при использовании решения Microsoft Exchange). Поэтому дополнительно в состав Защиты от почтовых угроз включено расширение для Microsoft Office Outlook. Расширение позволяет проверять сообщения на *уровне почтового клиента*. Расширение компонента Защита от почтовых угроз поддерживает работу с 32- и 64-разрядными версиями Outlook 2010, 2013, 2016, 2019, 2021, 2024, 365. На компьютерах с архитектурой Arm расширение компонента Защита от почтовых угроз поддерживает работу с 32- и 64-разрядной версией Outlook 2016 и Outlook 2021, 2024, 365 для Arm64. **Защита от сетевых угроз** Компонент *Защита от сетевых угроз* (также Intrusion Detection System (IDS) – система обнаружения вторжений) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, приложение блокирует сетевое соединение с атакующим компьютером. Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах приложения. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей приложения. **Сетевой экран** Сетевой экран блокирует несанкционированные подключения к компьютеру во время работы в интернете или локальной сети. Также Сетевой экран контролирует сетевую активность приложений на компьютере. Это позволяет защитить локальную сеть организации от кражи персональных данных и других атак. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и предустановленных *сетевых правил*. **Защита от атак BadUSB** Компонент Защита от атак BadUSB позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру. **AMSI-защита** Компонент AMSI-защита предназначен для поддержки интерфейса Antimalware Scan Interface от Microsoft. *Интерфейс Antimalware Scan Interface (AMSI)* позволяет сторонним приложениям с поддержкой AMSI отправлять объекты (например, скрипты PowerShell) в Kaspersky Endpoint Security для дополнительной проверки и получать результаты проверки этих объектов.

Раздел	Компонент
Продвинутая защита 	**Kaspersky Security Network** *Kaspersky Security Network (KSN)* – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, приложение Kaspersky Endpoint Security получает от служб KSN сведения о репутации проверяемых веб-адресов, а также сведения о категории и репутации проверяемых файлов. **Анализ поведения** Компонент Анализ поведения получает данные о действиях приложений на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы. Компонент Анализ поведения использует шаблоны опасного поведения приложений. Если активность приложения совпадает с одним из шаблонов опасного поведения, Kaspersky Endpoint Security выполняет выбранное ответное действие. Функциональность Kaspersky Endpoint Security, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера. Компонент Анализ поведения дополнительно контролирует сетевые порты для процессов приложений, которые могут представлять угрозу безопасности компьютера. Приложение получает данные о таких процессах с антивирусными базами. **Защита от шифрования** Компонент Защита от шифрования обеспечивает анализ активности в папках общего доступа. Если активность совпадает с одним из шаблонов поведения, характерного для внешнего шифрования, Kaspersky Endpoint Security выполняет выбранное действие. **Защита от эксплойтов** Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимое приложение. При обработке этих данных уязвимое приложение выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО. Если попытка запустить исполняемый файл из уязвимого приложения не была произведена пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла или информирует пользователя. Компонент Защита от эксплойтов дополнительно контролирует сетевые порты для процессов приложений, которые могут представлять угрозу безопасности компьютера. Приложение получает данные о таких процессах с антивирусными базами. **Предотвращение вторжений** Компонент Предотвращение вторжений (англ. Host Intrusion Prevention System, HIPS) предотвращает выполнение приложениями опасных для системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и персональным данным. Компонент обеспечивает защиту компьютера с помощью антивирусных баз и облачной службы Kaspersky Security Network. **Откат вредоносных действий** Компонент Откат вредоносных действий позволяет Kaspersky Endpoint Security отменять действия, произведенные вредоносными приложениями в операционной системе.
Удаленный доступ 	Встроенный VPN-агент обеспечивает защищенное подключение к корпоративной сети через общедоступные сети. Для этого Kaspersky Endpoint Security использует инфраструктуру Kaspersky NGFW. Данная функция находится на этапе бета-тестирования и доступна только участникам программы бета-тестирования решений "Лаборатории Касперского". Работа функции может быть нестабильной.

Раздел	Компонент
Контроль безопасности 	**Контроль приложений** Контроль приложений управляет запуском приложений на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании приложений. Также Контроль приложений снижает риск заражения компьютера, ограничивая доступ к приложениям. **Контроль устройств** Контроль устройств управляет доступом пользователей к установленным или подключенным к компьютеру устройствам (например, жестким дискам, камере или модулю Wi-Fi). Это позволяет защитить компьютер от заражения при подключении этих устройств и предотвратить потерю или утечку данных. **Веб-Контроль** Веб-Контроль управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени. При попытке пользователя открыть веб-сайт, доступ к которому ограничен Веб-Контролем, Kaspersky Endpoint Security заблокирует доступ или покажет предупреждение. **Адаптивный контроль аномалий** Компонент Адаптивный контроль аномалий отслеживает и блокирует действия, нехарактерные для компьютеров сети организации. Для отслеживания нехарактерных действий Адаптивный контроль аномалий использует набор правил (например, правило *Запуск Windows PowerShell из офисного приложения*). Правила созданы специалистами "Лаборатории Касперского" на основе типичных сценариев вредоносной активности. Вы можете выбрать поведение Адаптивного контроля аномалий для каждого из правил и, например, разрешить запуск PowerShell-скриптов для автоматизации решения корпоративных задач. Kaspersky Endpoint Security обновляет набор правил с базами приложения. **Анализ журналов** Анализ журналов контролирует целостность защищаемой среды на основе журналов событий Windows. При обнаружении признаков нетипичного поведения в системе приложение информирует администратора, так как это поведение может указывать на попытки кибератак. **Контроль целостности системы** Контроль целостности системы отслеживает изменения в операционной системе, которые могут указывать на нарушения безопасности компьютера. Обнаружив такие изменения, Kaspersky Endpoint Security формирует соответствующие события и предупреждает администратора.
Задачи 	**Поиск вредоносного ПО** Kaspersky Endpoint Security выполняет проверку компьютера на присутствие вирусов и других приложений, представляющих угрозу. Поиск вредоносного ПО позволяет исключить возможность распространения вредоносных приложений, которые не были обнаружены компонентами, например, из-за установленного низкого уровня защиты. **Обновление баз и модулей приложения** Kaspersky Endpoint Security загружает обновленные базы и модули приложения. Это обеспечивает актуальность защиты компьютера от вирусов и других приложений, представляющих угрозу. По умолчанию приложение обновляется автоматически, но при необходимости вы можете вручную обновить базы и модули приложения. **Откат последнего обновления** Kaspersky Endpoint Security отменяет последнее обновление баз и модулей. Это позволяет вернуться к использованию предыдущих баз и модулей приложения при необходимости, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасное приложение. **Проверка целостности приложения** Kaspersky Endpoint Security проверяет модули приложения, находящиеся в папке установки приложения, на наличие повреждений или изменений. Если модуль приложения имеет некорректную цифровую подпись, то такой модуль считается поврежденным.
Шифрование данных 	**Шифрование файлов** Компонент позволяет создавать правила шифрования файлов. Вы можете выбрать для шифрования стандартные папки, выбрать папку вручную или выбрать отдельные файлы по расширению. **Полнодисковое шифрование** Компонент позволяет зашифровать диск с помощью следующих технологий: Шифрование диска Kaspersky или Шифрование диска BitLocker. **Шифрование съемных дисков** Компонент позволяет защитить данные на съемных дисках. Вы можете использовать следующие виды шифрования: полнодисковое шифрование (FDE) и шифрование файлов (FLE).

Раздел	Компонент
Detection and Response 	**Endpoint Detection and Response Optimum** Встроенный агент для работы решения Kaspersky Endpoint Detection and Response Optimum (далее также "EDR Optimum"). *Решение Kaspersky Endpoint Detection and Response* – решение, предназначенное для защиты IT-инфраструктуры организации от сложных кибернетических угроз. Функционал решения сочетает автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для противодействия сложным атакам, в том числе новым эксплойтам (exploits), программам-вымогателям (ransomware), бесфайловым атакам (fileless attacks), а также методам, использующим законные системные инструменты. Подробнее о решении см. в справке Kaspersky Endpoint Detection and Response Optimum. **Endpoint Detection and Response Expert** Встроенный агент для работы решения Kaspersky Endpoint Detection and Response Expert (далее также "EDR Expert"). EDR Expert предлагает пользователю больше функций для мониторинга и реагирования на угрозы информационной безопасности, чем EDR Optimum. Подробнее о решении см. в справке Kaspersky Endpoint Detection and Response Expert. **Endpoint Detection and Response Expert (on-premises)** и **Network Detection and Response (KATA)** Встроенные агенты для работы компонентов Endpoint Detection and Response и Network Detection and Response, которые входят в состав решения Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* – решение, предназначенное для своевременного обнаружения сложных угроз, таких как целевые атаки, сложные постоянные угрозы (англ. Advanced Persistent Threat, APT), атаки "нулевого дня" и другие. Kaspersky Anti Targeted Attack Platform включает в себя три функциональных блока: • Kaspersky Anti Targeted Attack (далее также "*KATA*"); • Kaspersky Endpoint Detection and Response (далее также "*EDR (KATA)*"); • Network Detection and Response (далее также "*NDR (KATA)*"). Вы можете приобрести все функциональные блоки или приобрести функциональные блоки по отдельности. Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform. **Sandbox** Встроенный агент для работы Sandbox. *Sandbox* обнаруживает и автоматически блокирует сложные угрозы на компьютерах. Sandbox анализирует поведение объектов для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации. Sandbox выполняет анализ и проверку объектов на специальных серверах с развернутыми виртуальными образами операционных систем Microsoft Windows (серверы Sandbox). Подробнее о решении см. в справке Kaspersky Sandbox и справке Kaspersky Anti Targeted Attack Platform. **Managed Detection and Response** Встроенный агент для работы решения Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* – решение, которое автоматически обнаруживает и анализирует инциденты безопасности в вашей инфраструктуре. Для этого MDR использует данные телеметрии, полученные от конечных точек, и машинное обучение. Данные об инцидентах MDR передает экспертам "Лаборатории Касперского". Далее эксперты могут самостоятельно обработать инцидент и, например, добавить новую запись в антивирусные базы. Или эксперты могут дать рекомендации по обработке инцидента и, например, предложить изолировать компьютер от сети. Подробную информацию о работе решения см. в справке Kaspersky Managed Detection and Response.

Режимы работы приложения: Стандартный, EDR-агент, Легкий агент

Kaspersky Endpoint Security для Windows входит в состав многих решений от "Лаборатории Касперского". В зависимости от решения вам нужно выбрать режим работы приложения.



Стандартный режим

Это основной режим работы приложения и режим работы по умолчанию. Вы можете установить приложение в этом режиме в составе EPP-решений от "Лаборатории Касперского" (Endpoint Protection Platform). Например, Kaspersky Endpoint Security в стандартном режиме входит в состав решения Kaspersky Endpoint Security для бизнеса. Kaspersky Endpoint Security обеспечивает комплексную защиту рабочих станций и серверов от различного вида угроз, сетевых и мошеннических атак. Также в стандартном режиме доступны встроенные агенты для взаимодействия с решениями Detection and Response от "Лаборатории Касперского": EDR, MDR, KUMA и другие.



EDR-агент

Этот режим позволяет развернуть решения Detection and Response от "Лаборатории Касперского" совместно с EPP-решениями от сторонних поставщиков. К Detection and Response решениям относятся Kaspersky Managed Detection and Response (MDR) и Kaspersky Anti Targeted Attack Platform (KATA). Также EDR-агент поддерживает работу с SIEM-решением от "Лаборатории Касперского" – *Kaspersky Unified Monitoring and Analysis Platform (KUMA)*.

В этом режиме недоступны стандартные компоненты защиты, например, Защита от файловых угроз или Защита от веб-угроз. Стандартную защиту компьютера обеспечивает EPP-решение от стороннего поставщика. EDR-агент осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами и взаимодействует с решениями Detection and Response.



Легкий агент

Это режим защиты виртуальных сред. Kaspersky Endpoint Security в режиме Легкого агента входит в состав решения Kaspersky Security для виртуальных и облачных сред. Легкий агент обеспечивает защиту виртуальных машин с гостевыми операционными системами для рабочих станций и серверов. В этом режиме доступны те же компоненты защиты и контроля, что и для стандартного режима. Отличие заключается в том, что проверку объектов на наличие вирусов и других вредоносных приложений выполняет специальный компонент решения, установленный на отдельную виртуальную машину – SVM (Secure Virtual Machine). Таким образом, Легкий агент использует ресурсы SVM для обеспечения безопасности инфраструктуры, а не ресурсы виртуальной машины.

Комплект поставки

Комплект поставки содержит следующие дистрибутивы:

- **AES256**

  Дистрибутив предназначен для установки на компьютеры с x86/x64-архитектурой. Дистрибутив содержит криптографические средства, реализующие криптографический алгоритм AES (Advanced Encryption Standard) с эффективной длиной ключа 256 бит.

- **AES56**

  Дистрибутив предназначен для установки на компьютеры с x86/x64-архитектурой. Дистрибутив содержит криптографические средства, реализующие криптографический алгоритм AES с эффективной длиной ключа 56 бит.

- **Arm64**

  Дистрибутив предназначен для установки на компьютеры с Arm-архитектурой. Дистрибутив не предназначен для установки на серверы.

Перед установкой убедитесь, что дистрибутив соответствует архитектуре процессора компьютера. Если дистрибутив не соответствует архитектуре процессора, инсталлятор завершит установку с ошибкой.

Дистрибутив представляет собой самораспаковывающийся архив в формате EXE. Для просмотра содержания дистрибутива вам нужно распаковать архив в отдельную папку. Каждый дистрибутив содержит следующие файлы:

Комплект поставки

Файл	Описание
`kes_win.msi`	Пакет установки Kaspersky Endpoint Security.
`setup_kes.exe`	Файлы, необходимые для установки приложения всеми доступными способами.
`kes_win.kud`	Файл для создания инсталляционного пакета Kaspersky Endpoint Security.
`klcfginst.msi`	Пакет установки плагина управления приложением в Консоли администрирования Kaspersky Security Center.
`bases.cab`	Файлы пакетов обновлений, которые используются при установке приложения.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Файлы для удаления несовместимого программного обеспечения.
`incompatible.txt`	Файл со списком ПО, с которым у приложения Kaspersky Endpoint Security могут быть проблемы совместимости. "Лаборатория Касперского" не гарантирует совместимость приложения Kaspersky Endpoint Security с приложениями из списка.
`ksn_<language ID>.txt`	Файл, с помощью которого вы можете ознакомиться с условиями участия в Kaspersky Security Network.
`license.txt`	Файл, с помощью которого вы можете ознакомиться с Лицензионным соглашением и Политикой конфиденциальности.
`installer.ini`	Файл, содержащий внутренние параметры дистрибутива.
`kes.cab`	Файлы для работы графического интерфейса программы.

`aes256.cab` / `aes56.cab`	Файлы для работы криптографического алгоритма AES (не входят в состав дистрибутива Arm64).
`package.kcat`	Файл с подписями дистрибутива приложения. Цифровая подпись обеспечивает подлинность и целостность дистрибутива приложения.

Не рекомендуется изменять значения этих параметров. Если вы хотите изменить параметры установки, используйте файл setup.ini.

Аппаратные и программные требования

В этой статье указаны версии программного обеспечения, на которых приложение было протестировано и для которых гарантируется его корректная работа. Приложение также может работать с другими версиями программного обеспечения, но такие конфигурации не проходили полного цикла тестирования и не входят в список гарантированно поддерживаемых.

Для функционирования Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Для установки приложения необходимо владеть правами администратора на компьютере.

Минимальные общие требования

Минимальные требования	Рабочая станция (x86/x64)	Сервер (x86/x64)	Arm
Хранилище	2 ГБ	2 ГБ	2 ГБ
Процессор	1 ГГц, поддержка инструкций SSE2	1.4 ГГц, поддержка инструкций SSE2	1 ГГц, архитектура Armv8.1
Оперативная память	рабочая станция (x86) – 1 ГБ рабочая станция (x64) – 2 ГБ	2 ГБ Примечание: на сервере для установки приложения со встроенным агентом для интеграции с Kaspersky Anti Targeted Attack Platform необходимо 8 ГБ.	4 ГБ
Microsoft .NET Framework	4 или выше	4 или выше	4.8 или выше

Рабочие станции

Поддерживаемые операционные системы для рабочих станций:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise / Enterprise multi-session;

- Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise / Enterprise multi-session;
- Windows 11 для Arm64 Home / Pro / Pro для рабочих станций / Education / Enterprise.

Операционные системы Windows, начиная с версии 11 24H2, поддерживают технологию UDP Receive Segment Coalescing Offload (URO). Технология включена по умолчанию, если на компьютере установлены совместимая сетевая карта и драйверы. Отключение URO на компьютере пользователя может значительно снизить производительность приложения.

Для корректной работы Kaspersky Endpoint Security на компьютере пользователя должна быть запущена служба Windows Security Center (wscsvc).

Приложение Kaspersky Endpoint Security не может быть установлено на Microsoft Windows 7, если не установлены обновления операционной системы KB4490628 (обновление от 12 марта 2019) и KB4474419 (обновление от 23 сентября 2019). Подробнее см. в базе знаний Службы технической поддержки.

Особенности поддержки операционной системы Microsoft Windows 10 вы можете узнать в базе знаний Службы технической поддержки.

Особенности поддержки операционной системы Microsoft Windows 11 вы можете узнать в базе знаний Службы технической поддержки.

Серверы

Kaspersky Endpoint Security поддерживает работу основных компонентов приложения на компьютерах под управлением операционной системы Windows для серверов. Вы можете использовать Kaspersky Endpoint Security для Windows вместо Kaspersky Security для Windows Server на серверах и кластерах организации (англ. Cluster Mode). Также приложение поддерживает режим основных серверных компонентов (англ. Server Core Mode) (см. известные ограничения).

Поддерживаемые операционные системы для серверов:

- Windows Small Business Server 2011 Essentials / Standard (64-разрядная);

  Windows Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2.

- Windows MultiPoint Server 2011 (64-разрядная);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1;
- Windows Web Server 2008 R2 Service Pack 1;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);

- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2016 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая режим Server Core);
- Windows Server 2025 Standard / Datacenter.

Приложение Kaspersky Endpoint Security не может быть установлено на Microsoft Windows Server 2008 R2, если не установлены обновления операционной системы KB4490628 (обновление от 12 марта 2019) и KB4474419 (обновление от 23 сентября 2019).

Особенности поддержки операционной системы Microsoft Windows Server 2016 и Microsoft Windows Server 2019 вы можете узнать в базе знаний Службы технической поддержки.

Особенности поддержки операционной системы Microsoft Windows Server 2022 вы можете узнать в базе знаний Службы технической поддержки.

Неподдерживаемые операционные системы для серверов:

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2;
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2;
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2;
- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2;
- Windows Small Business Server 2008 Standard / Premium Service Pack 2.

Виртуальные платформы

Поддерживаемые виртуальные платформы для работы приложения в стандартном режиме:

- VMware Workstation Pro 26H1u1;
- VMware ESXi 8.0 Update 3k;
- Windows Server 2025;
- Citrix Virtual Apps and Desktops 7 2607 LTSR;
- Citrix Provisioning 2607 LTSR;
- XenServer 8.4.

Приложение поддерживает работу на виртуальных машинах с Windows 11 Pro Arm64, созданных с использованием Hyper-V.

Виртуальные машины для установки Легкого агента

Установка Kaspersky Endpoint Security в режиме Легкого агента на виртуальные машины с Arm-архитектурой не поддерживается.

BIOS на виртуальных машинах должен поддерживать спецификацию SMBIOS версии 2.1 или выше.

На виртуальных машинах должны быть установлены следующие пакеты и утилиты:

- При использовании Microsoft Hyper-V – пакет служб интеграции (Integration Services).
- При использовании VMware vSphere – пакет VMware Tools.
- При использовании XenServer – пакет XenTools.
- При использовании HUAWEI FusionSphere – пакет HUAWEI Tools.
- При использовании гипервизоров на базе KVM – QEMU Guest Agent.

Требования к виртуальной инфраструктуре для работы приложения в режиме Легкого агента см. в справке Kaspersky Security для виртуальных сред Легкий агент.

Для корректной работы приложения необходимо использовать виртуализированный сетевой интерфейс с полосой пропускания не менее 100 Мбит/сек.

Терминальные серверы

Поддерживаемые типы терминальных серверов:

- Microsoft Remote Desktop Services на базе Windows Server 2008 R2 SP1;
- Microsoft Remote Desktop Services на базе Windows Server 2012;
- Microsoft Remote Desktop Services на базе Windows Server 2012 R2;
- Microsoft Remote Desktop Services на базе Windows Server 2016;
- Microsoft Remote Desktop Services на базе Windows Server 2019;
- Microsoft Remote Desktop Services на базе Windows Server 2022;
- Microsoft Remote Desktop Services на базе Windows Server 2025;
- Citrix RDSH из состава Citrix Virtual Apps and Desktops 7 2507 LTSR.

Поддержка Kaspersky Security Center

Kaspersky Endpoint Security поддерживает работу со следующими версиями Kaspersky Security Center:

- Kaspersky Security Center 14.2;
- Kaspersky Security Center Linux 14.2;
- Kaspersky Security Center Linux 15;
- Kaspersky Security Center Windows 15.1;
- Kaspersky Security Center Linux 15.1;
- Kaspersky Security Center Linux 15.2;
- Kaspersky Security Center Linux 15.3;
- Kaspersky Security Center Linux 15.4;
- Kaspersky Security Center Linux 16;
- Kaspersky Security Center Linux 16.1;
- Kaspersky Security Center Linux 16.2;
- Kaspersky Security Center Linux 16.3;
- Kaspersky Security Center Linux 17.

Сравнение функций приложения в зависимости от типа операционной системы

Набор доступных функций Kaspersky Endpoint Security зависит от типа операционной системы: рабочая станция или сервер (см. таблицу ниже).

Начиная с версии Kaspersky Endpoint Security для Windows 12.8 добавлена возможность настраивать разные наборы компонентов для разных типов операционных систем в инсталляционном пакете. То есть вы можете разворачивать приложение на рабочие станции и серверы с помощью одного инсталляционного пакета.

Установка Kaspersky Endpoint Security в режиме Легкого агента на виртуальные машины с Arm-архитектурой не поддерживается.

Функция	Рабочая станция	Рабочая станция на базе архитектуры Arm	Сервер	Режим Server Core
Продвинутая защита				
Kaspersky Security Network	✓	✓	✓	✓
Анализ поведения	✓	✓	✓	✓
Защита от шифрования	✓	✓	✓	✓
Защита от эксплойтов	✓	✓	✓	✓
Предотвращение вторжений	✓	✓	–	–
Откат вредоносных действий	✓	✓	✓	✓
Базовая защита				
Защита от файловых угроз	✓	✓	✓	✓
Защита от веб-угроз	✓	✓	✓	–
Защита от почтовых угроз	✓	✓	✓	–
Сетевой экран	✓	✓	✓	✓
Защита от сетевых угроз	✓	✓	✓	✓
Защита от атак BadUSB	✓	✓	✓	–
AMSI-защита	✓	✓	✓	✓
Контроль безопасности				
Анализ журналов	–	–	✓	–
Контроль приложений	✓	✓	✓	✓
Контроль устройств	✓	✓	✓	✓
Веб-Контроль	✓	✓	✓	–
Адаптивный контроль аномалий	✓	✓	–	–
Контроль целостности системы	–	–	✓	–
Cloud Discovery	✓	✓	–	–
Удаленный доступ	✓	✓	✓	✓
Шифрование данных				
Шифрование диска Kaspersky	✓	–	–	–
Шифрование диска BitLocker	✓	✓	✓	✓
Шифрование файлов	✓	–	–	–
Шифрование съемных дисков	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	✓	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
Интеграция с KUMA	✓	✓	✓	✓

Сравнение функций приложения в зависимости от инструментов управления

Набор доступных функций Kaspersky Endpoint Security зависит от инструментов управления (см. таблицу ниже).

Вы можете управлять приложением с помощью следующих консолей Kaspersky Security Center:

- Консоль администрирования. Оснастка к Microsoft Management Console (MMC), которая устанавливается на рабочее место администратора.
- Web Console. Компонент Kaspersky Security Center, который устанавливается на Сервер администрирования. Вы можете работать в Web Console через браузер на любом компьютере.

Вы также можете управлять приложением с помощью Kaspersky Security Center Cloud Console. *Kaspersky Security Center Cloud Console* – это облачная версия Kaspersky Security Center. То есть, Сервер администрирования и другие компоненты Kaspersky Security Center установлены в облачной инфраструктуре "Лаборатории Касперского". Подробнее об управлении приложением с помощью Kaspersky Security Center Cloud Console см. в справке Kaspersky Security Center Cloud Console.

Kaspersky Endpoint Security входит в состав решения Kaspersky Next Pro View. Подробнее о доступных функциях приложения в составе этого решения см. в справке Kaspersky Next.

Сравнение функций Kaspersky Endpoint Security

Функция	Kaspersky Security Center		Kaspersky Security Center
	Консоль администрирования	Web Console	Cloud Console
Продвинутая защита			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Анализ поведения	✓	✓	✓
Защита от шифрования			
Защита от эксплойтов	✓	✓	✓
Предотвращение вторжений	✓	✓	✓
Откат вредоносных действий	✓	✓	✓
Базовая защита			
Защита от файловых угроз	✓	✓	✓
Защита от веб-угроз	✓	✓	✓
Защита от почтовых угроз	✓	✓	✓
Сетевой экран	✓	✓	✓
Защита от сетевых угроз	✓	✓	✓
Защита от атак BadUSB	✓	✓	✓
AMSI-защита	✓	✓	✓
Контроль безопасности			

Функция	Kaspersky Security Center		Kaspersky Security Center
	Консоль администрирования	Web Console	Cloud Console
Анализ журналов	✓	✓	✓
Контроль приложений	✓	✓	✓
Контроль устройств	✓	✓	✓
Веб-Контроль	✓	✓	✓
Адаптивный контроль аномалий	✓	✓	✓
Контроль целостности системы	✓	✓	✓
Cloud Discovery	–	–	✓
Удаленный доступ	✓	✓	✓
Шифрование данных			
Шифрование диска Kaspersky	✓	✓	–
Шифрование диска BitLocker	✓	✓	✓
Шифрование файлов	✓	✓	–
Шифрование съемных дисков	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
Интеграция с KUMA	✓	✓	✓
Задачи			
Добавление ключа	✓	✓	✓
Изменение состава компонентов приложения	✓	✓	✓
Инвентаризация	✓	✓	✓
Обновление	✓	✓	✓
Откат обновления	✓	✓	✓
Поиск вредоносного ПО	✓	✓	✓
Проверка целостности приложения	✓	✓	–
Удаление данных	✓	✓	✓
Управление учетными записями Агента аутентификации (Шифрование диска Kaspersky)	✓	✓	–
Поиск IOC (EDR)	–	✓	✓
Помещение файла на карантин (EDR)	–	✓	✓
Получение файла (EDR)	–	✓	✓
Удаление файла (EDR)	–	✓	✓
Запуск процесса (EDR)	–	✓	✓
Завершение процесса (EDR)	–	✓	✓

Совместимость с другими приложениями

Приложение Kaspersky Endpoint Security несовместимо с некоторыми приложениями "Лаборатории Касперского", а также приложениями от сторонних поставщиков. Поэтому Kaspersky Endpoint Security проверяет компьютер на наличие таких приложений перед установкой, обновлением версии приложения и изменением состава компонентов.

Совместимость с сторонними приложениями

Приложение Kaspersky Endpoint Security несовместимо с приложениями, которые входят в состав систем защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков. Также Kaspersky Endpoint Security может иметь проблемы совместимости с другими приложениями. Для проверки совместимости Kaspersky Endpoint Security использует список ПО, составленный в "Лаборатории Касперского". Этот список сформирован в файле incompatible.txt. Файл добавлен в комплект поставки.

"Лаборатория Касперского" не гарантирует совместимость приложения Kaspersky Endpoint Security с приложениями из списка. При обнаружении приложения из списка установщик останавливает развертывание Kaspersky Endpoint Security. Некоторые приложения из списка установщик может удалить автоматически. Если несмотря на риски вам нужно установить приложение Kaspersky Endpoint Security и приложение из списка на один компьютер, вы можете пропустить проверку компьютера (см. инструкцию ниже).



ЗАГРУЗИТЬ ФАЙЛ INCOMPATIBLE.TXT

Совместимость с приложениям "Лаборатории Касперского"

Приложение Kaspersky Endpoint Security несовместимо со следующими приложениями "Лаборатории Касперского":

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.

- Endpoint Sensor в составе решений Kaspersky Anti Targeted Attack Platform и Kaspersky Endpoint Detection and Response.
- Kaspersky Endpoint Agent в составе решений Detection and Response от "Лаборатории Касперского".

  "Лаборатория Касперского" переводит все решения Detection and Response на работу со встроенным агентом Kaspersky Endpoint Security вместо Kaspersky Endpoint Agent. Начиная с версии 12.1 приложение поддерживает работу со всеми решениями Detection and Response.

- Kaspersky Security для виртуальных сред Легкий агент.
- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security для Windows Server.

  Начиная с Kaspersky Endpoint Security версии 12.0 вы можете мигрировать с Kaspersky Security для Windows Server на Kaspersky Endpoint Security для Windows и использовать единое решение для защиты рабочих станций и серверов.

- Kaspersky Embedded Systems Security.

Если на компьютере установлены приложения "Лаборатории Касперского" из списка, Kaspersky Endpoint Security удаляет эти приложения. Дождитесь завершения этого процесса, чтобы продолжить установку Kaspersky Endpoint Security.

Пропуск проверки на наличие ПО, с которым могут быть проблемы совместимости

Если Kaspersky Endpoint Security обнаружил на компьютере приложение из списка incompatible.txt, установка приложения будет прекращена. Для продолжения установки вам нужно удалить это приложение. Но, если поставщик стороннего ПО указал в своей документации совместимость с системами защиты конечных устройств (англ. Endpoint Protection Platform, EPP), вы можете установить Kaspersky Endpoint Security на компьютер с приложением этого поставщика. Например, поставщик решения Endpoint Detection and Response (EDR) может заявить совместимость со сторонними EPP-системами. В этом случае вам нужно запустить установку Kaspersky Endpoint Security без проверки установленного ПО. Для этого вам нужно передать в установщик следующие параметры:

- `SKIPPRODUCTCHECK=1`. Выключение проверки установленного ПО. Список ПО, с которым могут быть проблемы совместимости, приведен в файле incompatible.txt в комплекте поставки. Если параметр не задан, при обнаружении приложения из списка установка Kaspersky Endpoint Security будет прекращена.
- `SKIPPRODUCTUNINSTALL=1`. Запрет на автоматическое удаление найденных приложений из списка incompatible.txt. Если параметр не задан, Kaspersky Endpoint Security пытается удалить приложения, с которыми могут быть проблемы совместимости.
- `CLEANERSIGNCHECK=0`. Выключение проверки цифровой подписи обнаруженных при проверке приложений. Если параметр не задан, то при развертывании приложения через Kaspersky Security Center проверка цифровой подписи выключена. При локальной установке приложения проверка цифровой подписи включена по умолчанию.

Вы можете передать параметры в командной строке при локальной установке приложения.

Если во время установки приложения вы пропустили проверку на наличие ПО, с которым могут быть проблемы совместимости, Kaspersky Endpoint Security может выполнить эту проверку повторно при изменении состава компонентов приложения. Для пропуска проверки установленного ПО вам нужно настроить задачу *Изменение состава компонентов приложения*.

Пример

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

Для дистанционной установки Kaspersky Endpoint Security вам нужно добавить параметры в файл для создания инсталляционного пакета `kes_win.kud` в разделе `[Setup]` (см. ниже). Файл `kes_win.kud` входит в комплект поставки.

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

Установка и удаление приложения

Приложение Kaspersky Endpoint Security может быть установлено на компьютер следующими способами:

- Локально с помощью мастера установки приложения.
- Локально из командной строки.
- Удаленно с помощью Kaspersky Security Center.
- Удаленно через редактор управления групповыми политиками Microsoft Windows (подробнее см. на сайте Службы технической поддержки Microsoft).
- Удаленно с помощью System Center Configuration Manager.

Вы можете настроить параметры установки приложения несколькими способами. Если вы одновременно используете несколько способов настройки параметров, Kaspersky Endpoint Security применяет параметры с наивысшим приоритетом. Kaspersky Endpoint Security использует следующий порядок приоритетов:

1. Параметры, полученные из файла setup.ini.
2. Параметры, полученные из файла installer.ini.
3. Параметры, полученные из командной строки.
4. Параметры, полученные из конфигурационного файла (install.cfg).

Перед началом установки Kaspersky Endpoint Security (в том числе удаленной) рекомендуется закрыть все работающие приложения.

При установке Kaspersky Endpoint Security операционная система может показывать собственные сообщения. Также при установке приложения возможны прерывания подключения к сети и Интернету.

При установке, обновлении или удалении Kaspersky Endpoint Security могут возникать ошибки. Подробнее об их решении этих ошибок см. в базе знаний Службы технической поддержки.

Развертывание через Kaspersky Security Center

Kaspersky Endpoint Security можно разворачивать на компьютерах в сети организации несколькими способами. Вы можете выбрать наиболее подходящий для вашей организации способ развертывания, а также использовать несколько способов развертывания одновременно. Перед установкой приложения на компьютере должен быть установлен Агент администрирования Kaspersky Security Center. *Агент администрирования* обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером.

Kaspersky Security Center поддерживает следующие основные способы развертывания:

- Установка приложения с помощью мастера развертывания защиты.

  Стандартный способ установки, который удобен, если вас удовлетворяют параметры Kaspersky Endpoint Security по умолчанию и в вашей организации простая инфраструктура, которая не требует специальной настройки.

- Установка приложения с помощью задачи удаленной установки.

  Универсальный способ установки, который позволяет настроить параметры Kaspersky Endpoint Security и гибко управлять задачами удаленной установки. Установка Kaspersky Endpoint Security состоит из следующих этапов:

  1. создание инсталляционного пакета;
  2. создание задачи удаленной установки.

Kaspersky Security Center также поддерживает другие способы установки Kaspersky Endpoint Security, например, развертывание в составе образа операционной системы. Подробнее о других способах развертывания см. в справке Kaspersky Security Center.

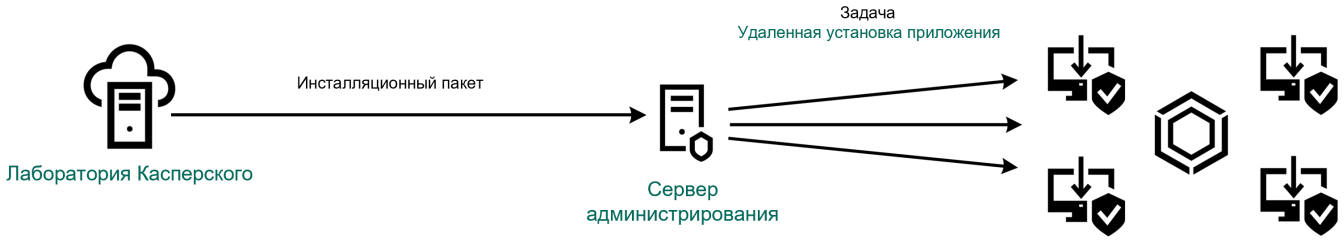
Стандартная установка приложения

Для установки приложения на компьютерах организации в Kaspersky Security Center предусмотрен мастер развертывания защиты. Мастер развертывания защиты включает в себя следующие основные действия:

1. Выбор инсталляционного пакета Kaspersky Endpoint Security.

   Инсталляционный пакет – набор файлов, формируемый для удаленной установки приложения "Лаборатории Касперского" при помощи Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки приложения и обеспечения ее работоспособности сразу после установки. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива приложения. Инсталляционный пакет Kaspersky Endpoint Security общий для всех поддерживаемых версий операционной системы Windows и типов архитектуры процессора.

2. Создание задачи Сервера администрирования Kaspersky Security Center *Удаленная установка приложения*.



Развертывание Kaspersky Endpoint Security

Как запустить мастер развертывания защиты в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно** → **Удаленная установка**.
3. Нажмите на ссылку **Развернуть инсталляционный пакет на управляемые устройства (рабочие места)**.

В результате запустится мастер развертывания защиты. Следуйте его указаниям.

На клиентском компьютере необходимо открыть порты TCP 139 и 445, UDP 137 и 138.

Шаг 1. Выбор инсталляционного пакета

В списке инсталляционных пакетов выберите пакет Kaspersky Endpoint Security. Если в списке отсутствует инсталляционный пакет Kaspersky Endpoint Security, вы можете создать пакет в мастере.

Вы можете настроить параметры инсталляционного пакета в Kaspersky Security Center, например, выбрать компоненты приложения, которые будут установлены на компьютер.

Также с Kaspersky Endpoint Security будет установлен Агент администрирования. *Агент администрирования* обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

Шаг 2. Выбор источника инсталляционного пакета

Выберите источник **Развернуть пакет Kaspersky Security Center**.

Шаг 3. Выбор устройств для установки

Выберите компьютеры, на которые будет установлено приложение Kaspersky Endpoint Security. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. На нераспределенных устройствах не установлен Агент администрирования. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Определение параметров задачи удаленной установки

Настройте следующие дополнительные параметры приложения:

- **Принудительно скачать инсталляционный пакет**. Выберите средства установки приложения:

  - **С помощью Агента администрирования**. Доставку инсталляционного пакета Kaspersky Endpoint Security на клиентские компьютеры выполняет Агент администрирования. Если Агент администрирования не установлен, выполнение задачи завершится ошибкой. В этом случае вам нужно добавить инсталляционный пакет Агента администрирования в задачу *Удаленная установка приложения* и включить доставку файлов средствами операционной системы. Тогда Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security устанавливается средствами Агента администрирования.

  - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.

  - **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

- **Поведение устройств, управляемых другими Серверами администрирования**. Выберите способ установки Kaspersky Endpoint Security. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одного и того же приложения на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

- **Не устанавливать приложение, если оно уже установлено**. Снимите этот флажок, если вы хотите, например, установить приложение более ранней версии.

- **Назначить установку Агента администрирования в групповых политиках Active Directory**. Установка Агента администрирования средствами Active Directory вручную. Для установки Агента администрирования задача удаленной установки должна быть запущена с правами администратора домена.

Шаг 5. Выбор лицензионного ключа

Добавьте ключ в инсталляционный пакет для активации приложения. Этот шаг не является обязательным. Если на Сервере администрирования размещен лицензионный ключ с функцией автоматического распространения, ключ будет добавлен автоматически позднее. Также вы можете активировать приложение позднее с помощью задачи *Добавление ключа*.

Шаг 6. Выбор параметра перезагрузки операционной системы

Выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера. При установке Kaspersky Endpoint Security перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые приложения. Также перезагрузка может потребоваться при обновлении версии приложения.

Шаг 7. Удаление несовместимых приложений перед установкой приложения

Ознакомьтесь со списком несовместимых приложений и разрешите удаление этих приложений. Если на компьютере установлены несовместимые приложения, установка Kaspersky Endpoint Security завершается с ошибкой.

Шаг 8. Выбор учетной записи для доступа к устройствам

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки Kaspersky Endpoint Security средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 9. Запуск установки

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как запустить мастер развертывания защиты в Web Console

В главном окне Web Console выберите **Обнаружение устройств и развертывание → Развертывание и назначение → Мастер развертывания защиты**.

В результате запустится мастер развертывания защиты. Следуйте его указаниям.

На клиентском компьютере необходимо открыть порты TCP 139 и 445, UDP 137 и 138.

Шаг 1. Выбор инсталляционного пакета

В списке инсталляционных пакетов выберите пакет Kaspersky Endpoint Security. Если в списке отсутствует инсталляционный пакет Kaspersky Endpoint Security, вы можете создать пакет в мастере. Для создания инсталляционного пакета вам не нужно искать дистрибутив и сохранять его в память компьютера. В Kaspersky Security Center доступен список дистрибутивов, размещенных на серверах "Лаборатории Касперского", и создание инсталляционного пакета выполняется автоматически. "Лаборатория Касперского" обновляет список после выпуска новых версий приложений.

Вы можете настроить параметры инсталляционного пакета в Kaspersky Security Center, например, выбрать компоненты приложения, которые будут установлены на компьютер.

Шаг 2. Выбор лицензионного ключа

Добавьте ключ в инсталляционный пакет для активации приложения. Этот шаг не является обязательным. Если на Сервере администрирования размещен лицензионный ключ с функцией автоматического распространения, ключ будет добавлен автоматически позднее. Также вы можете активировать приложение позднее с помощью задачи *Добавление ключа*.

Шаг 3. Выбор Агента администрирования

Выберите версию Агента администрирования, который будет установлен вместе с Kaspersky Endpoint Security. *Агент администрирования* обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

Шаг 4. Выбор устройств для установки

Выберите компьютеры, на которые будет установлено приложение Kaspersky Endpoint Security. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. На нераспределенных устройствах не установлен Агент администрирования. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 5. Настройка дополнительных параметров

Настройте следующие дополнительные параметры приложения:

- **Принудительно загрузить инсталляционный пакет**. Выбор средства установки приложения:
  - **С помощью Агента администрирования**. Доставку инсталляционного пакета Kaspersky Endpoint Security на клиентские компьютеры выполняет Агент администрирования. Если Агент администрирования не установлен, выполнение задачи завершится ошибкой. В этом случае вам нужно добавить инсталляционный пакет Агента администрирования в задачу *Удаленная установка приложения* и включить доставку файлов средствами операционной системы. Тогда Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security устанавливается средствами Агента администрирования.
  - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.
  - **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.
- **Не устанавливать программу, если она уже установлена**. Снимите этот флажок, если вы хотите, например, установить приложение более ранней версии.
- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**. Установка Kaspersky Endpoint Security выполняется средствами Агента администрирования или средствами Active Directory вручную. Для установки Агента администрирования задача удаленной установки должна быть запущена с правами администратора домена.

Шаг 6. Выбор параметра перезагрузки операционной системы

Выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера. При установке Kaspersky Endpoint Security перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые приложения. Также перезагрузка может потребоваться при обновлении версии приложения.

Шаг 7. Удаление несовместимых приложений перед установкой приложения

Ознакомьтесь со списком несовместимых приложений и разрешите удаление этих приложений. Если на компьютере установлены несовместимые приложения, установка Kaspersky Endpoint Security завершается с ошибкой.

Шаг 8. Перемещение в группу администрирования

Выберите группу администрирования, в которую будут перемещены компьютеры после установки Агента администрирования. Перемещение в группу администрирования необходимо для применения политик и групповых задач. Если компьютер уже состоит в любой группе администрирования, то компьютер перемещен не будет. Если вы не выберете группу администрирования, компьютеры будут добавлены в группу **Нераспределенные устройства**.

Шаг 9. Выбор учетной записи для доступа к устройствам

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки Kaspersky Endpoint Security средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 10. Запуск установки

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Создание инсталляционного пакета

Инсталляционный пакет – набор файлов, формируемый для удаленной установки приложения "Лаборатории Касперского" при помощи Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки приложения и обеспечения ее работоспособности сразу после установки. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива приложения. Инсталляционный пакет Kaspersky Endpoint Security общий для всех поддерживаемых версий операционной системы Windows и типов архитектуры процессора.

Как создать инсталляционный пакет в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.

2. Нажмите на кнопку **Создать инсталляционный пакет**.

Запустится мастер создания инсталляционного пакета. Следуйте его указаниям.

Шаг 1. Выбор типа инсталляционного пакета

Выберите вариант **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.

Шаг 2. Определение имени инсталляционного пакета

Введите имя инсталляционного пакета, например, *Kaspersky Endpoint Security для Windows 14.3*.

Шаг 3. Выбор дистрибутива приложения для установки

Нажмите на кнопку **Обзор** и выберите файл `kes_win.kud`, который входит в комплект поставки.

Если требуется, обновите антивирусные базы в инсталляционном пакете с помощью флажка **Скопировать обновления из хранилища в инсталляционный пакет**.

Шаг 4. Лицензионное соглашение и Политика конфиденциальности

Прочитайте и примите условия Лицензионного соглашения и Политики конфиденциальности.

Завершение работы мастера

Инсталляционный пакет будет создан и добавлен в Kaspersky Security Center. С помощью инсталляционного пакета вы можете установить Kaspersky Endpoint Security на компьютеры сети организации или обновить версию приложения.

В параметрах инсталляционного пакета вы можете выбрать компоненты приложения для разных типов операционных систем. То есть инсталляционный пакет включает в себя два набора компонентов: для рабочих станций и для серверов. Установщик перед разворачиванием инсталляционного пакета определяет тип операционной системы и устанавливает только те компоненты приложения, которые вы выбрали для определенного типа операционной системы. Таким образом, вы можете использовать один инсталляционный пакет для рабочих станций и серверов.

Инсталляционный пакет содержит антивирусные базы из хранилища Сервера администрирования. Вы можете обновлять базы в инсталляционном пакете, чтобы уменьшить расход трафика при обновлении баз после установки Kaspersky Endpoint Security.

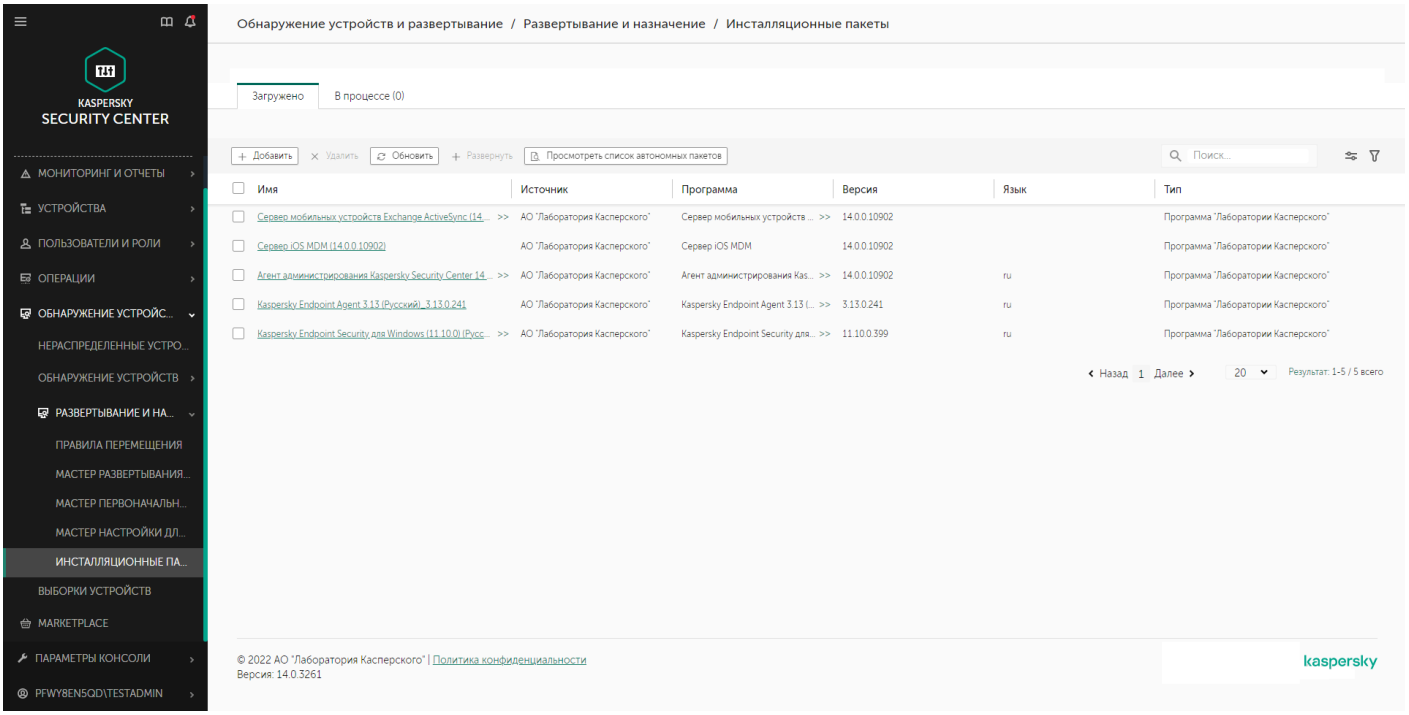
Как создать инсталляционный пакет в Web Console

1. В главном окне Web Console выберите **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания инсталляционного пакета. Следуйте его указаниям.



Список инсталляционных пакетов

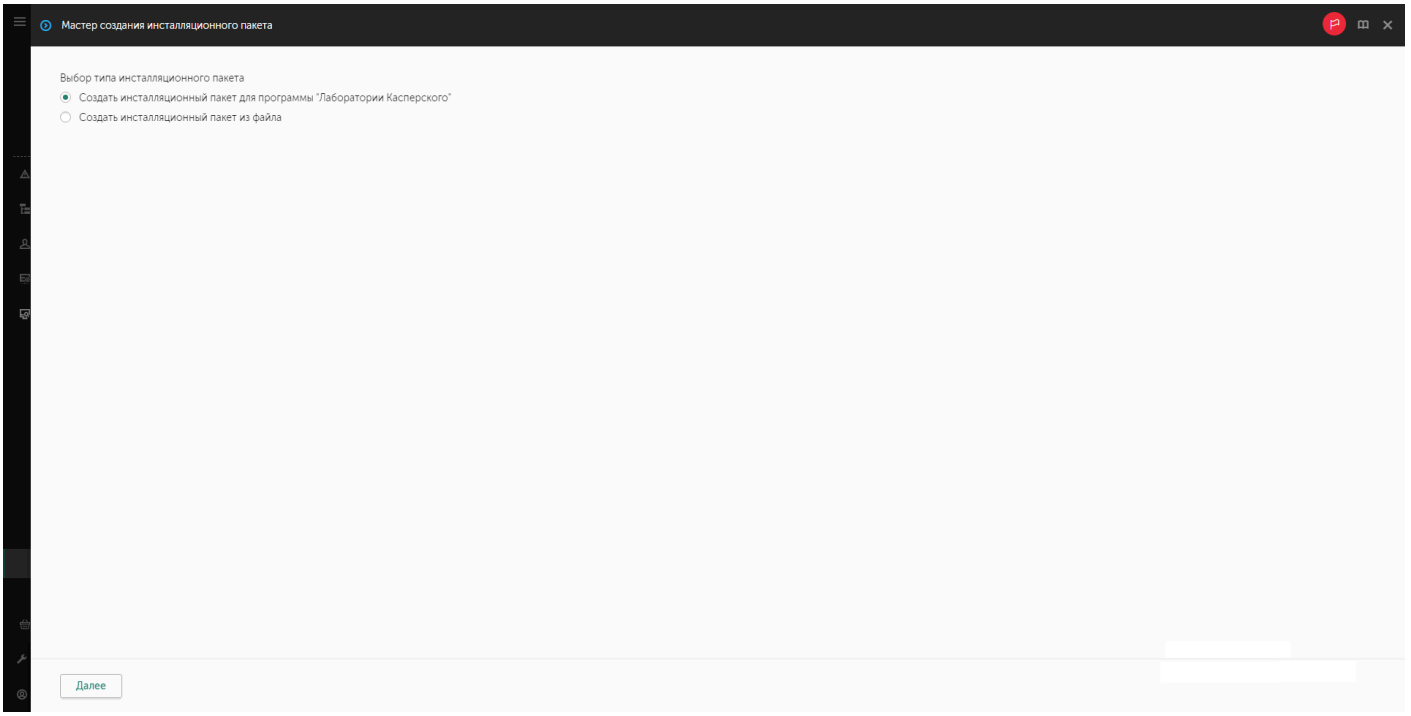
Шаг 1. Выбор типа инсталляционного пакета

Выберите вариант **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.

Мастер создаст инсталляционный пакет из дистрибутива, размещенного на серверах "Лаборатории Касперского". Список обновляется автоматически по мере выпуска новых версий приложений. Для установки Kaspersky Endpoint Security рекомендуется выбрать этот вариант.

Также вы можете создать инсталляционный пакет из файла.

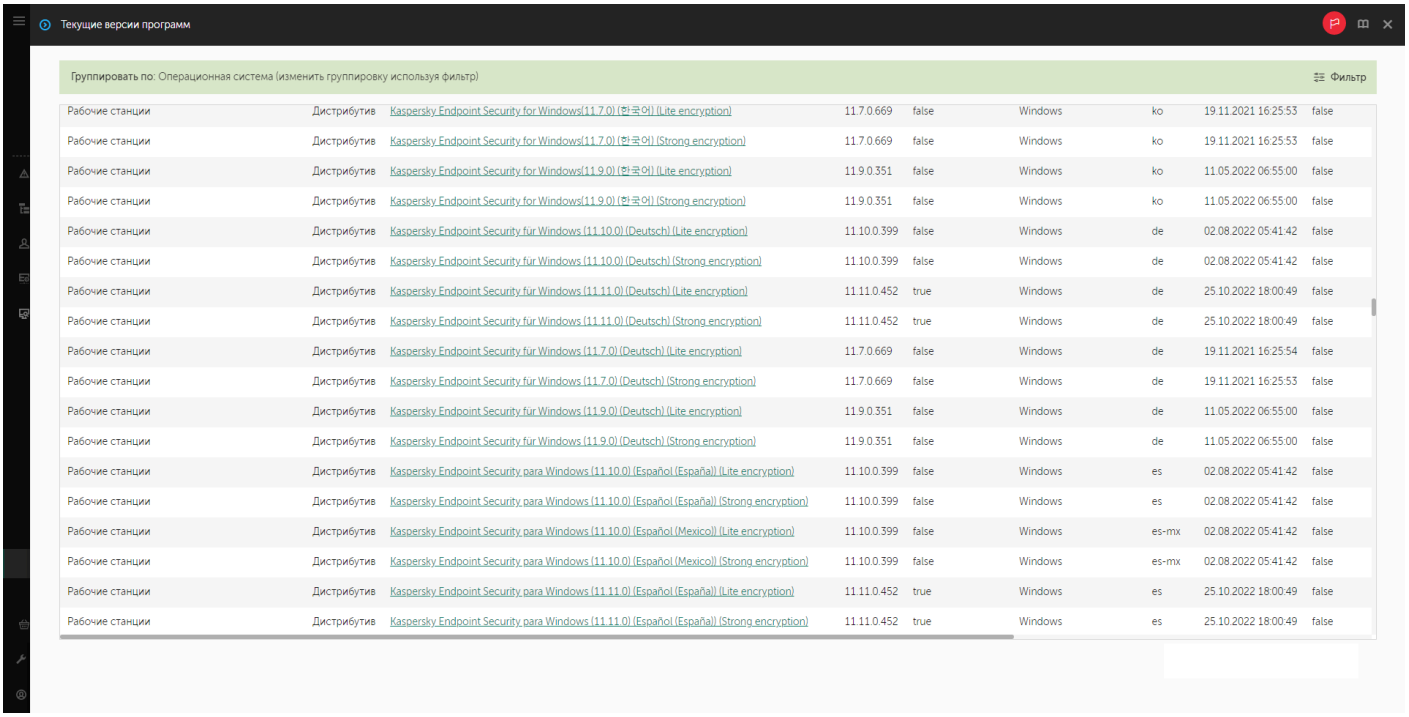
Создание инсталляционного пакета Kaspersky Endpoint Security из файла доступно только в Kaspersky Security Center Web Console.



Типы инсталляционных пакетов

Шаг 2. Инсталляционные пакеты

Выберите инсталляционный пакет Kaspersky Endpoint Security для Windows. Запустится процесс создания инсталляционного пакета. Во время создания инсталляционного пакета необходимо принять условия Лицензионного соглашения и Политики конфиденциальности.



Рабочие станции	Дистрибутив	Kaspersky Endpoint Security for Windows(11.7.0) (한국어) (Lite encryption)	11.7.0.669	false	Windows	ko	19.11.2021 16:25:53	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security for Windows(11.7.0) (한국어) (Strong encryption)	11.7.0.669	false	Windows	ko	19.11.2021 16:25:53	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security for Windows(11.9.0) (한국어) (Lite encryption)	11.9.0.351	false	Windows	ko	11.05.2022 06:55:00	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security for Windows(11.9.0) (한국어) (Strong encryption)	11.9.0.351	false	Windows	ko	11.05.2022 06:55:00	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security für Windows (11.10.0) (Deutsch) (Lite encryption)	11.10.0.399	false	Windows	de	02.08.2022 05:41:42	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security für Windows (11.10.0) (Deutsch) (Strong encryption)	11.10.0.399	false	Windows	de	02.08.2022 05:41:42	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security für Windows (11.11.0) (Deutsch) (Lite encryption)	11.11.0.452	true	Windows	de	25.10.2022 18:00:49	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security für Windows (11.11.0) (Deutsch) (Strong encryption)	11.11.0.452	true	Windows	de	25.10.2022 18:00:49	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security für Windows (11.7.0) (Deutsch) (Lite encryption)	11.7.0.669	false	Windows	de	19.11.2021 16:25:54	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security für Windows (11.7.0) (Deutsch) (Strong encryption)	11.7.0.669	false	Windows	de	19.11.2021 16:25:53	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security für Windows (11.9.0) (Deutsch) (Lite encryption)	11.9.0.351	false	Windows	de	11.05.2022 06:55:00	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security für Windows (11.9.0) (Deutsch) (Strong encryption)	11.9.0.351	false	Windows	de	11.05.2022 06:55:00	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security para Windows (11.10.0) (Español (España)) (Lite encryption)	11.10.0.399	false	Windows	es	02.08.2022 05:41:42	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security para Windows (11.10.0) (Español (España)) (Strong encryption)	11.10.0.399	false	Windows	es	02.08.2022 05:41:42	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security para Windows (11.10.0) (Español (Mexico)) (Lite encryption)	11.10.0.399	false	Windows	es-mx	02.08.2022 05:41:42	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security para Windows (11.10.0) (Español (Mexico)) (Strong encryption)	11.10.0.399	false	Windows	es-mx	02.08.2022 05:41:42	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security para Windows (11.11.0) (Español (España)) (Lite encryption)	11.11.0.452	true	Windows	es	25.10.2022 18:00:49	false
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security para Windows (11.11.0) (Español (España)) (Strong encryption)	11.11.0.452	true	Windows	es	25.10.2022 18:00:49	false

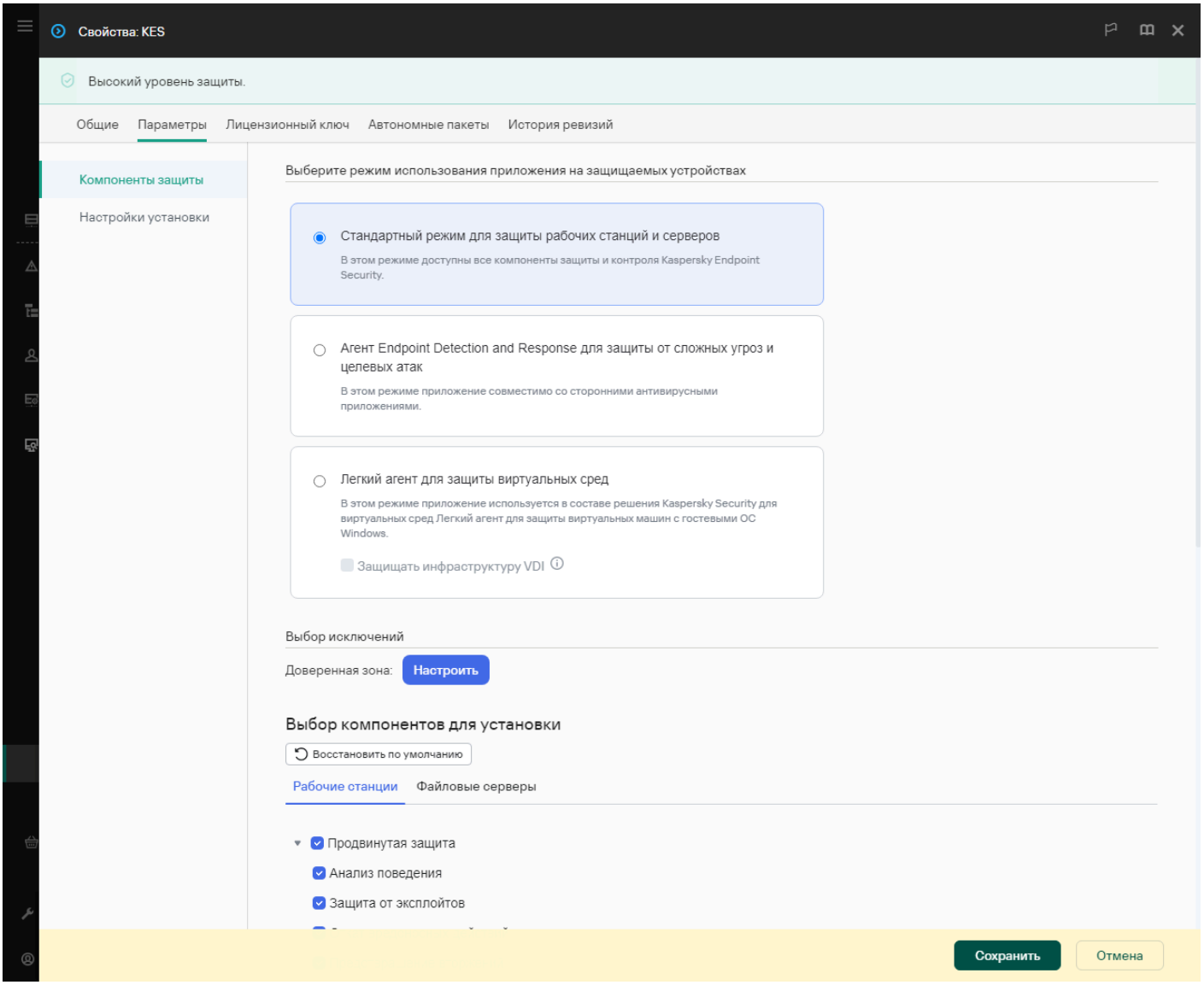
Список инсталляционных пакетов на серверах "Лаборатории Касперского"

Завершение работы мастера

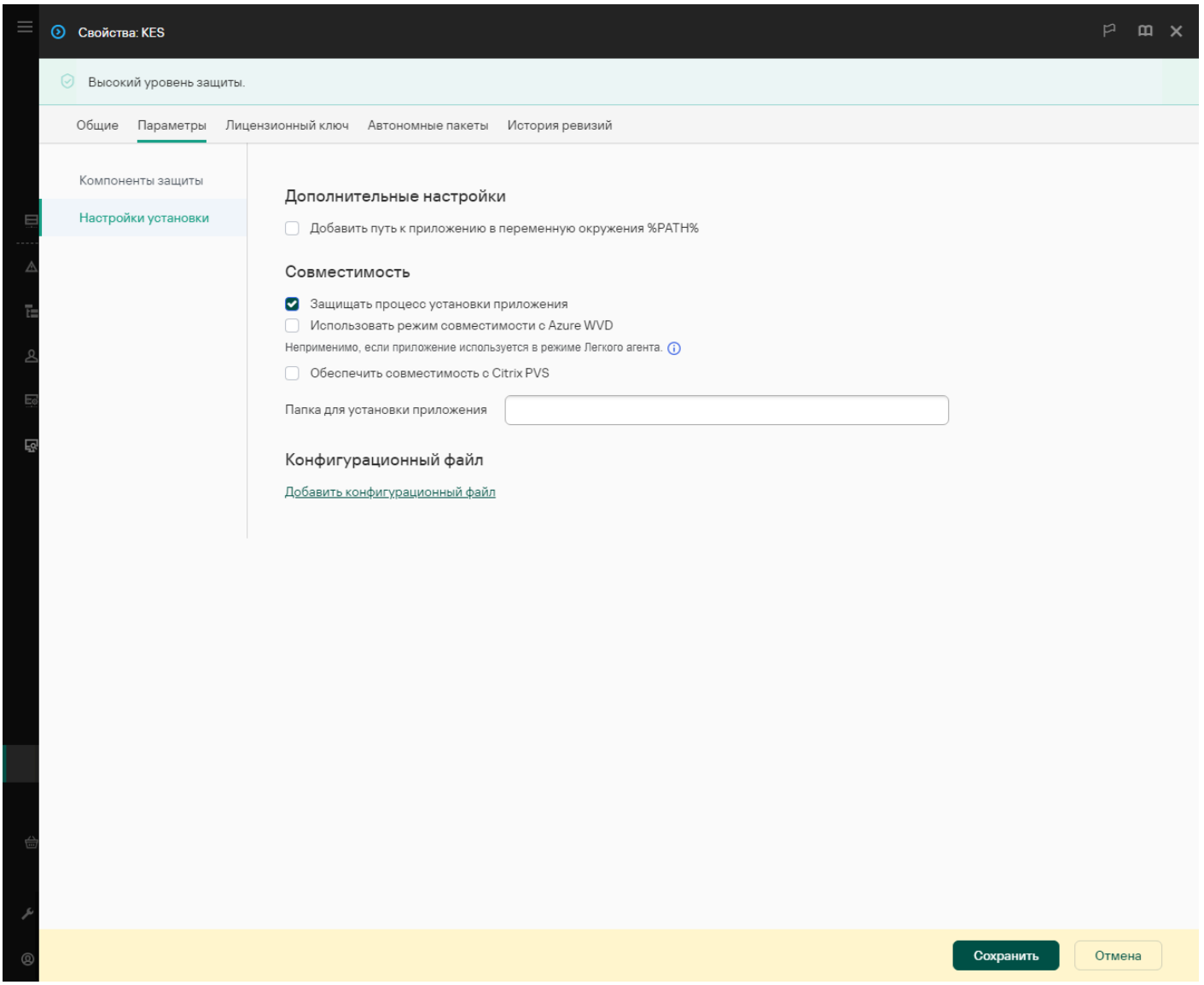
Инсталляционный пакет будет создан и добавлен в Kaspersky Security Center. С помощью инсталляционного пакета вы можете установить Kaspersky Endpoint Security на компьютеры сети организации или обновить версию приложения.

В параметрах инсталляционного пакета вы можете выбрать компоненты приложения для разных типов операционных систем. То есть инсталляционный пакет включает в себя два набора компонентов: для рабочих станций и для серверов. Установщик перед разворачиванием инсталляционного пакета определяет тип операционной системы и устанавливает только те компоненты приложения, которые вы выбрали для определенного типа операционной системы. Таким образом, вы можете использовать один инсталляционный пакет для рабочих станций и серверов.

Инсталляционный пакет содержит антивирусные базы из хранилища Сервера администрирования. Вы можете обновлять базы в инсталляционном пакете, чтобы уменьшить расход трафика при обновлении баз после установки Kaspersky Endpoint Security.



Состав компонентов в инсталляционном пакете



Параметры установки инсталляционного пакета

Параметры инсталляционного пакета

Раздел	Описание
Компоненты защиты	**Стандартный режим**. Конфигурация по умолчанию. В этой конфигурации вам доступны все компоненты приложения, включая компоненты для работы решений Detection and Response. Эта конфигурация нужна для развертывания комплексной защиты компьютера от различного вида угроз, сетевых и мошеннических атак. **Агент Endpoint Detection and Response**. В этой конфигурации вы можете установить только компоненты для работы решений Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), а также KUMA. Эта конфигурация нужна в том случае, если в вашей организации развернута система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков и решение Detection and Response от "Лаборатории Касперского". Таким образом, Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента может быть совместим со сторонними EPP-приложениями. **Легкий агент для защиты виртуальных сред**. Эта конфигурация предназначена для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Легкий агент должен быть установлен на каждой виртуальной машине, которую требуется защищать с помощью решения. В этой конфигурации недоступны компоненты шифрования данных и Адаптивный контроль аномалий. Если вы устанавливаете Легкий агент на шаблон виртуальных машин, из которого вы будете создавать *временные виртуальные машины*, установите флажок **Защищать инфраструктуру VDI** (Virtual Desktop Infrastructure). Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. В этом режиме Легкий агент отклоняет обновления приложения, требующие перезагрузки виртуальной машины. При получении обновлений приложения, требующих перезагрузки, Легкий агент формирует событие о необходимости обновить шаблон защищенных виртуальных машин.

Раздел	Описание
Исключения	Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах. Начиная с версии Kaspersky Endpoint Security для Windows 12.8 добавлена установка приложения в режиме Легкого агента для защиты виртуальных сред. Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в виртуальных средах Citrix и VMware. Вы также можете настроить доверенную зону позднее в свойствах политики: исключения из проверки и доверенные приложения.
Выбор компонентов для установки	В этом разделе вы можете выбрать компоненты приложения, которые будут доступны. Вы можете изменить состав компонентов приложения позднее с помощью задачи *Изменение состава компонентов приложения*. Вы можете создать отдельный набор компонентов для рабочих станций и отдельный набор компонентов для серверов. Установщик перед развертыванием инсталляционного пакета определяет тип операционной системы и устанавливает только те компоненты приложения, которые вы выбрали для определенного типа операционной системы. Таким образом, вы можете использовать один инсталляционный пакет для рабочих станций и серверов. Набор доступных компонентов зависит от конфигурации приложения: **Стандартный режим** Компоненты Шифрование данных Kaspersky, Шифрование файлов, Удаленный доступ и все встроенные агенты, кроме EDR Optimum, не устанавливаются по умолчанию. Эти компоненты можно добавить в параметрах инсталляционного пакета. **Агент Endpoint Detection and Response** В этой конфигурации доступны только встроенные агенты для работы решений Detection and Response от "Лаборатории Касперского". **Легкий агент для защиты виртуальных сред** В этой конфигурации доступны почти все компоненты приложения, что доступны в конфигурации **Стандартный режим**, кроме компонентов шифрования данных и Адаптивного контроля аномалий.
Лицензионный ключ	В этом разделе вы можете активировать приложение. Для активации приложения вам нужно выбрать лицензионный ключ. Перед этим вам нужно добавить ключ на Сервер администрирования. Подробнее о добавлении ключей на Сервер администрирования Kaspersky Security Center см. в справке Kaspersky Security Center.
Несовместимые приложения	Ознакомьтесь со списком несовместимых приложений и разрешите удаление этих приложений. Если на компьютере установлены несовместимые приложения, установка Kaspersky Endpoint Security завершается с ошибкой.
Настройки установки	**Добавить путь к файлу avp.com в системную переменную %PATH%**. Вы можете добавить путь установки в переменную %PATH% для удобства использования интерфейса командной строки. **Защищать процесс установки приложения**. Защита установки включает в себя защиту от подмены дистрибутива вредоносными приложениями, блокирование доступа к папке установки Kaspersky Endpoint Security и блокирование доступа к разделу системного реестра с ключами приложения. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку приложения (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop). **Обеспечить совместимость с Citrix PVS**. Вы можете включить поддержку Citrix Provisioning Services для установки Kaspersky Endpoint Security на виртуальную машину. **Использовать режим совместимости с Azure WVD**. Функция позволяет корректно показывать состояние виртуальной машины Azure в консоли Kaspersky Anti Targeted Attack Platform. Для контроля за состоянием компьютера Kaspersky Endpoint Security отправляет на серверы KATA телеметрию. Телеметрия включает в себя идентификатор компьютера (Sensor ID). Режим совместимости с Azure WVD позволяет назначать постоянный уникальный Sensor ID для этих виртуальных машин. Если режим совместимости выключен, то из-за особенностей работы виртуальных машин Azure Sensor ID может изменяться после перезагрузки компьютера. Из-за этого возможно дублирование виртуальных машин в консоли. **Папка для установки приложения**. Вы можете изменить путь установки Kaspersky Endpoint Security на клиентском компьютере. По умолчанию приложение устанавливается в папку `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.3`. **Конфигурационный файл**. Установка приложение с заранее заданными параметрами. Для этого вам нужно загрузить файл, который задает параметры работы Kaspersky Endpoint Security. Вы можете создать конфигурационный файл в локальном интерфейсе приложения. Мастер создания инсталляционного пакета не поддерживает зашифрованные конфигурационные файлы. При экспорте конфигурационного файла пропустите шаг шифрования файла.

Обновление баз в инсталляционном пакете

Инсталляционный пакет содержит антивирусные базы из хранилища Сервера администрирования, актуальные при создании инсталляционного пакета. После создания инсталляционного пакета вы можете обновлять антивирусные базы в инсталляционном пакете. Это позволяет уменьшить расход трафика на обновление антивирусных баз после установки Kaspersky Endpoint Security.

Чтобы обновить антивирусные базы в хранилище Сервера администрирования, используйте задачу Сервера администрирования *Загрузка обновлений в хранилище Сервера администрирования*. Подробнее об обновлении антивирусных баз в хранилище Сервера администрирования см. в справке Kaspersky Security Center.

Вы можете обновлять базы в инсталляционном пакете только в Консоли администрирования и Kaspersky Security Center Web Console. Обновлять базы в инсталляционном пакете в Kaspersky Security Center Cloud Console невозможно.

Как обновить антивирусные базы в инсталляционном пакете через Консоль администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно → Удаленная установка → Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.
3. Откройте свойства инсталляционного пакета.
4. В разделе **Общие** нажмите на кнопку **Обновить базы**.

   В результате антивирусные базы в инсталляционном пакете будут обновлены из хранилища Сервера администрирования. Файл `bases.cab`, который входит в комплект поставки, будет заменен папкой `bases`. Внутри папки будут расположены файлы пакетов обновлений.

Как обновить антивирусные базы в инсталляционном пакете через Web Console

1. В главном окне Web Console выберите **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Web Console.
2. Нажмите на название инсталляционного пакета Kaspersky Endpoint Security, в котором вы хотите обновить антивирусные базы.

   Откроется окно свойств инсталляционного пакета.
3. На вкладке **Общая информация** нажмите на ссылку **Обновить базы**.

   В результате антивирусные базы в инсталляционном пакете будут обновлены из хранилища Сервера администрирования. Файл `bases.cab`, который входит в комплект поставки, будет заменен папкой `bases`. Внутри папки будут расположены файлы пакетов обновлений.

Создание задачи удаленной установки

Для удаленной установки Kaspersky Endpoint Security предназначена задача *Удаленная установка приложения*. Задача *Удаленная установка приложения* позволяет развернуть инсталляционный пакет приложения на все компьютеры организации. Перед развертыванием инсталляционного пакета вы можете обновить антивирусные базы внутри пакета, а также выбрать доступные компоненты приложения в свойствах инсталляционного пакета.

Как создать задачу удаленной установки в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.

   Откроется список задач.
3. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Сервер администрирования Kaspersky Security Center → Удаленная установка приложения**.

Шаг 2. Выбор инсталляционного пакета

В списке инсталляционных пакетов выберите пакет Kaspersky Endpoint Security. Если в списке отсутствует инсталляционный пакет Kaspersky Endpoint Security, вы можете создать пакет в мастере.

Вы можете настроить параметры инсталляционного пакета в Kaspersky Security Center, например, выбрать компоненты приложения, которые будут установлены на компьютер.

Также с Kaspersky Endpoint Security будет установлен Агент администрирования. *Агент администрирования* обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

Шаг 3. Дополнительно

Выберите инсталляционный пакет Агента администрирования. Выбранная версия Агента администрирования будет установлена вместе с Kaspersky Endpoint Security.

Шаг 4. Параметры

Настройте следующие дополнительные параметры приложения:

- **Принудительно скачать инсталляционный пакет**. Выберите средства установки приложения:

  - **С помощью Агента администрирования**. Доставку инсталляционного пакета Kaspersky Endpoint Security на клиентские компьютеры выполняет Агент администрирования. Если Агент администрирования не установлен, выполнение задачи завершится ошибкой. В этом случае вам нужно добавить инсталляционный пакет Агента администрирования в задачу *Удаленная установка приложения* и включить доставку файлов средствами операционной системы. Тогда Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security устанавливается средствами Агента администрирования.

  - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.

  - **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

- **Поведение устройств, управляемых другими Серверами администрирования**. Выберите способ установки Kaspersky Endpoint Security. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одного и того же приложения на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

- **Не устанавливать приложение, если оно уже установлено**. Снимите этот флажок, если вы хотите, например, установить приложение более ранней версии.

Шаг 5. Выбор параметра перезагрузки операционной системы

Выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера. При установке Kaspersky Endpoint Security перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые приложения. Также перезагрузка может потребоваться при обновлении версии приложения.

Шаг 6. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которые будет установлено приложение Kaspersky Endpoint Security. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, — *нераспределенные устройства*. На нераспределенных устройствах не установлен Агент администрирования. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 7. Выбор учетной записи для запуска задачи

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки Kaspersky Endpoint Security средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 8. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 9. Определение названия задачи

Введите название задачи, например, *Установка Kaspersky Endpoint Security для Windows 14.3*.

Шаг 10. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи. Установка приложения будет выполнена в тихом режиме. После установки в области уведомлений компьютера пользователя будет добавлен значок . Если значок имеет вид , убедитесь, что вы активировали приложение.

Как создать задачу удаленной установки в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Приложение** выберите **Kaspersky Security Center**.
2. В раскрывающемся списке **Тип задачи** выберите **Удаленная установка приложения**.
3. В поле **Название задачи** введите короткое описание, например, *Установка Kaspersky Endpoint Security для менеджеров*.
4. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Выбор компьютеров для установки

На этом шаге выберите компьютеры, на которые будет установлено приложение Kaspersky Endpoint Security, в соответствии с выбранным вариантом области действия задачи.

Шаг 3. Настройка параметров инсталляционного пакета

На этом шаге настройте параметры инсталляционного пакета:

1. Выберите инсталляционный пакет Kaspersky Endpoint Security для Windows (14.3).
2. Выберите инсталляционный пакет Агента администрирования.

   Выбранная версия Агента администрирования будет установлена вместе с Kaspersky Endpoint Security. *Агент администрирования* обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

3. В блоке **Принудительно скачать инсталляционный пакет** выберите средства установки приложения:

   - **С помощью Агента администрирования**. Доставку инсталляционного пакета Kaspersky Endpoint Security на клиентские компьютеры выполняет Агент администрирования. Если Агент администрирования не установлен, выполнение задачи завершится ошибкой. В этом случае вам нужно добавить инсталляционный пакет Агента администрирования в задачу *Удаленная установка приложения* и включить доставку файлов средствами операционной системы. Тогда Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security устанавливается средствами Агента администрирования.

   - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.

   - **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

4. В поле **Максимальное количество одновременных загрузок** установите ограничение количества запросов к Серверу администрирования для загрузки инсталляционного пакета. Ограничение запросов позволит избежать перегрузки сети.

5. В поле **Максимальное количество попыток установок** установите ограничение попыток установить приложение. Если установка Kaspersky Endpoint Security завершается с ошибкой, задача автоматически запускает установку повторно.

6. Если требуется, снимите флажок **Не устанавливать приложение, если оно уже установлено**. Это позволит, например, установить приложение более ранней версии.

7. Если требуется, снимите флажок **Предварительно проверять тип операционной системы перед загрузкой**. Это позволит избежать загрузки дистрибутива приложения, если операционная система компьютера не соответствует программным требованиям. Если вы уверены, что операционная система компьютера соответствует программным требованиям, проверку можно пропустить.

8. Если требуется, установите флажок **Назначить установку инсталляционного пакета в групповых политиках Active Directory**. Установка Kaspersky Endpoint Security выполняется средствами Агента администрирования или средствами Active Directory вручную. Для установки Агента администрирования задача удаленной установки должна быть запущена с правами администратора домена.

9. Если требуется, установите флажок **Предлагать пользователю закрыть работающие приложения**. Установка Kaspersky Endpoint Security требует ресурсов компьютера. Для удобства пользователя мастер установки приложения предлагает закрыть работающие приложения перед началом установки. Это позволит избежать замедление в работе других приложений и возможных сбоев в работе компьютера.

10. В блоке **Поведение устройств, управляемых другими Серверами администрирования** выберите способ установки Kaspersky Endpoint Security. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одного и того же приложения на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

Шаг 4. Выбор учетной записи для запуска задачи

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки Kaspersky Endpoint Security средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 5. Завершение создания задачи

Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача. Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку **Запустить**. Установка приложения будет выполнена в тихом режиме. После установки в области уведомлений компьютера пользователя будет добавлен значок . Если значок имеет вид , убедитесь, что вы активировали приложение.

Локальная установка приложения с помощью мастера

Интерфейс мастера установки приложения состоит из последовательности окон, соответствующих шагам установки приложения. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов.

Чтобы установить приложение или обновить предыдущую версию приложения с помощью мастера установки приложения, выполните следующие действия:

1. Скопируйте папку комплекта поставки на компьютер пользователя.
2. Запустите файл setup_kes.exe.

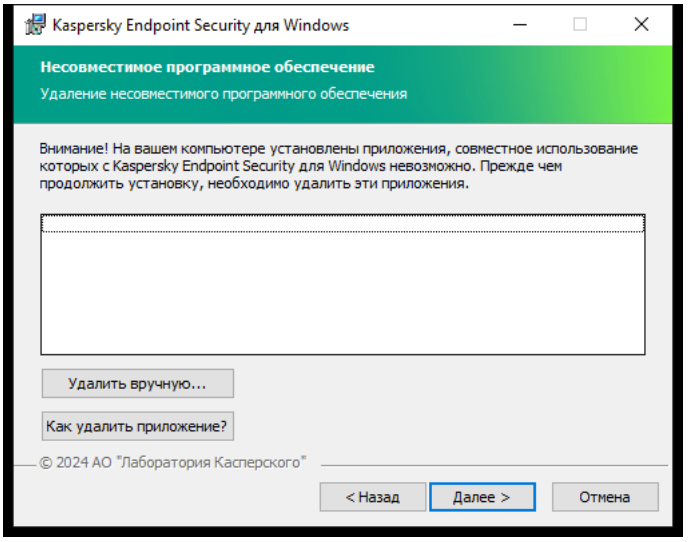
   Запустится мастер установки приложения.

Подготовка к установке

Перед установкой Kaspersky Endpoint Security на компьютер или обновлением предыдущей версии приложения проверяются следующие условия:

- наличие программного обеспечения, с которым у приложения Kaspersky Endpoint Security могут быть проблемы совместимости (список ПО приведен в файле incompatible.txt в комплекте поставки);
- выполнение аппаратных и программных требований;
- наличие Microsoft .NET Framework;
- наличие прав на установку программного обеспечения.

Если какое-либо из перечисленных условий не выполнено, на экран выводится соответствующее уведомление. Например, уведомление о наличии несовместимого ПО (см. рис. ниже).



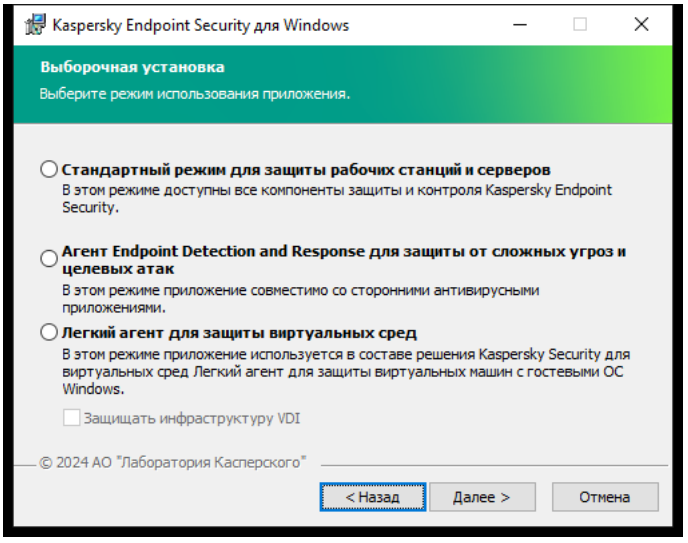
Удаление несовместимого программного обеспечения

Если компьютер соответствует предъявляемым требованиям, мастер установки приложения выполняет поиск приложений "Лаборатории Касперского", одновременная работа которых может привести к возникновению конфликтов. Если такие приложения найдены, вам предлагается удалить их вручную.

Если в числе обнаруженных приложений есть предыдущие версии Kaspersky Endpoint Security, то все данные, которые могут быть мигрированы (например, информация об активации, параметры приложения), сохраняются и используются при установке Kaspersky Endpoint Security 14.3 для Windows, а предыдущая версия приложения автоматически удаляется. Это относится к следующим версиям приложения:

- Kaspersky Endpoint Security для Windows 12.3 (сборка 12.3.0.493).
- Kaspersky Endpoint Security для Windows 12.4 (сборка 12.4.0.467).
- Kaspersky Endpoint Security для Windows 12.5 (сборка 12.5.0.539).
- Kaspersky Endpoint Security для Windows 12.6 (сборка 12.6.0.438).
- Kaspersky Endpoint Security для Windows 12.7 (сборка 12.7.0.533).
- Kaspersky Endpoint Security для Windows 12.8 (сборка 12.8.0.505).
- Kaspersky Endpoint Security для Windows 12.9 (сборка 12.9.0.384).
- Kaspersky Endpoint Security для Windows 12.10 (сборка 12.10.0.466).
- Kaspersky Endpoint Security для Windows 12.11 (сборка 12.11.0.637).
- Kaspersky Endpoint Security для Windows 12.12 (сборка 12.12.0.522).
- Kaspersky Endpoint Security для Windows 14.0 (сборка 14.0.0.504).
- Kaspersky Endpoint Security для Windows 14.1 (сборка 14.1.0.423).
- Kaspersky Endpoint Security для Windows 14.2 (сборка 14.2.0.536).

Конфигурация Kaspersky Endpoint Security



Выбор конфигурации приложения

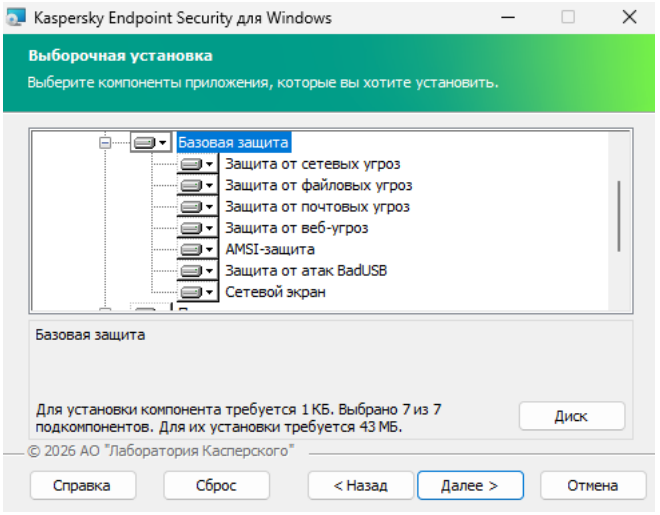
Стандартный режим. Конфигурация по умолчанию. В этой конфигурации вам доступны все компоненты приложения, включая компоненты для работы решений Detection and Response. Эта конфигурация нужна для развертывания комплексной защиты компьютера от различного вида угроз, сетевых и мошеннических атак.

Агент Endpoint Detection and Response. В этой конфигурации вы можете установить только компоненты для работы решений Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), а также KUMA. Эта конфигурация нужна в том случае, если в вашей организации развернута система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков и решение Detection and Response от "Лаборатории Касперского". Таким образом, Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента может быть совместим со сторонними EPP-приложениями.

Легкий агент для защиты виртуальных сред. Эта конфигурация предназначена для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Легкий агент должен быть установлен на каждой виртуальной машине, которую требуется защищать с помощью решения. В этой конфигурации недоступны компоненты шифрования данных и Адаптивный контроль аномалий. Если вы устанавливаете Легкий агент на шаблон виртуальных машин, из которого вы будете создавать *временные виртуальные машины*, установите флажок **Защищать инфраструктуру VDI** (Virtual Desktop Infrastructure). Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. В этом режиме Легкий агент отклоняет обновления приложения, требующие перезагрузки виртуальной машины. При получении обновлений приложения, требующих перезагрузки, Легкий агент формирует событие о необходимости обновить шаблон защищенных виртуальных машин.

Компоненты Kaspersky Endpoint Security

В процессе установки вы можете выбрать компоненты Kaspersky Endpoint Security, которые вы хотите установить (см. рис. ниже). Компонент Защита от файловых угроз является обязательным компонентом для установки. Вы не можете отменить его установку.



Выбор компонентов для установки приложения

По умолчанию для установки выбраны все компоненты приложения, кроме следующих компонентов:

- Удаленный доступ.
- Шифрование диска Kaspersky.
- Шифрование файлов.
- Endpoint Detection and Response Expert (on-premises).
- Endpoint Detection and Response Expert (cloud).
- Sandbox.
- Managed Detection and Response.
- Network Detection and Response (KATA).
- Интеграция с KUMA.

Вы можете изменить состав компонентов после установки приложения. Для этого вам нужно запустить мастер установки повторно и выбрать операцию изменения состава компонентов.

Если вам нужно установить компоненты Detection and Response, Kaspersky Endpoint Security поддерживает следующие конфигурации:

- только Endpoint Detection and Response Optimum;
- только Endpoint Detection and Response Expert (cloud);
- только Endpoint Detection and Response Expert (on-premises);

- только Network Detection and Response (KATA);
- только Sandbox;
- Endpoint Detection and Response Optimum и Sandbox;
- Endpoint Detection and Response Expert (cloud) и Sandbox;
- Endpoint Detection and Response Expert (on-premises) и Sandbox;
- Network Detection and Response (KATA) и Endpoint Detection and Response Expert (on-premises);
- Network Detection and Response (KATA) и Managed Detection and Response.

Kaspersky Endpoint Security проверяет выбор компонентов перед установкой приложения. Если конфигурация компонентов Detection and Response не поддерживается, установить Kaspersky Endpoint Security невозможно.

Выбор папки для установки приложения

Вы можете изменить путь установки Kaspersky Endpoint Security на клиентском компьютере. По умолчанию приложение устанавливается в папку `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.3`.

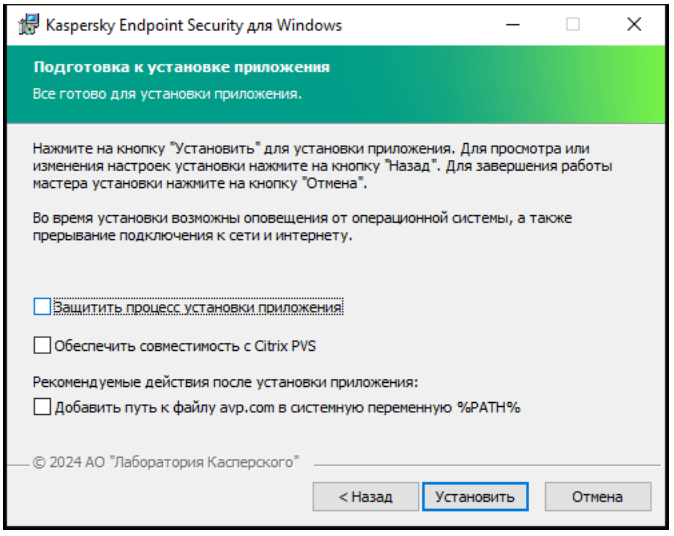
Настройка доверенной зоны

Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах.

Начиная с версии Kaspersky Endpoint Security для Windows 12.8 добавлена установка приложения в режиме Легкого агента для защиты виртуальных сред. Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в виртуальных средах Citrix и VMware.

Вы также можете настроить доверенную зону позднее в свойствах политики: исключения из проверки и доверенные приложения.

Дополнительные параметры



Дополнительные параметры установки приложения

Защитить процесс установки приложения. Защита установки включает в себя защиту от подмены дистрибутива вредоносными приложениями, блокирование доступа к папке установки Kaspersky Endpoint Security и блокирование доступа к разделу системного реестра с ключами приложения. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку приложения (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop).

Обеспечить совместимость с Citrix PVS. Вы можете включить поддержку Citrix Provisioning Services для установки Kaspersky Endpoint Security на виртуальную машину.

Добавить путь к файлу avp.com в системную переменную %PATH%. Вы можете добавить путь установки в переменную %PATH% для удобства использования интерфейса командной строки.

Удаленная установка приложения с помощью System Center Configuration Manager

Инструкция актуальна для версии System Center Configuration Manager 2012 R2.

Чтобы удаленно установить приложение с помощью System Center Configuration Manager, выполните следующие действия:

1. Откройте консоль Configuration Manager.
2. В правой части консоли в блоке **Управление приложениями** выберите раздел **Пакеты**.
3. В верхней части консоли в панели управления нажмите на кнопку **Создать пакет**.

   Запустится *Мастер создания пакетов и приложений*.

4. В Мастере создания пакетов и приложений выполните следующие действия:

   a. В разделе **Пакет** выполните следующие действия:

      - В поле **Имя** введите имя инсталляционного пакета.
      - В поле **Исходная папка** укажите путь к папке, в которой расположен дистрибутив Kaspersky Endpoint Security.

   b. В разделе **Тип программы** выберите вариант **Стандартная программа**.

   c. В разделе **Стандартная программа** выполните следующие действия:

      - В поле **Имя** введите уникальное имя инсталляционного пакета (например, название приложения с указанием версии).
      - В поле **Командная строка** укажите параметры установки Kaspersky Endpoint Security из командной строки.
      - По кнопке **Обзор** задайте путь к исполняемому файлу приложения.
      - Убедитесь, что в раскрывающемся списке **Режим выполнения** выбран элемент **Запустить с правами администратора**.

   d. В разделе **Требования** выполните следующие действия:

      - Установите флажок **Запустить сначала другую программу**, если вы хотите, чтобы перед установкой Kaspersky Endpoint Security было запущено другое приложение.

        Выберите приложение из раскрывающегося списка **Программа** или укажите путь к исполняемому файлу этого приложения по кнопке **Обзор**.

      - Выберите вариант **Эту программу можно запускать только на указанных платформах** в блоке **Требования к платформе**, если вы хотите, чтобы приложение было установлено только в указанных операционных системах.

        В списке ниже установите флажки напротив тех операционных систем, в которых должен быть установлен Kaspersky Endpoint Security.

      Этот шаг не является обязательным.

   e. В разделе **Сводка** проверьте все заданные значения параметров и нажмите на кнопку **Далее**.

   Созданный инсталляционный пакет появится в разделе **Пакеты** в списке доступных инсталляционных пакетов.

5. В контекстном меню инсталляционного пакета выберите пункт **Развернуть**.

   Запустится *Мастер развертывания программного обеспечения*.

6. В Мастере развертывания программного обеспечения выполните следующие действия:

   a. В разделе **Общие** выполните следующие действия:

      - В поле **Программное обеспечение** введите уникальное имя инсталляционного пакета или выберите инсталляционный пакет из списка по кнопке **Обзор**.
      - В поле **Коллекция** введите название коллекции компьютеров, на которые должно быть установлено приложение, или выберите эту коллекцию по кнопке **Обзор**.

   b. В разделе **Содержимое** добавьте точки распространения (более подробную информацию вы можете найти в сопроводительной документации для System Center Configuration Manager).

   c. Если требуется, укажите значения других параметров в мастере развертывания программного обеспечения. Эти параметры являются необязательными для удаленной установки Kaspersky Endpoint Security.

   d. В разделе **Сводка** проверьте все заданные значения параметров и нажмите на кнопку **Далее**.

После завершения работы Мастера развертывания программного обеспечения будет создана задача по удаленной установке Kaspersky Endpoint Security.

Описание параметров установки в файле setup.ini

Файл setup.ini используется при установке приложения из командной строки или с помощью редактора управления групповыми политиками Microsoft Windows. Чтобы применить параметры из файла setup.ini, разместите файл в папке с дистрибутивом Kaspersky Endpoint Security.

Используйте файл setup.ini только при установке приложения в тихом режиме.

Добавить путь к конфигурационному файлу install.cfg в файле setup.ini невозможно. Также приложение пропускает конфигурационный файл install.cfg, если он просто находится в папке с дистрибутивом Kaspersky Endpoint Security. Чтобы применить параметры из конфигурационного файла install.cfg, вам нужно указать путь к файлу в команде установки приложения: `CONFIGPATH=<path to the configuration file>`.

ЗАГРУЗИТЬ ФАЙЛ SETUP.INI

Файл setup.ini состоит из следующих разделов:

- `[Setup]` – общие параметры установки приложения.
- `[Components]` – выбор компонентов приложения для установки в стандартном режиме. Если не указан ни один из компонентов, то устанавливаются все доступные для операционной системы компоненты. Защита от файловых угроз является обязательным компонентом и устанавливается на компьютер независимо от того, какие параметры указаны в этом блоке.
- `[Tasks]` – выбор задач для включения в список задач Kaspersky Endpoint Security. Если не указана ни одна задача, все задачи включаются в список задач Kaspersky Endpoint Security.

Вместо значения `1` могут использоваться значения `yes`, `on`, `enable`, `enabled`, `true`. Вместо значения `0` могут использоваться значения `no`, `off`, `disable`, `disabled`, `false`.

Параметры файла setup.ini

Раздел	Параметр	Описание
`[Setup]`	`InstallDir`	Путь к папке установки приложения.
	`ActivationCode`	Код активации Kaspersky Endpoint Security.
	`Eula`	Согласие с положениями Лицензионного соглашения. Текст Лицензионного соглашения входит в комплект поставки Kaspersky Endpoint Security. Согласие с положениями Лицензионного соглашения является необходимым условием для установки приложения или обновления версии приложения.
	`PrivacyPolicy`	Согласие с Политикой конфиденциальности. Текст Политики конфиденциальности входит в комплект поставки Kaspersky Endpoint Security. Согласие с Политикой конфиденциальности является необходимым условием для установки приложения или обновления версии приложения.
	`KSN`	Согласие или отказ участвовать в Kaspersky Security Network (KSN). Если параметр не указан, Kaspersky Endpoint Security запросит подтверждения участия в KSN при первом запуске приложения. Возможные значения: • `1` – согласие участвовать в KSN. • `0` – отказ участвовать в KSN (значение по умолчанию). Дистрибутив Kaspersky Endpoint Security оптимизирован для использования Kaspersky Security Network. Если вы отказались от участия в Kaspersky Security Network, то сразу после завершения установки обновите Kaspersky Endpoint Security.
	`CLEANERSIGNCHECK`	Проверка цифровых подписей файлов найденного ПО из файла incompatible.txt. Для удаления ПО приложение Kaspersky Endpoint Security запускает файл инсталлятора программного обеспечения. Если у файла инсталлятора нет цифровой подписи, Kaspersky Endpoint Security считает такой файл недоверенным, и для предотвращения исполнения вредоносного кода приложение прекращает удаление ПО. Если приложение не может проверить цифровую подпись файла найденного ПО, установка Kaspersky Endpoint Security будет остановлена с ошибкой. Значение по умолчанию отличается в зависимости от способа установки приложения: • `0` – проверка цифровой подписи выключена (значение по умолчанию при развертывании через Kaspersky Security Center). • `1` – проверка цифровой подписи включена (значение по умолчанию при локальной установке приложения).
	`Login`	Установка имени пользователя для доступа к управлению функциями и параметрами Kaspersky Endpoint Security (компонент Защита паролем). Имя пользователя устанавливается вместе с параметрами `Password` и `PasswordArea`. По умолчанию используется имя пользователя KLAdmin.

Раздел	Параметр	Описание
	`Password`	Установка пароля для доступа к управлению функциями и параметрами Kaspersky Endpoint Security (пароль устанавливается вместе с параметрами `Login` и `PasswordArea`). Если вы указали пароль, но не задали имя пользователя с помощью параметра `Login`, то по умолчанию используется имя пользователя KLAdmin.
	`PasswordArea`	Определение области действия пароля для доступа к Kaspersky Endpoint Security. При попытке пользователя выполнить действие из этой области Kaspersky Endpoint Security запрашивает учетные данные пользователя (параметры `Login` и `Password`). Для указания множественного значения используйте символ `;`. Возможные значения: • `SET` – изменение параметров приложения. • `EXIT` – завершение работы приложения. • `DISPROTECT` – выключение компонентов защиты и остановка задач проверки. • `DISPOLICY` – выключение политики Kaspersky Security Center. • `UNINST` – удаление приложения с компьютера. • `DISCTRL` – выключение компонентов контроля. • `REMOVELIC` – удаление ключа. • `REPORTS` – просмотр отчетов. • `EXPORT` – экспорт параметров приложения. Например, `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.
	`SelfProtection`	Включение или выключение механизма защиты установки приложения. Возможные значения: • `1` – механизм защиты установки приложения включен (значение по умолчанию). • `0` – механизм защиты установки приложения выключен. Защита установки включает в себя защиту от подмены дистрибутива вредоносными приложениями, блокирование доступа к папке установки Kaspersky Endpoint Security и блокирование доступа к разделу системного реестра с ключами приложения. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку приложения (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop).
	`PROTECTOSSERVICES`	Функция Защита сервисов операционной системы. Защита сервисов операционной системы предотвращает вмешательство сторонних приложений в работу сервисов операционной системы. К таким сервисам относится, например, сервис автозапуска приложений. • `1` – Защита сервисов операционной системы включена (значение по умолчанию). • `0` – Защита сервисов операционной системы выключена.
	`EnableAzureSupport`	Включение или выключения режима совместимости с Azure WVD. Возможные значения: • `1` – режим совместимости с Azure WVD включен. • `0` – режим совместимости с Azure WVD выключен (значение по умолчанию). Функция позволяет корректно показывать состояние виртуальной машины Azure в консоли Kaspersky Anti Targeted Attack Platform. Для контроля за состоянием компьютера Kaspersky Endpoint Security отправляет на серверы KATA телеметрию. Телеметрия включает в себя идентификатор компьютера (Sensor ID). Режим совместимости с Azure WVD позволяет назначать постоянный уникальный Sensor ID для этих виртуальных машин. Если режим совместимости выключен, то из-за особенностей работы виртуальных машин Azure Sensor ID может изменяться после перезагрузки компьютера. Из-за этого возможно дублирование виртуальных машин в консоли.
	`Reboot`	Автоматическая перезагрузка компьютера после установки или обновления приложения, если требуется. Если параметр не задан, автоматическая перезагрузка компьютера запрещена. При установке Kaspersky Endpoint Security перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые приложения. Также перезагрузка может потребоваться при обновлении версии приложения.
	`AddEnvironment`	Добавление в системную переменную %PATH% пути к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security. Возможные значения: • `1` – в системную переменную %PATH% добавляется путь к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security. • `0` – в системную переменную %PATH% не добавляется путь к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security.

Раздел	Параметр	Описание
	AMPPL	Включение или выключение защиты процессов Kaspersky Endpoint Security с использованием технологии AM-PPL (Antimalware Protected Process Light). Подробнее о технологии AM-PPL см. на сайте Microsoft. Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019. Возможные значения: • 1 – защита процессов Kaspersky Endpoint Security с использованием технологии AM-PPL включена (значение по умолчанию). • 0 – защита процессов Kaspersky Endpoint Security с использованием технологии AM-PPL выключена.
	UPGRADEMODE	Режим обновления приложения: • Seamless – обновление приложения с перезагрузкой компьютера (значение по умолчанию). • Force – обновление приложения без перезагрузки. Вы можете обновлять версию приложения без перезагрузки начиная с версии 11.10.0. Для обновление более ранних версий приложения необходимо выполнять перезагрузку компьютера. Также вы можете устанавливать патчи без перезагрузки начиная с версии 11.11.0. При установке Kaspersky Endpoint Security перезагрузка не требуется. Таким образом, режим обновления приложения будет установлен в параметрах приложения. Вы можете изменить этот параметр в настройках приложения или в политике. Если приложение уже установлено, при установке обновления приоритет параметра из файла setup.ini выше, чем параметр, заданный в настройках приложения или в командной строке. То есть, если в файле setup.ini задан режим Force, а в параметрах приложения задан режим Seamless, инсталлятор установит обновление без перезагрузки (Force). Если вы используете для обновления файл setup.ini, в котором параметр UPGRADEMODE не задан, инсталлятор использует значение по умолчанию (Seamless) и установит обновление с перезагрузкой.
	SetupReg	Включение записи ключей реестра из файла setup.reg в реестр. Значение параметра SetupReg: setup.reg.
	EnableTraces	Включение или выключение трассировки приложения. После запуска Kaspersky Endpoint Security приложение сохраняет файлы трассировки в папке %ProgramData%\Kaspersky Lab\KES.14.3\Traces. Возможные значения: • 1 – трассировка включена. • 0 – трассировка выключена (значение по умолчанию).
	TracesLevel	Уровень детализации трассировки. Возможные значения: • 100 (критический). Только сообщения о неустранимых ошибках. • 200 (высокий). Сообщения обо всех ошибках, включая неустранимые. • 300 (диагностический). Сообщения обо всех ошибках, а также предупреждения. • 400 (важный). Сообщения обо всех ошибках, предупреждения, а также дополнительная информация. • 500 (обычный). Сообщения обо всех ошибках, предупреждениях, а также подробная информация о работе приложения в нормальном режиме (значение по умолчанию). • 600 (низкий). Все сообщения.
	RESTAPI	Управление приложением через REST API. Для управления приложением через REST API обязательно нужно задать имя пользователя (параметр RESTAPI_User). Возможные значения: • 1 – управление через REST API разрешено. • 0 – управление через REST API запрещено (значение по умолчанию). Для управления приложением через REST API должно быть разрешено управление с помощью систем администрирования. Для этого задайте параметр AdminKitConnector=1. Если вы управляете приложением через REST API, управлять приложением с помощью систем администрирования "Лаборатории Касперского" невозможно.
	RESTAPI_User	Имя пользователя доменной учетной записи Windows для управления приложением через REST API. Управление приложением через REST API доступно только этому пользователю. Введите имя пользователя в формате <DOMAIN>\<UserName> (например, RESTAPI_User=COMPANY\Administrator). Для работы с REST API вы можете выбрать только одного пользователя. Добавление имени пользователя является необходимым условием для управления приложением через REST API.
	RESTAPI_Port	Порт для управления приложением через REST API. По умолчанию используется порт 6782. Убедитесь, что порт свободен.

Раздел	Параметр	Описание
	`RESTAPI_Certificate`	Сертификат для идентификации запросов (например, `RESTAPI_Certificate=C:\cert.pem`). Для безопасной работы Kaspersky Endpoint Security с REST-клиентом вам нужно настроить идентификацию запросов. Для этого вам нужно установить сертификат и в дальнейшем подписывать полезные данные каждого запроса.
	`StandaloneMode`	Установка приложения в режиме Endpoint Detection and Response агент (EDR-агент). *Endpoint Detection and Response агент* – приложение, которое устанавливается на отдельные рабочие станции и серверы IT-инфраструктуры организации, для работы решений Kaspersky Managed Detection and Response и Kaspersky Anti Targeted Attack Platform. EDR-агент совместим со сторонними EPP-приложениями. Таким образом, вы можете использовать средства защиты инфраструктуры от сторонних поставщиков совместно с решениями Detection and Response от "Лаборатории Касперского". Для установки EDR-агента вам нужно в разделе `[Components]` выбрать компоненты `StandaloneKATA`, `StandaloneNDR` или `StandaloneMDR`. EDR-агент не поддерживает другие компоненты приложения. Возможные значения: • `1` – установка приложения в режиме EDR-агента. • `0` – установка приложения в стандартном режиме (значение по умолчанию).
	`KSVLAMode`	Установка приложения в режиме Легкого агента. Эта конфигурация предназначена для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Легкий агент должен быть установлен на каждой виртуальной машине, которую требуется защищать с помощью решения. Возможные значения: • `1` – установка приложения в режиме Легкого агента. • `0` – установка приложения в стандартном режиме (значение по умолчанию).
	`InstallOnVDI`	Включение режима защиты инфраструктуры VDI при установке приложения в режиме Легкого агента (`KSVLAMode=1`). Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. В этом режиме Легкий агент отклоняет обновления приложения, требующие перезагрузки виртуальной машины. При получении обновлений приложения, требующих перезагрузки, Легкий агент формирует событие о необходимости обновить шаблон защищенных виртуальных машин. Возможные значения: • `1` – включение режима защиты инфраструктуры VDI. • `0` – выключение режима защиты инфраструктуры VDI (значение по умолчанию).
	`KESExclusions`	Добавление предустановленных исключений из проверки и доверенных приложений при установке приложения на сервер. Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. Например, предустановленные исключения из проверки для SQL-серверов включают в себя файлы баз данных MDF и LDF. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах. Возможные значения: • `1` – предустановленные исключения из проверки и доверенные приложения включены. • `0` – предустановленные исключения из проверки и доверенные приложения выключены (значение по умолчанию).
	`LAExclusions`	Добавление предустановленных исключений из проверки и доверенных приложений при установке приложения на виртуальную машину (режим Легкого агента). Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в виртуальных средах Citrix и VMWare. Возможные значения: • `1` – предустановленные исключения из проверки и доверенные приложения включены. • `0` – предустановленные исключения из проверки и доверенные приложения выключены (значение по умолчанию).

Раздел	Параметр	Описание
	`EnableUniqueSensorID`	Создание уникального идентификатора компьютера (Sensor ID) при установке или обновлении приложения. Sensor ID используется в решении Kaspersky Anti Targeted Attack Platform для идентификации компьютеров, которые отправляют телеметрию на сервер. При создании Sensor ID приложение использует алгоритм, который учитывает конфигурацию компьютера, например, серийный номер материнской платы. В некоторых случаях, например, при использовании приложения в виртуальной среде, Sensor ID может повторяться. Таким образом, Kaspersky Anti Targeted Attack Platform не может идентифицировать компьютер, с которого отправлена телеметрия. Для создания уникального Sensor ID вам нужно задать параметр `EnableUniqueSensorID=1`. В результате приложение будет использовать другой алгоритм для создания Sensor ID, который учитывает другие данные о компьютере. Это обеспечивает уникальный Sensor ID. По умолчанию параметр не задан. Приложение наследует Sensor ID в следующих случаях: • обновление версии приложения; • миграция конфигурации [KES+KEA] на [KES+встроенный агент]. При восстановлении приложения установщик пытается наследовать Sensor ID. Если восстановить Sensor ID не удалось, приложение создает новый Sensor ID.
	`CitrixCompatibility`	Включение поддержки Citrix Provisioning Services для установки Kaspersky Endpoint Security на виртуальную машину.
`[Components]`	`ALL`	Установка всех компонентов. Если указано значение параметра `1`, все компоненты будут установлены независимо от параметров установки отдельных компонентов. Из-за особенностей поддержки решений Detection and Response на компьютер будут установлены компоненты Endpoint Detection and Response Optimum и Sandbox. Компонент Endpoint Detection and Response Expert (cloud) несовместим с такой конфигурацией приложения.
	`MailThreatProtection`	Защита от почтовых угроз.
	`WebThreatProtection`	Защита от веб-угроз.
	`AMSI`	AMSI-защита.
	`HostIntrusionPrevention`	Предотвращение вторжений.
	`BehaviorDetection`	Анализ поведения.
	`ExploitPrevention`	Защита от эксплойтов.
	`RemediationEngine`	Откат вредоносных действий.
	`Firewall`	Сетевой экран.
	`NetworkThreatProtection`	Защита от сетевых угроз.
	`WebControl`	Веб-Контроль.
	`DeviceControl`	Контроль устройств.
	`ApplicationControl`	Контроль приложений.
	`AdaptiveAnomaliesControl`	Адаптивный контроль аномалий.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Анализ журналов.
	`AntiCryptor`	Защита от шифрования.
	`FileThreatProtection`	Защита от файловых угроз.
	`SystemIntegrityMonitor`	Контроль целостности системы.
	`AntiCryptor`	Защита от шифрования.
	`FileEncryption`	Библиотеки для шифрования файлов.
	`DiskEncryption`	Библиотеки для полнодискового шифрования.
	`MSBitLocker`	Библиотеки для управления шифрованием BitLocker.

Раздел	Параметр	Описание
	`BadUSBAttackPrevention`	Защита от атак BadUSB.
	`EDR`	Endpoint Detection and Response Optimum. Компонент несовместим с компонентами Endpoint Detection and Response Expert (cloud) (`EDRCloud`) и Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`EDRCloud`	Endpoint Detection and Response Expert (cloud). Компонент несовместим с компонентами Endpoint Detection and Response Optimum (`EDR`) и Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises). Компонент несовместим с компонентами Endpoint Detection and Response Expert (cloud) (`EDRCloud`) и Endpoint Detection and Response Optimum (`EDR`).
	`SB`	Kaspersky Sandbox или KATA Sandbox. *Kaspersky Sandbox* – это отдельное решение Detection and Response от "Лаборатории Касперского". *KATA Sandbox* – это компонент решения Kaspersky Anti Targeted Attack Platform.
	`MDR`	Managed Detection and Response.
	`NDR`	Network Detection and Response (KATA). Компонент несовместим с компонентами Endpoint Detection and Response Expert (cloud) (`EDRCloud`) и Endpoint Detection and Response Optimum (`EDR`).
	`AdminKitConnector`	Управление приложением с помощью систем администрирования. К системам администрирования относится, например, Kaspersky Security Center. Кроме систем администрирования "Лаборатории Касперского" вы можете использовать сторонние решения. Для этого Kaspersky Endpoint Security предоставляет API. Возможные значения: • `1` – управление приложением с помощью систем администрирования разрешено (значение по умолчанию). • `0` – разрешено управление приложением только через локальный интерфейс.
	`KUMAIntegration`	Интеграция с KUMA.
	`StandaloneKATA`	Установка приложения в режиме Endpoint Detection and Response агент (EDR-агент) для интеграции с Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Установка приложения в режиме Endpoint Detection and Response агент (EDR-агент) для интеграции с Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Установка приложения в режиме Endpoint Detection and Response агент (EDR-агент) для интеграции с Kaspersky Anti Targeted Attack Platform (NDR)
	`StandaloneSiemTelemetry`	Установка приложения в режиме Endpoint Detection and Response агент (EDR-агент) для интеграции с KUMA.
`[Tasks]`	`ScanMyComputer`	Задача полной проверки. Возможные значения: • `1` – задача включается в список задач Kaspersky Endpoint Security. • `0` – задача не включается в список задач Kaspersky Endpoint Security.
	`ScanCritical`	Задача проверки важных областей. Возможные значения: • `1` – задача включается в список задач Kaspersky Endpoint Security. • `0` – задача не включается в список задач Kaspersky Endpoint Security.

Раздел	Параметр	Описание
	`Updater`	Задача обновления. Возможные значения: • `1` – задача включается в список задач Kaspersky Endpoint Security. • `0` – задача не включается в список задач Kaspersky Endpoint Security.

Процессы Kaspersky Endpoint Security для Windows

Kaspersky Endpoint Security для Windows запускает процессы, описанные в таблице ниже.

Процессы Kaspersky Endpoint Security для Windows

Имя файла	Назначение
avp.exe	Рабочий процесс Kaspersky Endpoint Security для Windows.
avpsus.exe	Процесс позволяет устанавливать и откатывать критические и одобренные обновления модулей приложения.

Изменение состава компонентов приложения

Во время установки приложения вы можете выбрать компоненты, которые будут доступны. Вы можете изменить состав приложения следующими способами:

- Локально с помощью мастера установки приложения.

  Изменение состава приложения выполняется обычным способом, принятым для операционной системы Windows, через Панель управления. Запустите мастер установки приложения и выберите операцию изменения состава компонентов приложения. Следуйте указаниям на экране.

  > Этот способ недоступен, если приложение установлено через Kaspersky Security Center. Вы можете изменить состав компонентов приложения через Панель управления только после локальной установки приложения.

- Удаленно с помощью Kaspersky Security Center.

  Для изменения состава компонентов Kaspersky Endpoint Security после установки приложения предназначена задача *Изменение состава компонентов приложения*.

Изменение состава компонентов приложения имеет следующие особенности:

- На компьютеры под управлением Windows Server можно установить не все компоненты Kaspersky Endpoint Security (например, недоступен компонент Адаптивный контроль аномалий).

- Если на компьютере жесткие диски защищены полнодисковым шифрованием (FDE), удалить компонент Полнодисковое шифрование невозможно. Для удаления компонента Полнодисковое шифрование расшифруйте все жесткие диски компьютера.

- Если на компьютере есть зашифрованные файлы (FLE) или пользователь использует зашифрованные съемные диски (FDE или FLE), после удаления компонентов шифрования данных получить доступ к файлам и съемным дискам будет невозможно. Вы можете получить доступ к файлам и съемным дискам, если переустановите компоненты шифрования данных.

- Если приложение установлено в режиме Легкого агента в инфраструктуре VDI, изменение состава компонентов не поддерживается.

Как добавить или удалить компоненты приложения в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Изменение состава приложения**.

Шаг 2. Параметры задачи изменения компонентов приложения

Выберите конфигурацию приложения:

- **Стандартный режим для защиты устройств**. Конфигурация по умолчанию. В этой конфигурации вам доступны все компоненты приложения, включая компоненты для работы решений Detection and Response. Эта конфигурация нужна для развертывания комплексной защиты компьютера от различного вида угроз, сетевых и мошеннических атак.

- **Агент Endpoint Detection and Response для защиты от сложных угроз и целевых атак**. В этой конфигурации вы можете установить только компоненты для работы решений Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), а также KUMA. Эта конфигурация нужна в том случае, если в вашей организации развернута система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков и решение Detection and Response от "Лаборатории Касперского". Таким образом, Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента может быть совместим со сторонними EPP-приложениями.

  При изменении конфигурации приложения на EDR-агент для работы с MDR убедитесь, что компоненты, обеспечивающие получение телеметрии, включены.

- **Легкий агент для защиты виртуальных сред**. Эта конфигурация предназначена для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Легкий агент должен быть установлен на каждой виртуальной машине, которую требуется защищать с помощью решения. В этой конфигурации недоступны компоненты шифрования данных и Адаптивный контроль аномалий. Если вы устанавливаете Легкий агент на шаблон виртуальных машин, из которого вы будете создавать *временные виртуальные машины*, установите флажок **Защищать инфраструктуру VDI** (Virtual Desktop Infrastructure). Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. В этом режиме Легкий агент отклоняет обновления приложения, требующие перезагрузки виртуальной машины. При получении обновлений приложения, требующих перезагрузки, Легкий агент формирует событие о необходимости обновить шаблон защищенных виртуальных машин.

Выберите компоненты приложения, которые будут доступны на компьютере пользователя.

Шаг 3. Дополнительные настройки

Настройте дополнительные параметры задачи (см. таблицу ниже).

Шаг 4. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 5. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 6. Определение названия задачи

Введите название задачи, например, *Добавление компонента Контроль приложений*.

Шаг 7. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как добавить или удалить компоненты приложения в Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.
2. В раскрывающемся списке **Тип задачи** выберите **Изменение состава компонентов приложения**.
3. В поле **Название задачи** введите короткое описание, например, *Добавление компонента Контроль приложений*.
4. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Например, выберите отдельную группу администрирования или сделайте выборку.

Шаг 3. Завершение создание задачи

Установите флажок **Открыть окно свойств задачи после ее создания** и завершите работу мастера.

В свойствах задачи выберите вкладку **Параметры приложения**. Далее выберите конфигурацию приложения:

- **Стандартный режим для защиты рабочих станций и серверов**. Конфигурация по умолчанию. В этой конфигурации вам доступны все компоненты приложения, включая компоненты для работы решений Detection and Response. Эта конфигурация нужна для развертывания комплексной защиты компьютера от различного вида угроз, сетевых и мошеннических атак.

- **Агент Endpoint Detection and Response для защиты от сложных угроз и целевых атак**. В этой конфигурации вы можете установить только компоненты для работы решений Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), а также KUMA. Эта конфигурация нужна в том случае, если в вашей организации развернута система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков и решение Detection and Response от "Лаборатории Касперского". Таким образом, Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента может быть совместим со сторонними EPP-приложениями.

  При изменении конфигурации приложения на EDR-агент для работы с MDR убедитесь, что компоненты, обеспечивающие получение телеметрии, включены.

- **Легкий агент для защиты виртуальных сред**. Эта конфигурация предназначена для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Легкий агент должен быть установлен на каждой виртуальной машине, которую требуется защищать с помощью решения. В этой конфигурации недоступны компоненты шифрования данных и Адаптивный контроль аномалий. Если вы устанавливаете Легкий агент на шаблон виртуальных машин, из которого вы будете создавать *временные виртуальные машины*, установите флажок **Защищать инфраструктуру VDI** (Virtual Desktop Infrastructure). Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. В этом режиме Легкий агент отклоняет обновления приложения, требующие перезагрузки виртуальной машины. При получении обновлений приложения, требующих перезагрузки, Легкий агент формирует событие о необходимости обновить шаблон защищенных виртуальных машин.

Выберите компоненты приложения, которые будут доступны на компьютере пользователя. Настройте дополнительные параметры задачи (см. таблицу ниже).

В результате на компьютерах пользователей будет изменен состав компонентов Kaspersky Endpoint Security в тихом режиме. В локальном интерфейсе приложения будут отображаться параметры доступных компонентов. Компоненты, которые не вошли в состав приложения, выключены, а параметры этих компонентов недоступны.

При установке, обновлении или удалении Kaspersky Endpoint Security могут возникать ошибки. Подробнее об их решении этих ошибок см. в базе знаний Службы технической поддержки.

Дополнительные параметры задачи

Параметр	Описание
Настройки задачи	**Проверять на наличие несовместимых приложений сторонних производителей**. По умолчанию Kaspersky Endpoint Security проверяет установленные приложения на совместимость. Список ПО, с которым могут быть проблемы совместимости, приведен в файле incompatible.txt. Файл входит в комплект поставки. Если проверка установленного ПО включена, при обнаружении приложения из списка Kaspersky Endpoint Security прекращает выполнение задачи. Вы можете выключить проверку установленного ПО, если поставщик стороннего ПО указал в своей документации совместимость с системами защиты конечных точек (англ. Endpoint Protection Platform, EPP). **Удалять несовместимые приложения сторонних производителей**. Функция автоматического удаления приложений, которые перечислены в файле incompatible.txt, перед изменением состава компонентов. Если функция включена, Kaspersky Endpoint Security пытается удалить приложения, с которыми могут быть проблемы совместимости, для продолжения выполнения задачи. **Использовать режим совместимости с Azure WVD**. Функция позволяет корректно показывать состояние виртуальной машины Azure в консоли Kaspersky Anti Targeted Attack Platform. Для контроля за состоянием компьютера Kaspersky Endpoint Security отправляет на серверы KATA телеметрию. Телеметрия включает в себя идентификатор компьютера (Sensor ID). Режим совместимости с Azure WVD позволяет назначать постоянный уникальный Sensor ID для этих виртуальных машин. Если режим совместимости выключен, то из-за особенностей работы виртуальных машин Azure Sensor ID может изменяться после перезагрузки компьютера. Из-за этого возможно дублирование виртуальных машин в консоли.
Исключения	Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах. Начиная с версии Kaspersky Endpoint Security для Windows 12.8 добавлена установка приложения в режиме Легкого агента для защиты виртуальных сред. Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в виртуальных средах Citrix и VMware. Вы также можете настроить доверенную зону позднее в свойствах политики: исключения из проверки и доверенные приложения.
Раздельный режим / Совмещенный режим	Вы можете создать отдельный набор компонентов для рабочих станций и отдельный набор компонентов для серверов – **Раздельный режим**. Установщик перед развертыванием инсталляционного пакета определяет тип операционной системы и устанавливает только те компоненты приложения, которые вы выбрали для определенного типа операционной системы. Таким образом, вы можете использовать один инсталляционный пакет для рабочих станций и серверов. **Совмещенный режим** предлагает общий список компонентов для рабочих станций и серверов. Набор доступных компонентов зависит от типа операционной системы. В этом режиме рекомендуется создавать отдельный инсталляционный пакет для рабочих станций и отдельный инсталляционный пакет для серверов. Настройка общего списка компонентов в инсталляционном пакете доступна только для Стандартного режима.
Использовать пароль для изменения состава компонентов	Как правило, для ограничения доступа к Kaspersky Endpoint Security администраторы включают Защиту паролем. То есть для изменения состава компонентов приложения вам нужно ввести учетные данные пользователя с разрешением **Удаление / изменение / восстановление приложения**. Например, вы можете использовать учетную запись KLAdmin.
Использовать пароль для удаления Kaspersky Endpoint Agent и Kaspersky Security для Windows Server	Как правило, для ограничения доступа к Kaspersky Endpoint Agent (KEA) и Kaspersky Security для Windows Server (KSWS) администраторы включают Защиту паролем в параметрах этих задач. То есть, если вы мигрируете с конфигурации [KES+KEA] на [KES+встроенный агент], или вы мигрируете с KSWS на KES, вам нужно ввести пароль для удаления этих программ.

Обновление предыдущей версии приложения

Обновление предыдущей версии приложения имеет следующие особенности:

- Перед началом обновления приложения рекомендуется закрыть все работающие приложения.
- Перед обновлением Kaspersky Endpoint Security блокирует функциональность полнодискового шифрования. Если функциональность полнодискового шифрования не удалось заблокировать, установка обновления не начнется. После обновления приложения функциональность полнодискового шифрования будет восстановлена.
- Для смены языка приложения необходимо выбрать в задаче *Удаленная установка приложения* инсталляционный пакет с нужной локализацией и обновить приложение. Смена языка приложения доступна начиная с версии Kaspersky Endpoint Security для Windows 14.2.

Kaspersky Endpoint Security поддерживает обновление следующих версий приложения:

- Kaspersky Endpoint Security для Windows 12.3 (сборка 12.3.0.493).
- Kaspersky Endpoint Security для Windows 12.4 (сборка 12.4.0.467).
- Kaspersky Endpoint Security для Windows 12.5 (сборка 12.5.0.539).
- Kaspersky Endpoint Security для Windows 12.6 (сборка 12.6.0.438).
- Kaspersky Endpoint Security для Windows 12.7 (сборка 12.7.0.533).
- Kaspersky Endpoint Security для Windows 12.8 (сборка 12.8.0.505).
- Kaspersky Endpoint Security для Windows 12.9 (сборка 12.9.0.384).
- Kaspersky Endpoint Security для Windows 12.10 (сборка 12.10.0.466).
- Kaspersky Endpoint Security для Windows 12.11 (сборка 12.11.0.637).
- Kaspersky Endpoint Security для Windows 12.12 (сборка 12.12.0.522).
- Kaspersky Endpoint Security для Windows 14.0 (сборка 14.0.0.504).
- Kaspersky Endpoint Security для Windows 14.1 (сборка 14.1.0.423).
- Kaspersky Endpoint Security для Windows 14.2 (сборка 14.2.0.536).

При установке, обновлении или удалении Kaspersky Endpoint Security могут возникать ошибки. Подробнее об их решении этих ошибок см. в базе знаний Службы технической поддержки.

Способы обновления версии приложения

Приложение Kaspersky Endpoint Security может быть обновлено на компьютере следующими способами:

- Через службу обновлений "Лаборатории Касперского" (Seamless Update – SMU).
- Локально с помощью мастера установки приложения.
- Локально из командной строки.
- Удаленно с помощью Kaspersky Security Center.
- Удаленно через редактор управления групповыми политиками Microsoft Windows (подробнее см. на сайте Службы технической поддержки Microsoft).
- Удаленно с помощью System Center Configuration Manager.

Если в сети организации развернуто приложение с набором компонентов, отличным от набора по умолчанию, обновление приложения через Консоль администрирования (MMC) отличается от обновления приложения через Web Console. Обновление Kaspersky Endpoint Security имеет следующие особенности:

- Kaspersky Security Center Web Console.

  Если вы создали инсталляционный пакет новой версии приложения с набором компонентов по умолчанию, после обновления набор компонентов на компьютере пользователя не будет изменен. Для использования Kaspersky Endpoint Security с набором компонентов по умолчанию нужно открыть свойства инсталляционного пакета, изменить набор компонентов, вернуть набор компонентов в исходное состояние и сохранить изменения.

- Консоль администрирования Kaspersky Security Center.

  Набор компонентов приложения после обновления будет соответствовать набору компонентов в инсталляционном пакете. То есть, если новая версия приложения имеет набор компонентов по умолчанию, то, например, встроенный агент MDR будет удален с компьютера, так как этот компонент исключен из набора по умолчанию. Для продолжения использования приложения с прежним набором компонентов нужно выбрать необходимые компоненты в параметрах инсталляционного пакета.

Обновление приложения без перезагрузки

Обновление приложения без перезагрузки позволяет обеспечить бесперебойную работу серверов при обновлении версии приложения.

Обновление приложения без перезагрузки имеет следующие ограничения:

- Вы можете обновлять версию приложения без перезагрузки начиная с версии 11.10.0. Для обновление более ранних версий приложения необходимо выполнять перезагрузку компьютера.
- Вы можете устанавливать патчи без перезагрузки начиная с версии 11.11.0. Для установки патчей для более ранних версий приложения может потребоваться перезагрузка компьютера.

- Обновление версии приложения без перезагрузки невозможно выполнить на компьютерах с включенным шифрованием данных (Шифрование Kaspersky (FDE), BitLocker, Шифрование файлов (FLE). Для обновления версии приложения на компьютерах с включенным шифрованием данных необходимо выполнять перезагрузку компьютера.
- Обновление версии приложения без перезагрузки невозможно выполнить на виртуальных машинах. Для обновления версии приложения на виртуальных машинах необходимо выполнять перезагрузку виртуальной машины.

После обновления приложения, установки патча, изменения состава компонентов приложения или восстановления приложение Kaspersky Endpoint Security выполняет перезапуск для перехода на новую версию. Перезапуск Kaspersky Endpoint Security может занять до одной минуты. В течение этого времени уровень защиты компьютера снижен. После перезапуска приложения уровень защиты компьютера будет восстановлен.

Как выбрать режим обновления приложения в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Общие настройки** → **Настройки приложения**.
5. В блоке **Дополнительные настройки** с помощью флажка **Устанавливать обновления приложения без перезагрузки** настройте режим обновления приложения.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как выбрать режим обновления приложения в Web Console

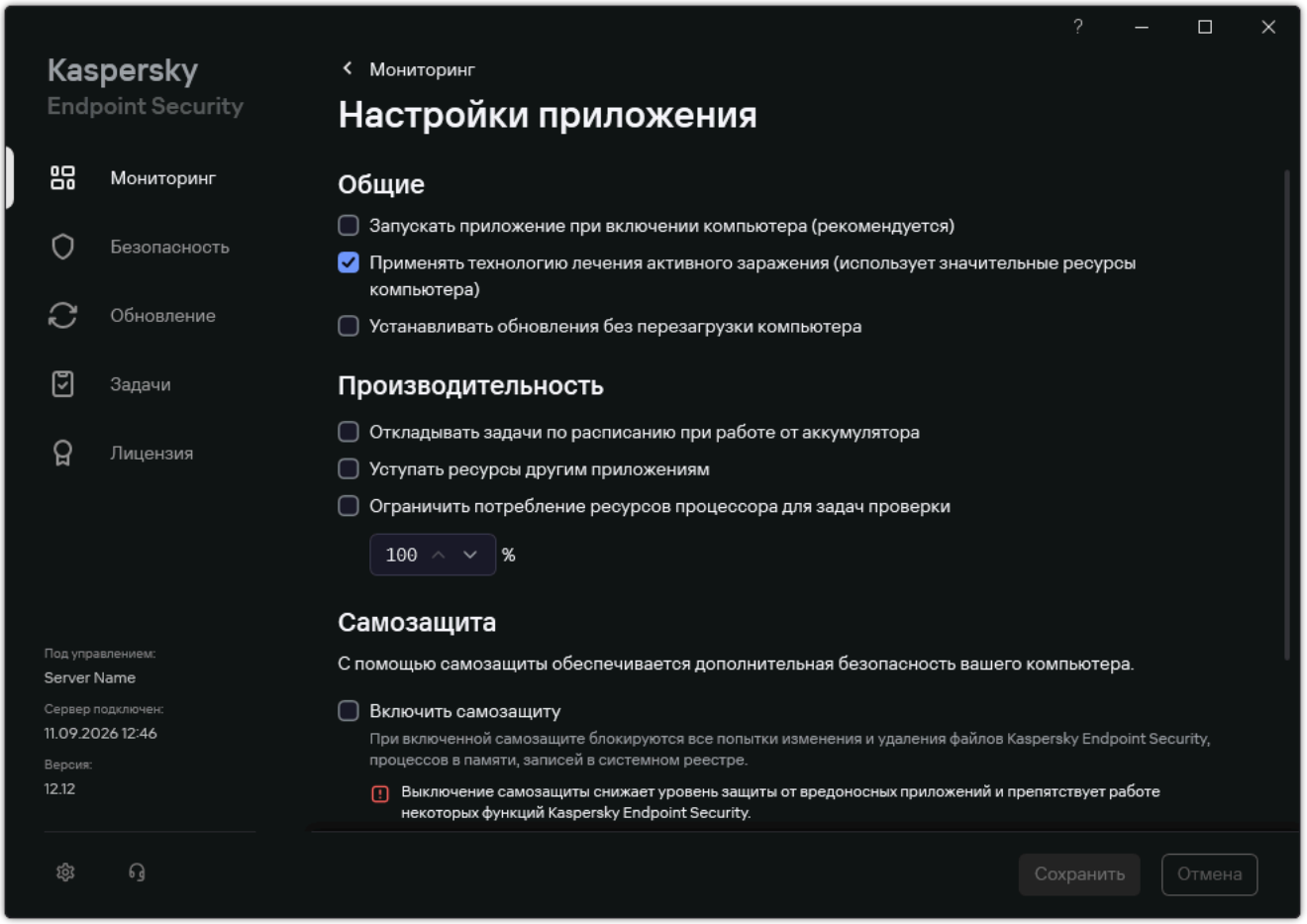
1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Взаимодействие с пользователем**.
5. В блоке **Настройки обновления приложения** с помощью флажка **Устанавливать обновления приложения без перезагрузки** настройте режим обновления приложения.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как выбрать режим обновления приложения в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.



Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Общие** с помощью флажка **Устанавливать обновления без перезагрузки компьютера** настройте режим обновления приложения.

4. Сохраните внесенные изменения.

Также вы можете выбрать режим обновления версии приложения при установке приложения из командной строки (параметр `UPGRADEMODE`).

После завершения процесса обновления версии приложения без перезагрузки на компьютер будет установлена новая версия Kaspersky Endpoint Security. Предыдущая версия приложения будет удалена автоматически.

Невозможно запустить обновление версии приложения до полного завершения предыдущего процесса обновления.

Вы можете проверить статус обновления Kaspersky Endpoint Security с помощью отчета о версиях программ "Лаборатории Касперского" в консоли Kaspersky Security Center.

SMU-обновление приложения

Для обновления версии приложения через службу обновлений "Лаборатории Касперского" (Seamless Update – SMU) не нужно запускать инсталлятор в отличии от других способов обновления. Kaspersky Endpoint Security получает новую версию приложения вместе с антивирусными базами из того же источника.

SMU-обновление позволяет обновить версию приложения на всех компьютерах организации до последней версии. Перед SMU-обновлением рекомендуется проверить новую версию приложения на нескольких компьютерах. Для этого вам нужно обновить версию приложения на компьютерах вручную (например, локально с помощью с помощью мастера установки приложения). Выбрать отдельные компьютеры для SMU-обновления приложения невозможно.

Расписание обновления приложения устанавливают специалисты "Лаборатории Касперского". Для проверки работы новой версии приложения специалисты "Лаборатории Касперского" распространяют обновления поэтапно. В результате вы можете получить SMU-обновление с задержкой до двух месяцев после выпуска новой версии.

Управление SMU-обновлением приложения осуществляется с помощью задачи *Обновление баз и модулей приложения*. Для включения новой версии приложения в один пакет с антивирусными базами вам нужно включить обновление *модулей приложения* в параметрах задачи *Обновление баз и модулей приложения*. Также в параметрах задачи *Обновление баз и модулей приложения* вы можете включить режим обновления приложения без перезагрузки.

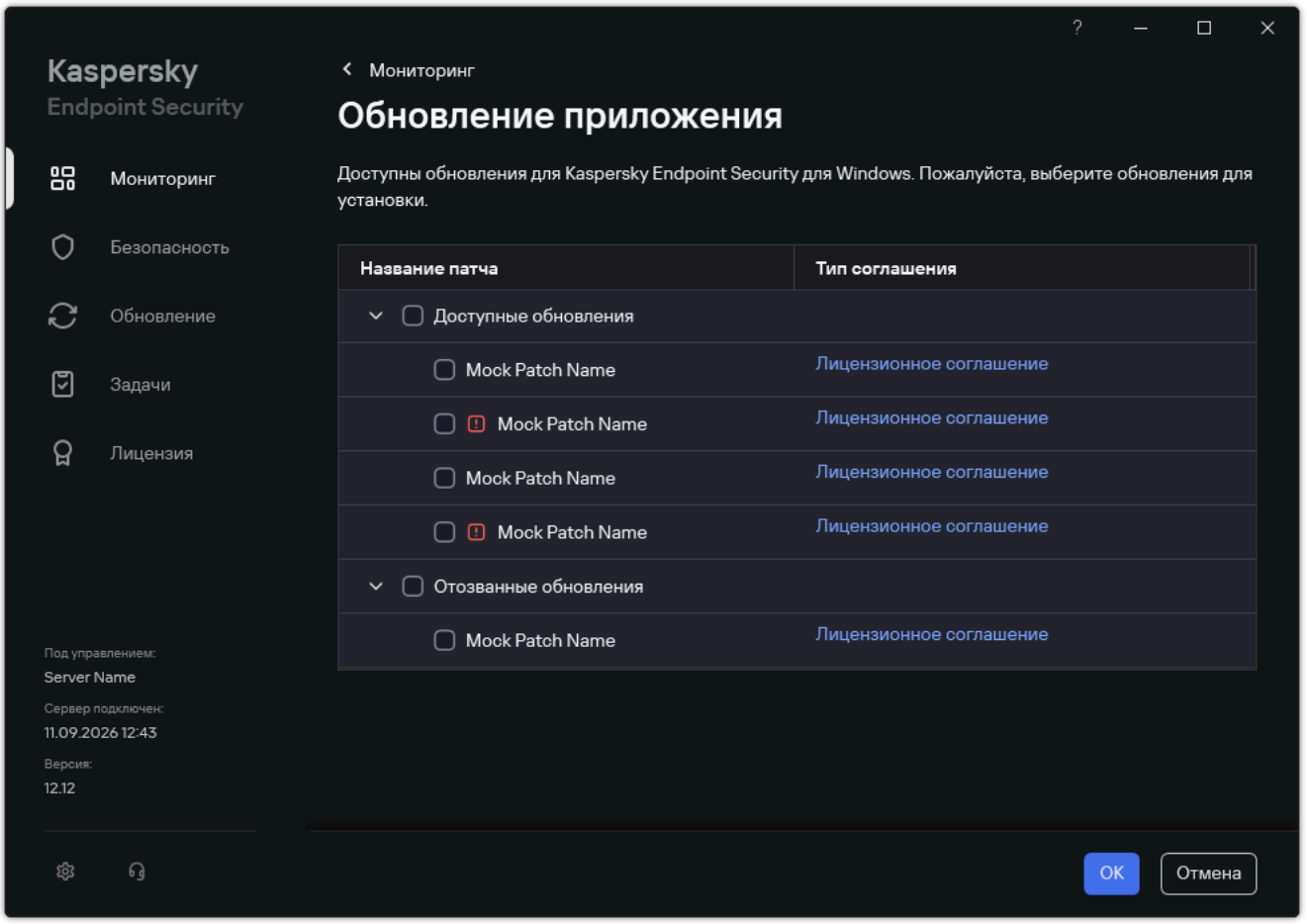
Этапы SMU-обновления приложения

1. **После выпуска новой версии приложение "Лаборатория Касперского" распространяет обновление.**
2. **Пользователь одобряет обновление приложения.**

   Если компьютер подключен к Kaspersky Security Center, обновление будет доступно в консоли Kaspersky Security Center в разделе **Обновление баз и программных модулей "Лаборатории Касперского"**. Подробнее об одобрении обновлений см. в справке Kaspersky Security Center.

   Если компьютер не подключен к Kaspersky Security Center, обновление будет доступно в интерфейсе приложения в разделе уведомлений – . Для одобрения обновления вам нужно выбрать версию приложения и принять условия соглашений (см. рис. ниже).
3. **Kaspersky Endpoint Security запускает задачу *Обновление баз и модулей приложения* по заданному расписанию.**

В результате Kaspersky Endpoint Security выполняет обновление версии приложения в "тихом" режиме.



Доступные обновления для приложения

Удаление приложения

В результате удаления Kaspersky Endpoint Security компьютер и данные пользователя окажутся незащищенными.

При установке, обновлении или удалении Kaspersky Endpoint Security могут возникать ошибки. Подробнее об их решении этих ошибок см. в базе знаний Службы технической поддержки.

Дистанционное удаление приложения с помощью Kaspersky Security Center

Вы можете удалить приложение дистанционно с помощью задачи *Удаленная деинсталляция приложения*. При выполнении задачи Kaspersky Endpoint Security загрузит на компьютер пользователя утилиту для удаления приложения. После завершения удаления приложения, утилита будет удалена автоматически.

Как удалить приложение через Консоль администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.

   Откроется список задач.
3. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Сервер администрирования Kaspersky Security Center → Дополнительно → Удаленная деинсталляция приложения**.

Шаг 2. Выбор удаляемого приложения

Выберите **Удалить приложение, поддерживаемое Kaspersky Security Center**.

Шаг 3. Параметры задачи удаления приложения

Выберите **Kaspersky Endpoint Security для Windows (14.3)**.

Шаг 4. Параметры утилиты деинсталляции

Настройте следующие дополнительные параметры приложения:

- **Принудительно скачать утилиту деинсталляции**. Выберите средства доставки утилиты:
  - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security удаляется средствами Агента администрирования.
  - **Средствами операционной системы с помощью Сервера администрирования**. Доставка утилиты на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.
  - **Средствами операционной системы с помощью точек распространения**. Утилита передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.
- **Предварительно проверять тип операционной системы перед загрузкой**. Если требуется, снимите этот флажок. Это позволит избежать загрузки утилиты деинсталляции, если операционная система компьютера не соответствует программным требованиям. Если вы уверены, что операционная система компьютеров соответствует программным требованиям, проверку можно пропустить.

Если операция удаления приложения защищена паролем, выполните следующие действия:

1. Установите флажок **Использовать пароль деинсталляции**.
2. Нажмите на кнопку **Изменить**.
3. Введите пароль учетной записи KLAdmin.

Шаг 5. Выбор параметра перезагрузки операционной системы

После удаления приложения требуется перезагрузка. Выберите действие, которое будет выполняться для перезагрузки компьютера.

Шаг 6. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, — *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 7. Выбор учетной записи для запуска задачи

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для удаления Kaspersky Endpoint Security средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 8. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 9. Определение названия задачи

Введите название задачи, например, *Удаление Kaspersky Endpoint Security 14.3*.

Шаг 10. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Удаление приложения будет выполнено в тихом режиме.

Как удалить приложение через Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Приложение** выберите **Kaspersky Security Center**.
2. В раскрывающемся списке **Тип задачи** выберите **Удаленная деинсталляция приложения**.
3. В поле **Название задачи** введите короткое описание, например, *Удаление Kaspersky Endpoint Security на компьютерах Службы технической поддержки*.
4. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Например, выберите отдельную группу администрирования или сделайте выборку.

Шаг 3. Настройка параметров удаления приложения

На этом шаге настройте параметры удаления приложения:

1. Выберите тип **Удалить управляемое приложение**.
2. Выберите **Kaspersky Endpoint Security для Windows**.

3. **Принудительно скачать утилиту деинсталляции**. Выберите средства доставки утилиты:

   - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Endpoint Security удаляется средствами Агента администрирования.

   - **Средствами операционной системы с помощью Сервера администрирования**. Доставка утилиты на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

   - **Средствами операционной системы с помощью точек распространения**. Утилита передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.

4. В поле **Максимальное количество одновременных загрузок** установите ограничение количества запросов к Серверу администрирования для загрузки утилиты для удаления приложения. Ограничение запросов позволит избежать перегрузки сети.

5. В поле **Максимальное количество попыток деинсталляции** установите ограничение попыток удалить приложение. Если удаление Kaspersky Endpoint Security завершается с ошибкой, задача автоматически запускает удаление повторно.

6. Если требуется, снимите флажок **Предварительно проверять тип операционной системы перед загрузкой**. Это позволит избежать загрузки утилиты деинсталляции, если операционная система компьютера не соответствует программным требованиям. Если вы уверены, что операционная система компьютеров соответствует программным требованиям, проверку можно пропустить.

Шаг 4. Выбор учетной записи для запуска задачи

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для удаления Kaspersky Endpoint Security средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 5. Завершение создания задачи

Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача.

Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку **Запустить**. Удаление приложения будет выполнено в тихом режиме. После завершения удаления Kaspersky Endpoint Security покажет запрос на перезагрузку компьютера.

Если операция удаления приложения защищена паролем, введите пароль учетной записи KLAdmin в свойствах задачи *Удаленная деинсталляция программы*. Без пароля задача не будет выполнена.

Чтобы использовать пароль учетной записи KLAdmin в задаче Удаленная деинсталляция программы, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Security Center **Удаленная деинсталляция приложения**.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. Установите флажок **Использовать пароль деинсталляции**.

5. Введите пароль учетной записи KLAdmin.

6. Сохраните внесенные изменения.

Для завершения удаления приложения необходимо перезагрузить компьютер. Для этого Агент администрирования покажет пользователю всплывающее окно.

Дистанционное удаление приложения с помощью Active Directory

Вы можете удалить приложение дистанционно с помощью политики Microsoft Windows. Для удаления приложения вам нужно открыть Консоль управления групповой политикой (gpmc.msc) и в редакторе управления групповыми политиками создать задачу удаления приложения (подробнее см. на сайте Службы технической поддержки Microsoft).

Если операция удаления приложения защищена паролем, вам нужно выполнить следующие действия:

1. Создайте bat-файл со следующим содержанием:

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   где `<GUID>` – уникальный идентификатор приложения. Вы можете узнать GUID приложения в базе знаний Службы технической поддержки или с помощью команды:

   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
   ```

   Пример

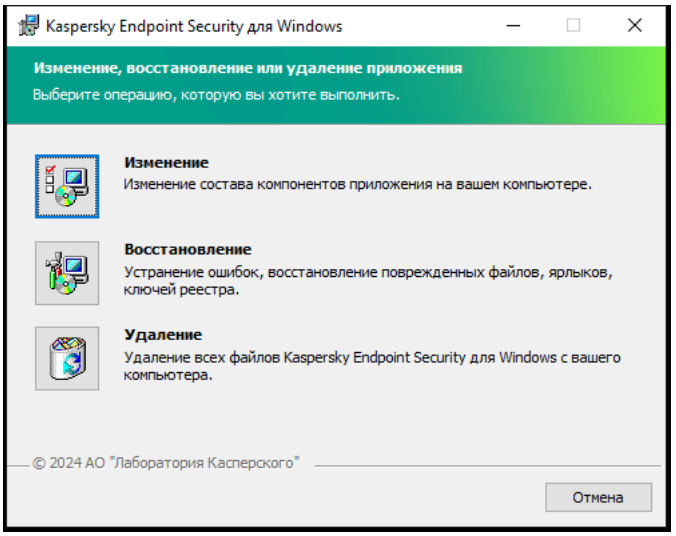
   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. Создайте новую политику Microsoft Windows для компьютеров в Консоли управления групповой политикой (gpmc.msc).

3. Запустите созданный bat-файл на компьютерах с помощью новой политики.

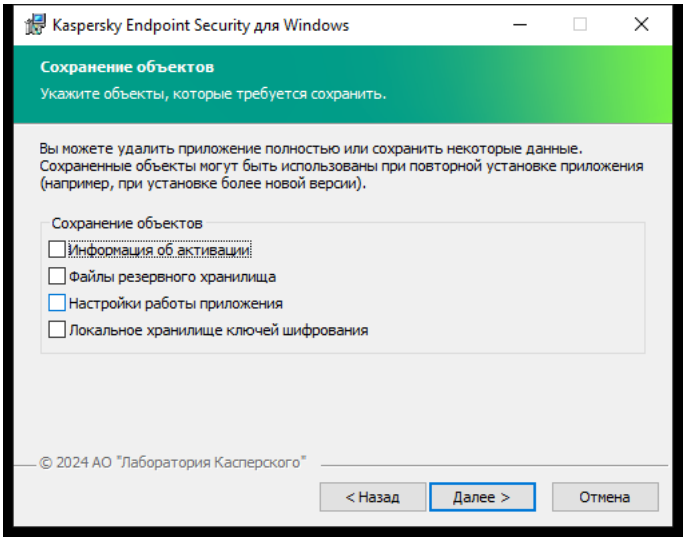
Локальное удаление приложения

Вы можете удалить приложение локально с помощью мастера установки приложения. Удаление Kaspersky Endpoint Security выполняется обычным способом, принятым для операционной системы Windows, через Панель управления. Запустится мастер установки приложения. Следуйте указаниям на экране.



Выбор операции удаления приложения

Вы можете указать, какие используемые приложением данные вы хотите сохранить для дальнейшего использования при повторной установке приложения (например, ее более новой версии). Если вы не укажете никаких данных, приложение будет удалено полностью (см. рис. ниже).



Сохранение данных после удаления

Вы можете сохранить следующие данные:

- **Информация об активации** – данные, позволяющие в дальнейшем не активировать приложение повторно. Kaspersky Endpoint Security автоматически добавляет лицензионный ключ, если срок действия лицензии не истек к моменту установки.

- **Файлы резервного хранилища** – файлы, проверенные приложением и помещенные в резервное хранилище.

Доступ к файлам резервного хранилища, сохраненным после удаления приложения, возможен только из той же версии приложения, в которой они были сохранены.

Если вы планируете использовать объекты резервного хранилища после удаления приложения, вам нужно восстановить их до удаления приложения. Однако эксперты "Лаборатории Касперского" не рекомендуют восстанавливать объекты из резервного хранилища, так как это может нанести вред компьютеру.

- **Настройки работы приложения** – значения параметров работы приложения, установленные в процессе ее настройки.
- **Локальное хранилище ключей шифрования** – данные, которые обеспечивают доступ к зашифрованным до удаления приложения файлам и дискам. Для доступа к зашифрованным файлам и дискам убедитесь, что вы выбрали функциональность шифрования данных при повторной установке Kaspersky Endpoint Security. Дополнительных действий для доступа к зашифрованным раннее файлам и дискам выполнять не требуется.

Kaspersky Endpoint Security сохраняет данные в папку `C:\ProgramData\Kaspersky Lab\KES.14.3\QB`.

Вы также можете удалить приложение локально из командной строки.

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения Kaspersky Endpoint Security.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать приложение.

Рекомендуется внимательно ознакомиться с условиями Лицензионного соглашения перед началом работы с приложением.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Endpoint Security в интерактивном режиме.
- Прочитав документ license.txt. Этот документ включен в комплект поставки приложения, а также находится в папке установки приложения `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES`.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки приложения. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку приложения.

О лицензии

Лицензия – это ограниченное по времени право на использование приложения, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на использование приложения в соответствии с условиями Лицензионного соглашения, а также получение технической поддержки. Список доступных функций и срок использования приложения зависят от типа лицензии, по которой было активировано приложение.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с приложением.

  Пробная лицензия обычно имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Endpoint Security прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать приложение по пробной лицензии только один раз. Активировать приложение по пробной лицензии после активной коммерческой лицензии невозможно.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении приложения.

Функциональность приложения, доступная по коммерческой лицензии, зависит от выбора продукта. Выбранный продукт указан в Лицензионном сертификате. Информацию о доступных продуктах вы можете найти на сайте "Лаборатории Касперского".

По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы приложения вам нужно продлить лицензию. Если вы не планируете продлевать лицензию, удалите приложение с компьютера.

О Лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- идентификатор лицензии или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о приложении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О подписке

Подписка на Kaspersky Endpoint Security – это заказ на использование приложения с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Endpoint Security можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме или отказаться от нее. Управление подпиской доступно на веб-сайте поставщика услуг.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Endpoint Security после истечения ограниченной подписки вам нужно ее продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность приложения сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Endpoint Security по подписке, вам нужно применить код активации, предоставленный поставщиком услуг. После применения кода активации добавляется активный ключ, определяющий лицензию на использование приложения по подписке. Активировать приложение по подписке с помощью файла ключа невозможно. Поставщик услуг может предоставить только код активации. Добавить резервный ключ по подписке невозможно.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Endpoint Security.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения.

Для ключа, добавленного по подписке, Лицензионный сертификат не предоставляется.

Вы можете добавить лицензионный ключ в приложение одним из следующих способов: применить файл ключа или ввести код активации.

Ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если ключ заблокирован, для обеспечения работы приложения вам нужно добавить другой ключ.

Ключ может быть активным и резервным.

Активный ключ – ключ, используемый в текущий момент для работы приложения. В качестве активного ключа может быть добавлен ключ для пробной или коммерческой лицензии. В приложении не может быть больше одного активного ключа.

Резервный ключ – ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. По истечении срока годности активного ключа резервный ключ автоматически становится активным. Резервный ключ может быть добавлен только при наличии активного ключа.

Ключ для пробной лицензии может быть добавлен только в качестве активного ключа. Он не может быть добавлен в качестве резервного ключа. Ключ для пробной лицензии не может заменить активный ключ для коммерческой лицензии.

Если ключ попадает в список запрещенных ключей, в течение восьми дней доступна функциональность приложения, определенная лицензией, по которой приложение активировано. Приложение уведомляет пользователя о том, что ключ помещен в список запрещенных ключей. По истечении восьми дней функциональность приложения соответствует ситуации, когда истекает срок действия лицензии. Вы можете использовать компоненты защиты и контроля и выполнять проверку на основе баз приложения, установленных до истечения срока действия лицензии. Кроме того, приложение продолжает шифровать изменяющиеся файлы, зашифрованные до истечения срока действия лицензии, но не шифрует новые файлы. Использование Kaspersky Security Network недоступно.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Endpoint Security. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Security.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

При активации приложения с помощью кода активации добавляется активный ключ. При этом резервный ключ может быть добавлен только с помощью кода активации и не может быть добавлен с помощью файла ключа.

Если код активации был потерян после активации приложения, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Если код активации был потерян после активации приложения, свяжитесь с партнером "Лаборатории Касперского", у которого вы приобрели лицензию.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего приложение.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Security или после заказа пробной версии Kaspersky Endpoint Security.

Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации.
- Получить файл ключа с другого Сервера администрирования.

При активации приложения с помощью файла ключа добавляется активный ключ. При этом резервный ключ может быть добавлен только с помощью файла ключа и не может быть добавлен с помощью кода активации.

Сравнение функций приложения в зависимости от типа лицензии для рабочих станций

Набор доступных функций Kaspersky Endpoint Security на рабочих станциях зависят от типа лицензии (см. таблицу ниже).

См. также сравнение функций приложения для серверов

Сравнение функций приложения для вариантов лицензий Kaspersky Next см. в справке Kaspersky Next.

Сравнение функций Kaspersky Endpoint Security

Функция	Kaspersky Endpoint Security для бизнеса Стандартный	Kaspersky Endpoint Security для бизнеса Расширенный	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Security для виртуальных и облачных сред Standard	Kaspersky Security для виртуальных и облачных сред Enterprise
Продвинутая защита								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Анализ поведения	✓	✓	✓	✓	✓	✓	✓	✓
Защита от шифрования	✓	✓	✓	✓	✓	✓	✓	✓
Защита от эксплойтов	✓	✓	✓	✓	✓	✓	✓	✓
Предотвращение вторжений	✓	✓	✓	✓	✓	✓	✓	✓
Откат вредоносных действий	✓	✓	✓	✓	✓	✓	✓	✓
Базовая защита								
Защита от файловых угроз	✓	✓	✓	✓	✓	✓	✓	✓
Защита от веб-угроз	✓	✓	✓	✓	✓	✓	✓	✓
Защита от почтовых угроз	✓	✓	✓	✓	✓	✓	✓	✓
Сетевой экран	✓	✓	✓	✓	✓	✓	✓	✓
Защита от сетевых угроз	✓	✓	✓	✓	✓	✓	✓	✓
Защита от атак BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
AMSI-защита	✓	✓	✓	✓	✓	✓	✓	✓
Контроль безопасности								
Анализ журналов	–	–	–	–	–	–	–	–

Функция	Kaspersky Endpoint Security для бизнеса Стандартный	Kaspersky Endpoint Security для бизнеса Расширенный	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Security для виртуальных и облачных сред Standard	Kaspersky Security для виртуальных и облачных сред Enterprise
Контроль приложений	✓	✓	✓	✓	✓	✓	✓	✓
Контроль устройств	✓	✓	✓	✓	✓	✓	✓	✓
Веб-Контроль	✓	✓	✓	✓	✓	✓	✓	✓
Адаптивный контроль аномалий	–	✓	✓	✓	✓	✓	–	✓
Контроль целостности системы	–	–	–	–	–	–	–	–
Шифрование данных								
Шифрование диска Kaspersky	–	✓	✓	✓	✓	✓	–	✓
Шифрование диска BitLocker	–	✓	✓	✓	✓	✓	–	✓
Шифрование файлов	–	✓	✓	✓	✓	✓	–	✓
Шифрование съемных дисков	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(лицензию на Kaspersky Sandbox нужно приобрести отдельно)*	✓	✓	✓	✓	✓	✓	✓	✓
Интеграция с KUMA *(лицензию на интеграцию с KUMA нужно приобрести отдельно)*	✓	✓	✓	✓	✓	✓	✓	✓
Режим Легкого агента *(для активации приложения вам нужно добавить лицензионный ключ на SVM, к которому подключен Легкий агент)*	–	–	–	–	–	–	✓	✓

Сравнение функций приложения в зависимости от типа лицензии для серверов

Набор доступных функций Kaspersky Endpoint Security на серверах зависит от типа лицензии (см. таблицу ниже).

См. также сравнение функций приложения для рабочих станций

Сравнение функций приложения для вариантов лицензий Kaspersky Next см. в справке Kaspersky Next.

Сравнение функций Kaspersky Endpoint Security

Функция	Kaspersky Endpoint Security для бизнеса Стандартный	Kaspersky Endpoint Security для бизнеса Расширенный	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Security для виртуальных и облачных сред Standard	Kaspersky Security для виртуальных и облачных сред Enterprise
Продвинутая защита								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Анализ поведения	✓	✓	✓	✓	✓	✓	✓	✓
Защита от шифрования	✓	✓	✓	✓	✓	✓	✓	✓
Защита от эксплойтов	✓	✓	✓	✓	✓	✓	✓	✓
Предотвращение вторжений	–	–	–	–	–	–	–	–
Откат вредоносных действий	✓	✓	✓	✓	✓	✓	✓	✓
Базовая защита								
Защита от файловых угроз	✓	✓	✓	✓	✓	✓	✓	✓
Защита от веб-угроз	–	✓	✓	✓	✓	✓	✓	✓
Защита от почтовых угроз	–	✓	✓	✓	✓	✓	✓	✓
Сетевой экран	✓	✓	✓	✓	✓	✓	✓	✓
Защита от сетевых угроз	✓	✓	✓	✓	✓	✓	✓	✓
Защита от атак BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
AMSI-защита	✓	✓	✓	✓	✓	✓	✓	✓
Контроль безопасности								
Анализ журналов	–	–	–	–	–	–	–	✓

Функция	Kaspersky Endpoint Security для бизнеса Стандартный	Kaspersky Endpoint Security для бизнеса Расширенный	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Security для виртуальных и облачных сред Standard	Kaspersky Security для виртуальных и облачных сред Enterprise
Контроль приложений	–	✓	✓	✓	✓	✓	–	✓
Контроль устройств	–	✓	✓	✓	✓	✓	✓	✓
Веб-Контроль	–	✓	✓	✓	✓	✓	✓	✓
Адаптивный контроль аномалий	–	–	–	–	–	–	–	–
Контроль целостности системы	–	–	–	–	–	–	–	✓
Шифрование данных								
Шифрование диска Kaspersky	–	–	–	–	–	–	–	–
Шифрование диска BitLocker	–	✓	✓	✓	✓	✓	–	✓
Шифрование файлов	–	–	–	–	–	–	–	–
Шифрование съемных дисков	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(лицензию на Kaspersky Sandbox нужно приобрести отдельно)*	✓	✓	✓	✓	✓	✓	✓	✓
Интеграция с KUMA *(лицензию на интеграцию с KUMA нужно приобрести отдельно)*	✓	✓	✓	✓	✓	✓	✓	✓
Режим Легкого агента *(для активации приложения вам нужно добавить лицензионный ключ на SVM, к которому подключен Легкий агент)*	–	–	–	–	–	–	✓	✓

Активация приложения

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии приложения в течение срока действия лицензии. Активация приложения заключается в добавлении лицензионного ключа.

Вы можете активировать приложение одним из следующих способов:

- Локально из интерфейса приложения с помощью мастера активации приложения. Этим способом вы можете добавить и активный, и резервный ключ.
- Удаленно с помощью программного комплекса Kaspersky Security Center:
  - С помощью задачи *Добавление ключа*.

    Этот способ позволяет добавить ключ на конкретный компьютер или компьютеры, входящие в группу администрирования. Этим способом вы можете добавить и активный, и резервный ключ.
  - Путем распространения на компьютеры ключа, размещенного на Сервере администрирования Kaspersky Security Center.

    Этот способ позволяет автоматически добавлять ключ на компьютеры, уже подключенные к Kaspersky Security Center, а также на новые компьютеры. Для использования этого способа вам нужно сначала добавить ключ на Сервер администрирования Kaspersky Security Center. Подробнее о добавлении ключей на Сервер администрирования Kaspersky Security Center см. в справке Kaspersky Security Center.

    Код активации, приобретенный по подписке, распространяется в первую очередь.
  - Путем добавления ключа в инсталляционный пакет Kaspersky Endpoint Security.

    Этот способ позволяет добавить ключ в свойствах инсталляционного пакета при развертывании Kaspersky Endpoint Security. Приложение будет активировано автоматически после установки.
- С помощью командной строки.

Во время активации приложения, удаленно или во время установки приложения в тихом режиме, с помощью кода активации возможна произвольная задержка, связанная с распределением нагрузки на серверы активации "Лаборатории Касперского". Если требуется немедленная активация приложения, вы можете прервать выполняющуюся активацию и запустить активацию приложения с помощью мастера активации приложения.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, отдельно активировать приложение не требуется.

Активация приложения

Как активировать приложение в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Добавление ключа**.

Шаг 2. Добавление ключа

Введите код активации или выберите файл ключа.

Подробнее о добавлении ключей в хранилище Kaspersky Security Center см. в справке Kaspersky Security Center.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 5. Определение названия задачи

Введите название задачи, например, *Активация Kaspersky Endpoint Security для Windows*.

Шаг 6. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи. В результате на компьютерах пользователей будет активировано приложение Kaspersky Endpoint Security в тихом режиме.

Как активировать приложение в Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.
2. В раскрывающемся списке **Тип задачи** выберите **Добавление ключа**.
3. В поле **Название задачи** введите короткое описание, например, *Активация Kaspersky Endpoint Security для Windows*.
4. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи. Перейдите к следующему шагу.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 3. Выбор лицензии

Выберите лицензию, по которой вы хотите активировать приложение. Перейдите к следующему шагу.

Вы можете добавлять ключи в Web Console (**Операции** → **Лицензирование**).

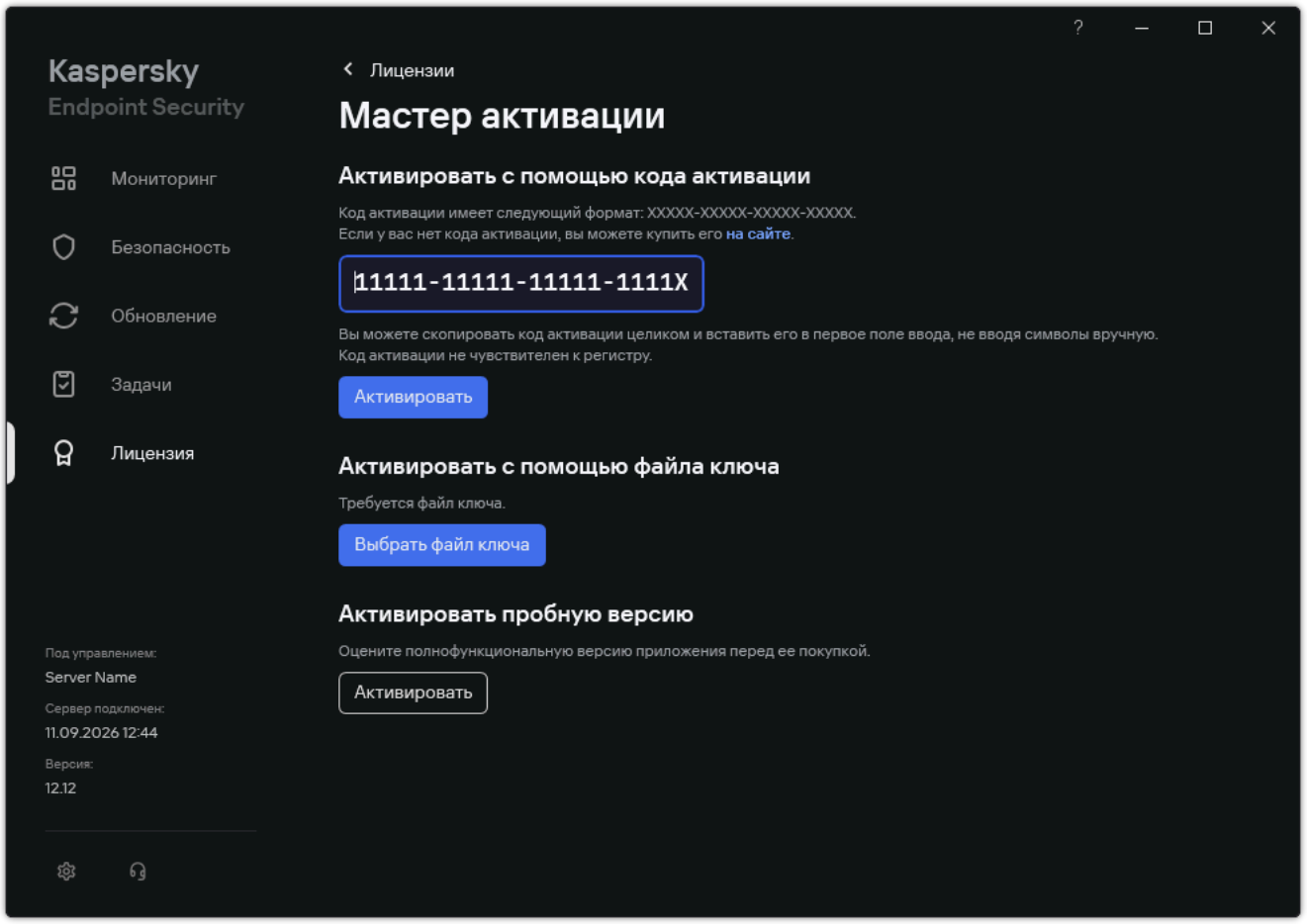
Шаг 4. Завершение создания задачи

Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача. Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку **Запустить**. В результате на компьютерах пользователей будет активировано приложение Kaspersky Endpoint Security в тихом режиме.

Как активировать приложение в интерфейсе приложения

1. В главном окне приложения перейдите в раздел **Лицензия**.
2. Нажмите на кнопку **Активировать приложение по новой лицензии**.

Запустится мастер активации приложения. Следуйте указаниям мастера активации приложения.



Активация приложения

В свойствах задачи *Добавление ключа* вы можете добавить на компьютер резервный ключ. *Резервный ключ* становится активным по истечении срока годности активного ключа. Наличие резервного ключа позволяет избежать ограничения функциональности приложения в момент окончания срока действия лицензии.

Как автоматически добавить лицензионный ключ на компьютеры через Консоль администрирования (MMC)

1. В Консоли администрирования перейдите в папку **Лицензии "Лаборатории Касперского"**.

   Откроется список лицензионных ключей.

2. Откройте свойства лицензионного ключа.

3. В разделе **Общие** установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**.

4. Сохраните внесенные изменения.

   В результате ключ будет автоматически распространяться на компьютеры, для которых он подходит. При автоматическом распространении ключа в качестве активного или резервного учитывается лицензионное ограничение на количество компьютеров, заданное в свойствах ключа. Если лицензионное ограничение достигнуто, распространение ключа на компьютеры автоматически прекращается. Вы можете просмотреть количество компьютеров, на которые добавлен ключ, и другие данные в свойствах ключа в разделе **Устройства**.

Как автоматически добавить лицензионный ключ на компьютеры через Web Console

1. В главном окне Web Console выберите **Операции** → **Лицензирование** → **Лицензии**.

   Откроется список лицензионных ключей.

2. Откройте свойства лицензионного ключа.

3. На вкладке **Общие** включите переключатель **Автоматически распространять лицензионный ключ на управляемые устройства**.

4. Сохраните внесенные изменения.

   В результате ключ будет автоматически распространяться на компьютеры, для которых он подходит. При автоматическом распространении ключа в качестве активного или резервного учитывается лицензионное ограничение на количество компьютеров, заданное в свойствах ключа. Если лицензионное ограничение достигнуто, распространение ключа на компьютеры автоматически прекращается. Вы можете просмотреть количество компьютеров, на которые добавлен ключ, и другие данные в свойствах ключа на вкладке **Устройства**.

При активации приложения с помощью *кода активации* нужен доступ в интернет для подключения к серверам активации "Лаборатории Касперского". При активации приложения с помощью *файла ключа* доступ в интернет не нужен. Если компьютеры находятся в изолированном сегменте сети без доступа в интернет, для активации приложения с помощью кода нужно разрешить использование Сервера администрирования Kaspersky Security Center в качестве прокси-сервера. То есть приложение получит доступ к серверам активации через Сервер администрирования с доступом в интернет.

Как включить использование Сервера администрирования в качестве прокси-сервера для активации приложения в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Общие настройки** → **Настройки приложения**.

4. Установить флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации**.

5. Сохраните внесенные изменения.

Как включить использование Сервера администрирования в качестве прокси-сервера для активации приложения в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки** → **Интеграция с KSC**.

5. Установить флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации**.

6. Сохраните внесенные изменения.

Если активировать приложение с помощью *кода активации* не удается, вы можете получить *файл ключа* с помощью решения "Лаборатории Касперского" и повторить попытку активацию приложения другим способом.

Мониторинг использования лицензий

Вы можете контролировать использование лицензий следующими способами:

- Просмотреть *Отчет об использовании лицензионных ключей* в инфраструктуре организации (**Мониторинг** → **Отчеты**).
- Просмотреть статусы компьютеров на вкладке **Управляемые устройства** → **Устройства**. Если приложение не активировано, то у компьютера будет статус ⚠ *Приложение не активировано*.
- Просмотреть информацию о лицензии в свойствах компьютера.
- Просмотреть свойства ключа (**Операции** → **Лицензирование**).

Особенности активации приложения в составе Kaspersky Security Center Cloud Console

Для Kaspersky Security Center Cloud Console предусмотрена пробная версия. *Пробная версия* – это специальная версия Kaspersky Security Center Cloud Console, предназначенная для ознакомления пользователя с функциями Kaspersky Security Center Cloud Console. В этой версии вы можете выполнять действия в рабочем пространстве в течение 30 дней. Все управляемые приложения запускаются по пробной лицензии Kaspersky Security Center Cloud Console автоматически, включая Kaspersky Endpoint Security. При этом активировать Kaspersky Endpoint Security по собственной пробной лицензии по истечении пробной лицензии Kaspersky Security Center Cloud Console невозможно. Подробнее о лицензировании Kaspersky Security Center см. в справке Kaspersky Security Center Cloud Console.

> Пробная версия Kaspersky Security Center Cloud Console не позволяет вам впоследствии перейти на коммерческую версию. Любое пробное рабочее пространство будет автоматически удалено со всем его содержимым по истечении 30-дневного срока.

Удаление лицензионного ключа

Для удаления лицензионного ключа вам нужно запустить на компьютерах специальную задачу. Вы можете удалить лицензионный ключ, например, для перераспределения количества единиц лицензирования. Также при истечении срока действия лицензии Kaspersky Endpoint Security уведомляет вас об этом. При этом, если вы добавили лицензионный ключ с коротким сроком действия для ознакомления с возможностями приложения (например, EDR Optimum Add-on), вы можете удалить лицензионный ключ и, таким образом, вы избавитесь от уведомлений и исправите статус компьютера.

Задача *Удаление ключа* позволяет удалять любые лицензионные ключи с компьютера. Вы можете удалять как активные ключи, так и резервные. Также кроме ключа для активации Kaspersky Endpoint Security вы можете удалять отдельные ключи для решений Detection and Response от "Лаборатории Касперского" (например, EDR Optimum Add-on).

Как удалить лицензионный ключ в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Удаление ключа**.

Шаг 2. Выбор лицензии

Выберите лицензионный ключ, который вы хотите удалить. Вы можете выбрать ключ из хранилища Kaspersky Security Center или выбрать файл ключа.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 5. Определение названия задачи

Введите название задачи, например, *Удаление ключа для beta*.

Шаг 6. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как удалить лицензионный ключ в Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.
2. В раскрывающемся списке **Тип задачи** выберите **Удаление ключа**.
3. В поле **Название задачи** введите короткое описание, например, *Удаление ключа для beta*.
4. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи. Перейдите к следующему шагу.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 3. Выбор лицензии

Выберите лицензионный ключ, который вы хотите удалить. Вы можете выбрать ключ из хранилища Kaspersky Security Center или выбрать файл ключа. Перейдите к следующему шагу.

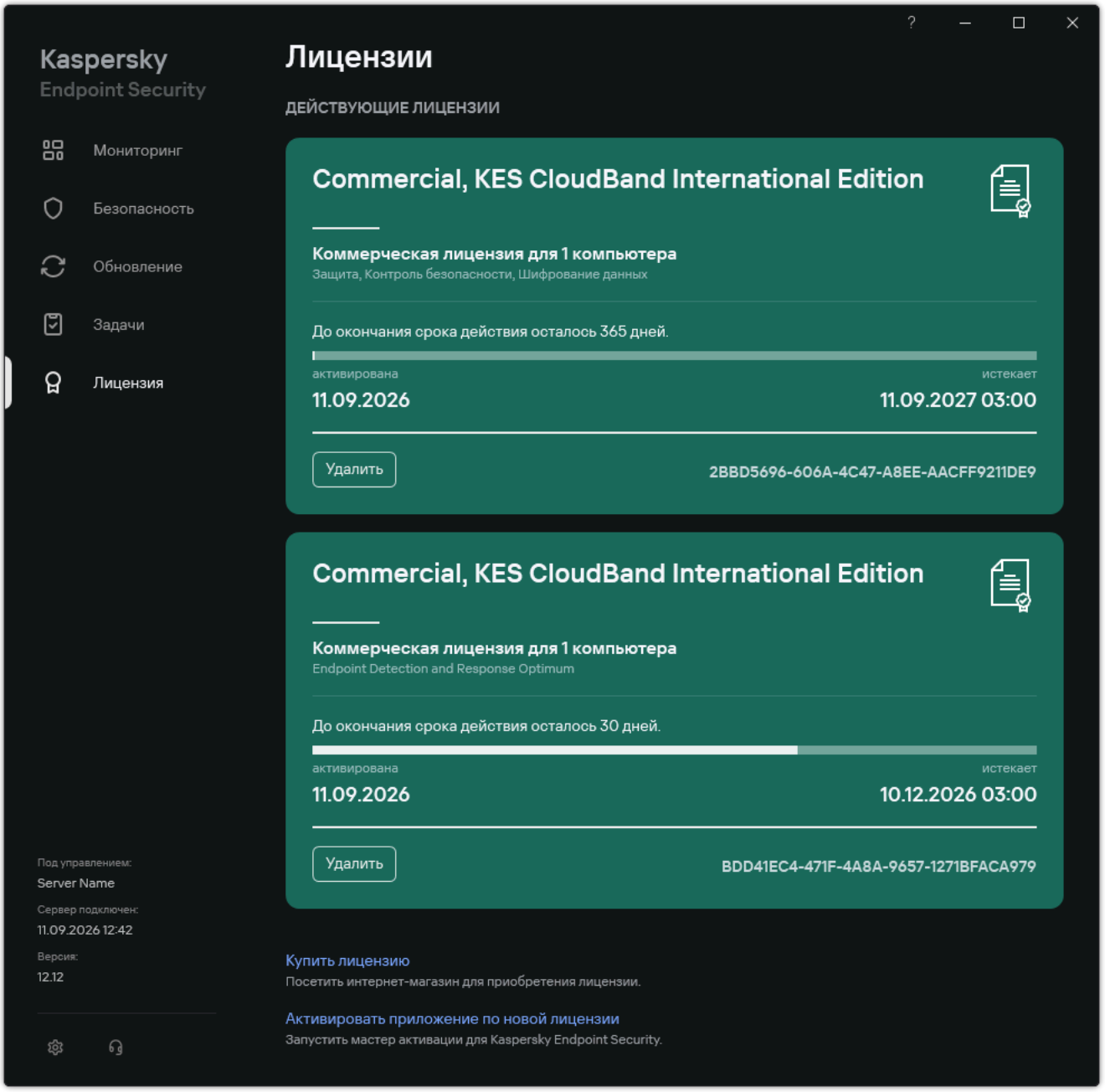
Шаг 4. Завершение создания задачи

Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача. Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку **Запустить**.

Как удалить лицензионный ключ в интерфейсе приложения

1. В главном окне приложения перейдите в раздел **Лицензия**.

2. Выберите ключ, который вы хотите удалить, и нажмите на кнопку **Удалить**.



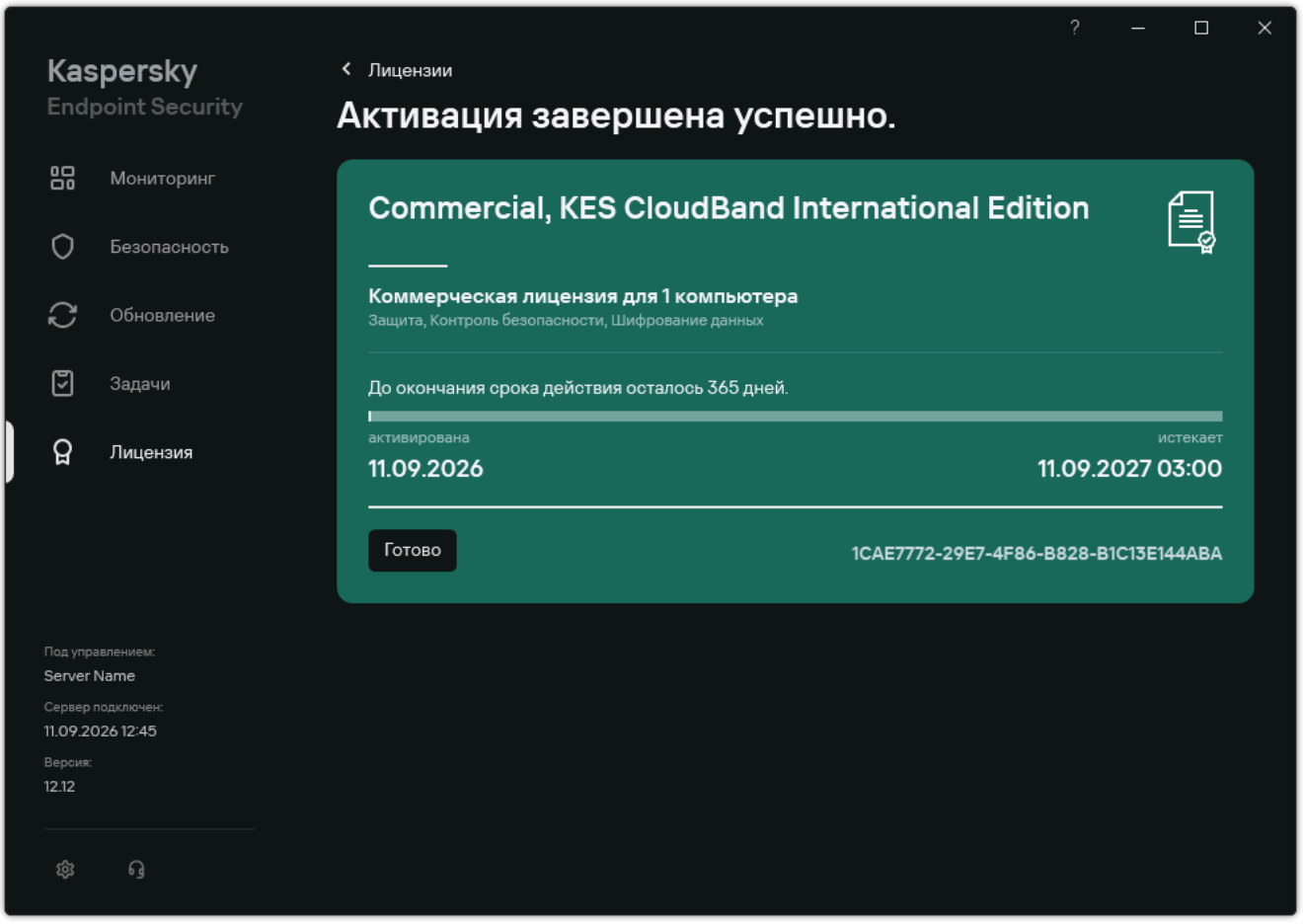
Окно Лицензирование

Также вы можете удалить лицензионный ключ из командной строки.

Просмотр информации о лицензии

Чтобы просмотреть информацию о лицензии,

в главном окне приложения перейдите в раздел **Лицензия** (см. рис. ниже).



Окно Лицензирование

В разделе представлена следующая информация:

- *Статус ключа*. На компьютере может быть несколько ключей. Ключ может быть активным и резервным. В приложении не может быть больше одного активного ключа. Резервный ключ может стать активным только после истечения срока годности активного ключа или после удаления активного ключа по кнопке **Удалить**.
- *Название приложения*. Полное название приобретенного приложения "Лаборатории Касперского".
- *Тип лицензии*. Предусмотрены следующие типы лицензий: пробная и коммерческая.
- *Функциональность*. Функции приложения, которые доступны по вашей лицензии. Предусмотрены следующие функции: Защита, Контроль безопасности, Шифрование данных и другие. Список доступных функций также указан в Лицензионном сертификате.

- *Дополнительная информация о лицензии*. Дата начала и дата и время окончания срока действия лицензии (только для активного ключа), оставшийся срок действия лицензии.

  Время окончания срока действия лицензии отображается в часовом поясе, настроенном в операционной системе.

- *Ключ*. Ключ – это уникальная буквенно-цифровая последовательность, которая формируется из кода активации или файла ключа.

Также в окне лицензирования доступны следующие действия:

- **Купить лицензию** / **Продлить срок действия лицензии**. Открывает веб-сайт интернет-магазина "Лаборатории Касперского", где вы можете приобрести лицензию или продлить срок действия лицензии. Для этого вам будет нужно ввести данные организации и оплатить заказ.

- **Активировать приложение по новой лицензии**. Запускает мастер активации приложения. Мастер позволяет добавить ключ с помощью кода активации или файла ключа. Мастер активации приложения позволяет добавить активный ключ и только один резервный ключ.

Приобретение лицензии

Вы можете приобрести лицензию уже после установки приложения. Приобретя лицензию, вы получите код активации или файл ключа, с помощью которых нужно активировать приложение.

Чтобы приобрести лицензию, выполните следующие действия:

1. В главном окне приложения перейдите в раздел **Лицензия**.

2. Выполните одно из следующих действий:

   - Нажмите на кнопку **Купить лицензию**, если не добавлен ни один ключ или добавлен ключ для пробной лицензии.

   - Нажмите на кнопку **Продлить срок действия лицензии**, если добавлен ключ для коммерческой лицензии.

   Откроется веб-сайт интернет-магазина "Лаборатории Касперского", где вы можете приобрести лицензию.

Продление подписки

При использовании приложения по подписке Kaspersky Endpoint Security автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки.

Если вы используете приложение по неограниченной подписке, Kaspersky Endpoint Security автоматически в фоновом режиме проверяет наличие обновленного ключа на сервере активации. Если на сервере активации есть ключ, приложение добавляет его в режиме замены предыдущего ключа. Таким образом неограниченная подписка на Kaspersky Endpoint Security продлевается без вашего участия.

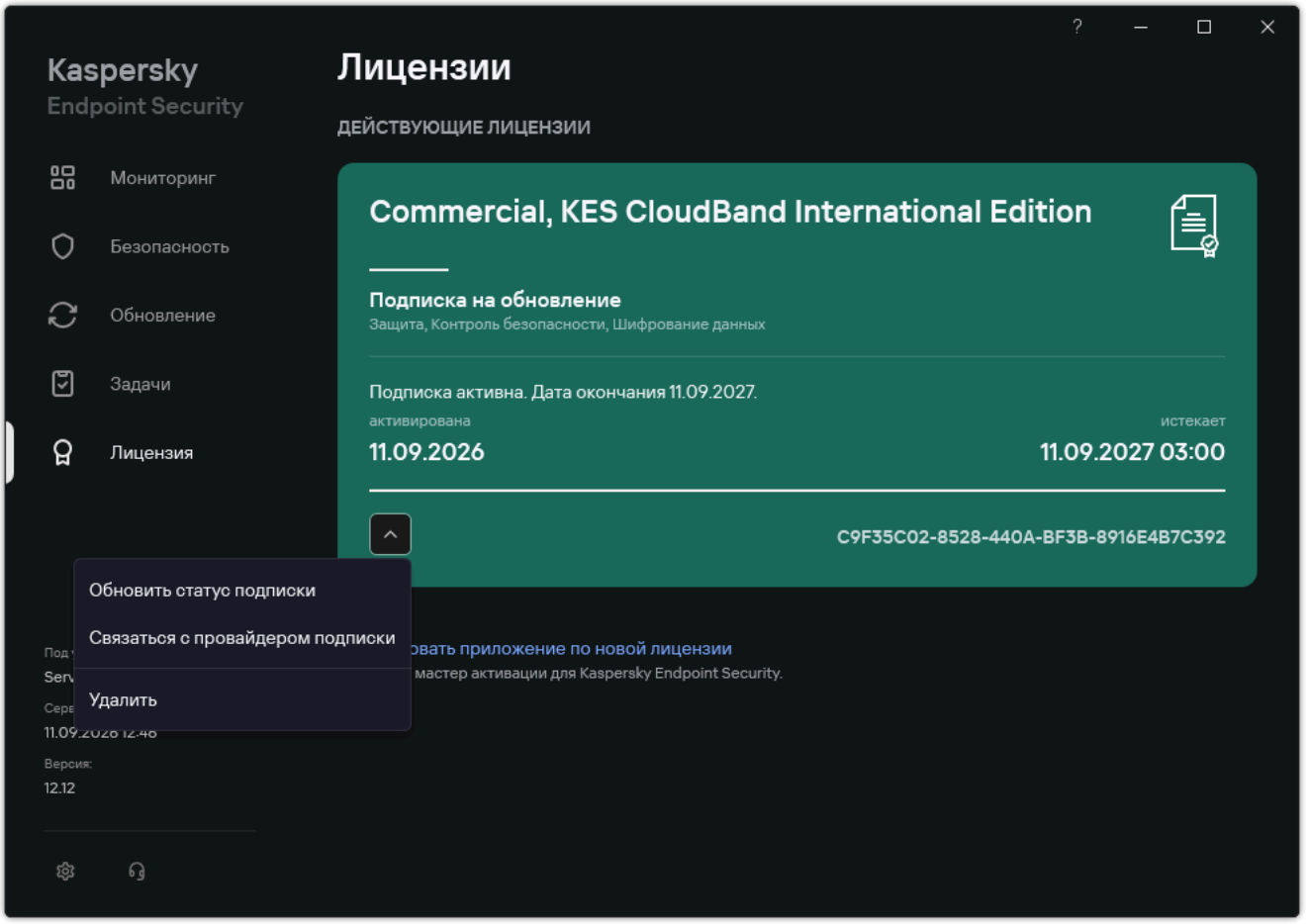
Если вы используете приложение по ограниченной подписке, в день истечения подписки или льготного периода после истечения подписки, во время которого доступно ее продление, Kaspersky Endpoint Security уведомляет вас об этом и прекращает попытки автоматического продления подписки. Поведение Kaspersky Endpoint Security при этом соответствует ситуации, когда истекает срок действия коммерческой лицензии на использование приложения, – приложение работает без обновлений и Kaspersky Security Network недоступен.

Вы можете продлить подписку на веб-сайте поставщика услуг.

Чтобы перейти на веб сайт поставщика услуг из интерфейса приложения, выполните следующие действия:

1. В главном окне приложения перейдите в раздел **Лицензия**.
2. Нажмите на кнопку **Связаться с поставщиком подписки**.

Вы можете обновить статус подписки вручную. Это может потребоваться, если подписка продлена после истечения льготного периода, и приложение автоматически не обновляет статус подписки.



Продление подписки

Начало работы

После установки Kaspersky Endpoint Security вы можете управлять приложением с помощью следующих интерфейсов:

- Локальный интерфейс приложения.
- Консоль администрирования Kaspersky Security Center.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Консоль администрирования Kaspersky Security Center

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Security, настраивать параметры работы приложения, изменять состав компонентов приложения, добавлять ключи, запускать и останавливать задачи обновления и проверки.

Управление приложением через Kaspersky Security Center осуществляется с помощью плагина управления Kaspersky Endpoint Security.

Подробнее об управлении приложением через Kaspersky Security Center см. в справке Kaspersky Security Center.

Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console

Kaspersky Security Center Web Console (далее также *Web Console*). Представляет собой веб-интерфейс для управления системой защиты, построенной на основе приложений "Лаборатории Касперского". Вы можете работать в Kaspersky Security Center Web Console через браузер на любом устройстве. Подробную информацию о Kaspersky Security Center Web Console см. в справке Kaspersky Security Center.

Kaspersky Security Center Cloud Console (далее также "*Cloud Console*") представляет собой облачное решение для защиты и контроля сети организации. Подробную информацию о Kaspersky Security Center Cloud Console см. в справке Kaspersky Security Center Cloud Console.

С помощью Web Console и Cloud Console вы можете выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- устанавливать приложения "Лаборатории Касперского" на устройства вашей сети;
- управлять установленными приложениями;
- просматривать отчеты о состоянии системы безопасности.

Управление приложением Kaspersky Endpoint Security через Web Console, Cloud Console и Консоль администрирования Kaspersky Security Center отличается. Также отличается список доступных компонентов и задач.

О плагине управления Kaspersky Endpoint Security для Windows

Плагин управления Kaspersky Endpoint Security для Windows обеспечивает взаимодействие Kaspersky Endpoint Security с Kaspersky Security Center. Плагин управления позволяет управлять Kaspersky Endpoint Security с помощью следующих инструментов: политики, задачи, а также локальные параметры приложения. Для взаимодействия с Kaspersky Security Center Web Console предназначен веб-плагин.

Версия плагина управления может отличаться от версии приложения Kaspersky Endpoint Security, установленной на клиентском компьютере. Если в установленной версии плагина управления предусмотрено меньше функций, чем в установленной версии Kaspersky Endpoint Security, то параметры недостающих функций не регулируются плагином управления. Такие параметры могут быть изменены пользователем в локальном интерфейсе Kaspersky Endpoint Security.

Веб-плагин по умолчанию не установлен в Kaspersky Security Center Web Console. Веб-плагин требуется установить на компьютер с установленным приложением Kaspersky Security Center Web Console. При этом функции веб-плагина доступны всем администраторам, у которых есть доступ к Web Console в браузере. Вы можете просмотреть список установленных веб-плагинов в интерфейсе Web Console (**Параметры консоли** → **Веб-плагины**).

Если вы используете Kaspersky Endpoint Security в составе решения Kaspersky Endpoint Detection and Response Optimum, вам нужно установить плагин управления Kaspersky Endpoint Detection and Response. Плагин управления нужен для отображения деталей алерта. *Детали алерта* – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Таким образом, для создания задач реагирования на угрозы вам нужен плагин управления Kaspersky Endpoint Security, а для просмотра деталей алерта вам нужен плагин управления EDR.

Установка веб-плагина

Вы можете установить веб-плагин следующими способами:

- Установить веб-плагин с помощью мастера первоначальной настройки Kaspersky Security Center Web Console.

  Web Console автоматически предлагает запустить мастер первоначальной настройки при первом подключении Web Console к Серверу администрирования. Также вы можете запустить мастер первоначальной настройки в интерфейсе Web Console (**Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер первоначальной настройки**). Мастер первоначальной настройки также может проверить актуальность установленных веб-плагинов и загрузит необходимые обновления для них. Подробнее о мастере первоначальной настройки Kaspersky Security Center Web Console см. в справке Kaspersky Security Center.

- Установить веб-плагин из списка доступных дистрибутивов в Web Console.

  Для установки веб-плагина требуется выбрать дистрибутив веб-плагина Kaspersky Endpoint Security в интерфейсе Web Console (**Параметры консоли** → **Веб-плагины**). Список доступных дистрибутивов обновляется автоматически после выпуска новых версий приложений "Лаборатории Касперского".

- Загрузить дистрибутив в Web Console из стороннего источника.

  Для установки веб-плагина требуется добавить ZIP-архив дистрибутива веб-плагина Kaspersky Endpoint Security в интерфейсе Web Console (**Параметры консоли** → **Веб-плагины**). Дистрибутив веб-плагина вы можете загрузить, например, на веб-сайте "Лаборатории Касперского".

Начиная с версии Kaspersky Endpoint Security для Windows 12.11 порядок установки веб-плагина изменился. Теперь дистрибутив содержит два веб-плагина: *Kaspersky Endpoint Security для Windows 14.2.0* и *Unified Protection and Management Plug-in*. Это связано с переходом на единый веб-плагин управления приложениями "Лаборатории Касперского". Единый веб-плагин позволит создавать одну политику для управления несколькими приложениями "Лаборатории Касперского" (например, Kaspersky Endpoint Security для Windows, macOS и Linux). Переход на единый веб-плагин может занять несколько релизов. После завершения перехода на единый веб-плагин дистрибутив будет содержать только *Unified Protection and Management Plug-in*.

Обновление плагина управления

Для обновления плагина управления Kaspersky Endpoint Security для Windows требуется загрузить последнюю версию плагина управления (входит в комплект поставки) и запустить мастер установки плагина.

При появлении новой версии веб-плагина Web Console отобразит уведомление *Доступны обновления для используемых плагинов*. Вы можете перейти к обновлению версии веб-плагина из уведомления Web Console. Также вы можете проверить наличие обновлений веб-плагина вручную в интерфейсе Web Console (**Параметры Консоли** → **Веб-плагины**). Предыдущая версия веб-плагина будут автоматически удалена во время обновления.

> При обновлении веб-плагина сохраняются уже существующие элементы (например, политики или задачи). Новые параметры элементов, реализующие новые функции Kaspersky Endpoint Security, появятся в существующих элементах и будут иметь значения по умолчанию.

Вы можете обновить веб-плагин следующими способами:

- Обновить веб-плагин в списке веб-плагинов в онлайн-режиме.

  Для обновления веб-плагина требуется выбрать дистрибутив веб-плагина Kaspersky Endpoint Security в интерфейсе Web Console и запустить обновление (**Параметры Консоли** → **Веб-плагины**). Web Console проверит наличие обновлений на серверах "Лаборатории Касперского" и загрузит необходимые обновления.

- Обновить веб-плагин из файла.

  Для обновления веб-плагина требуется выбрать ZIP-архив дистрибутива веб-плагина Kaspersky Endpoint Security в интерфейсе Web Console (**Параметры Консоли** → **Веб-плагины**). Дистрибутив веб-плагина вы можете загрузить, например, на веб-сайте "Лаборатории Касперского". Вы можете обновить веб-плагин Kaspersky Endpoint Security только до более новой версии. Обновить веб-плагин до более старой версии невозможно.

При открытии любого элемента (например, политики или задачи) веб-плагин проверяет информацию о совместимости. Если версия веб-плагина равна или выше версии, указанной в информации о совместимости, то вы можете изменять параметры этого элемента. В противном случае изменение параметров выбранного элемента с помощью веб-плагина недоступно. Рекомендуется обновить веб-плагин.

Особенности работы с плагинами управления разных версий

Для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center требуется плагин управления, версия которого равна или выше версии, указанной в информации о совместимости Kaspersky Endpoint Security с плагином управления. Вы можете посмотреть минимальную необходимую версию плагина управления в файле installer.ini, входящем в комплект поставки.

При открытии любого элемента (например, политики или задачи) плагин управления проверяет информацию о совместимости. Если версия плагина управления равна или выше версии, указанной в информации о совместимости, то вы можете изменять параметры этого элемента. В противном случае изменение параметров выбранного элемента с помощью плагина управления недоступно. Рекомендуется обновить плагин управления.

Если в Консоли администрирования установлен плагин управления Kaspersky Endpoint Security, то установка новой версии плагина управления имеет следующие особенности:

- Предыдущая версия плагина управления Kaspersky Endpoint Security будет удалена.
- Плагин управления Kaspersky Endpoint Security новой версии поддерживает управление приложением Kaspersky Endpoint Security для Windows предыдущей версии на компьютерах пользователей.
- С помощью плагина управления новой версии вы можете изменять параметры в политиках, задачах и т.п., созданных плагином управления предыдущей версии.
- Для новых параметров плагин управления новой версии устанавливает значения по умолчанию при первом сохранении политики, профиля политики или задачи.

  После обновления плагина управления рекомендуется проверить и сохранить значения новых параметров в политиках и профилях политик. Если вы этого не сделаете, новые блоки параметров Kaspersky Endpoint Security на компьютере пользователя будут иметь значения по умолчанию и доступны для изменения (атрибут). Рекомендуется выполнять проверку начиная с политик и профилей политик верхнего уровня иерархии. Также рекомендуется использовать учетную запись пользователя, для которой настроены права доступа ко всем функциональным областям Kaspersky Security Center.

  О новых возможностях приложения вы можете узнать в Release Notes или в справке к приложению.

- Если в блок параметров в новой версии плагина управления был добавлен новый параметр, то ранее заданный статус атрибута / для этого блока параметров не изменяется.

Особенности использования защищенных протоколов для взаимодействия с внешними службами

Kaspersky Endpoint Security и Kaspersky Security Center используют защищенный канал связи с TLS (Transport Layer Security) для работы с внешними службами "Лаборатории Касперского". Kaspersky Endpoint Security использует внешние службы для работы следующих функций:

- обновление баз и модулей приложения;
- активация приложения с помощью кода активации (тип активации 2.0);
- использование Kaspersky Security Network.

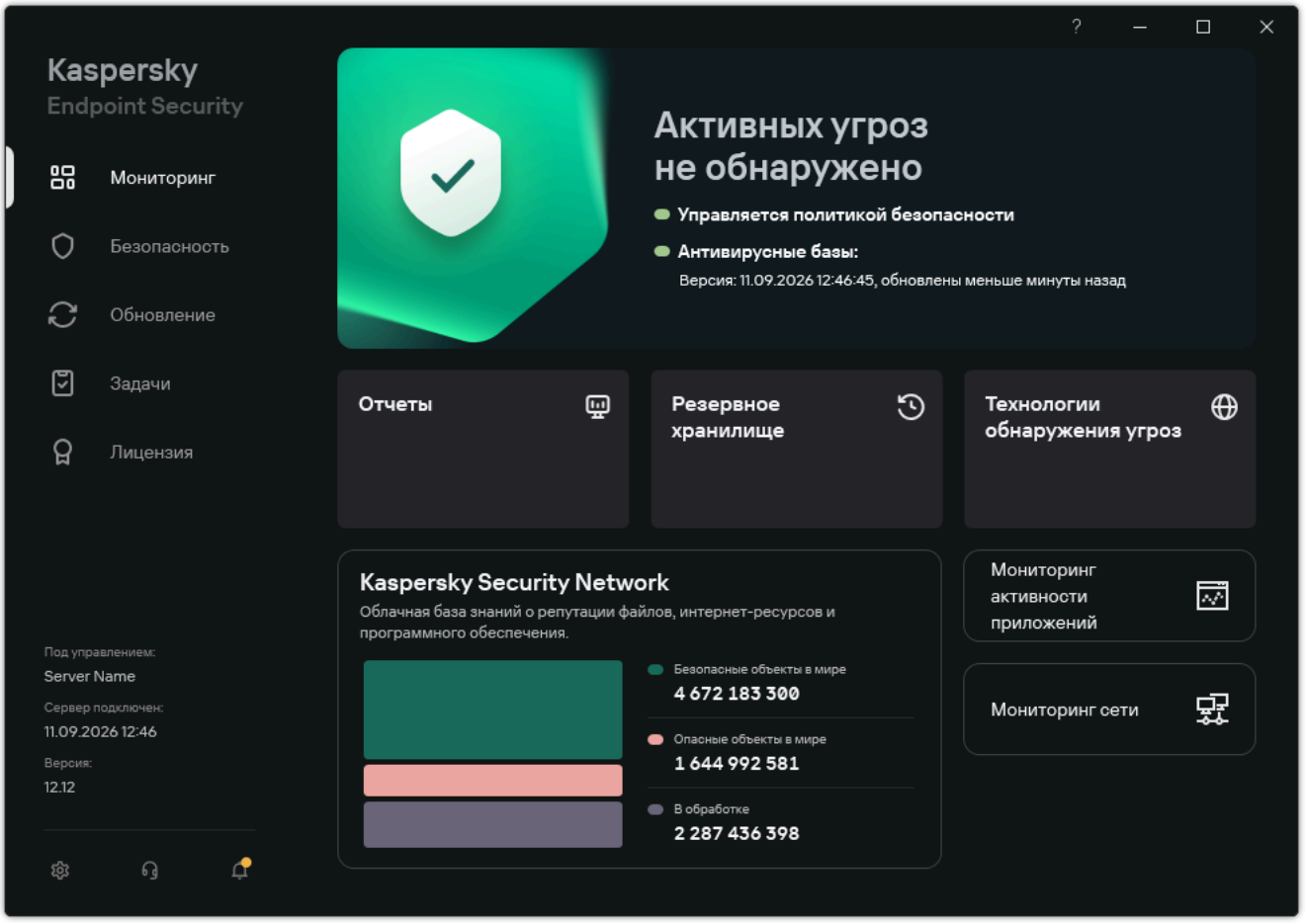
Использование TLS обеспечивает безопасность работы приложения за счет следующих свойств:

- Шифрование. Содержание сообщений конфиденциально и не раскрывается посторонним пользователям.
- Целостность. Получатель сообщения уверен в неизменности содержания с момента отсылки отправителем.
- Аутентификация. Получатель уверен, что связь устанавливается только с доверенным сервером "Лаборатории Касперского".

Для аутентификации серверов Kaspersky Endpoint Security использует сертификаты открытых ключей. Для работы с сертификатами требуется инфраструктура открытых ключей (англ. Public Key Infrastructure, PKI). Удостоверяющий центр является частью PKI. Так как службы "Лаборатории Касперского" не являются публичными и носят технический характер, "Лаборатория Касперского" использует собственный Удостоверяющий центр. В этом случае при отзыве корневых сертификатов Thawte, VeriSign, GlobalTrust и других, работоспособность PKI "Лаборатории Касперского" не будет нарушена.

Окружения, имеющие MITM (программные и аппаратные средства, поддерживающие разбор протокола HTTPS), Kaspersky Endpoint Security считает небезопасными. При работе со службами "Лаборатории Касперского" могут возникать ошибки, например, ошибки об использовании самозаверяющих сертификатов (англ. Self-Signed Certificate). Эти ошибки могут возникать из-за того, что средство HTTPS Inspection из вашего окружения не распознает PKI "Лаборатории Касперского". Для устранения проблем необходимо настроить исключения для взаимодействия с внешними службами.

Интерфейс приложения



Главное окно приложения

Мониторинг	• **Отчеты**. Просмотр событий, произошедших во время работы приложения, отдельных компонентов и задач. • **Резервное хранилище**. Просмотр списка копий зараженных файлов, которые были удалены в ходе работы приложения. • **Технологии обнаружения угроз**. Просмотр информации о технологиях обнаружения угроз и количестве угроз, обнаруженных с помощью этих технологий. • **Kaspersky Security Network**. Статус подключения Kaspersky Endpoint Security к Kaspersky Security Network и глобальная статистика KSN. *Kaspersky Security Network (KSN)* – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, приложение Kaspersky Endpoint Security получает от служб KSN сведения о репутации проверяемых веб-адресов, а также сведения о категории и репутации проверяемых файлов. • **Мониторинг активности приложений**. Просмотр информации о работе установленных приложениях. Мониторинг активности приложений отслеживает файловые, реестровые и системные события в операционной системе, связанные с приложением. • **Мониторинг сети**. Просмотр информации о сетевой активности компьютера в режиме реального времени. • **Мониторинг шифрования**. Контроль процесса шифрования или расшифровки дисков в режиме реального времени. Мониторинг шифрования доступен, если установлены компоненты Шифрование диска Kaspersky или Шифрование диска BitLocker.
Безопасность	Статус работы установленных компонентов. Также вы можете перейти к настройке компонентов или просмотреть отчеты.
Обновление	Управление задачами обновления Kaspersky Endpoint Security. Вы можете выполнять обновление антивирусных баз и модулей приложения и откат последнего обновления. Администратор может скрыть раздел от пользователя или ограничить управление задачами.
Задачи	Управление задачами проверки Kaspersky Endpoint Security. Вы можете выполнять поиск вредоносного ПО и проверку целостности приложения. Администратор может скрыть задачи от пользователя или ограничить управление задачами.

Лицензия	Лицензирование приложения. Вы можете приобрести лицензию, активировать приложение или продлить подписку. Так же вы можете просмотреть информацию о действующей лицензии.
⚙	Настройка параметров приложения. Администратор может запретить изменение параметров в Kaspersky Security Center.
	Информация о приложении: текущая версия Kaspersky Endpoint Security, дата выпуска баз, ключ и другая информация. Также вы можете перейти на информационные ресурсы "Лаборатории Касперского", чтобы получить полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.
	Сообщения с информацией о доступных обновлениях, а также запросы доступа к зашифрованным файлам и устройствам.

Значок приложения в области уведомлений

Сразу после установки Kaspersky Endpoint Security значок приложения появляется в области уведомлений панели задач Microsoft Windows.

Если значок приложения в области уведомлений скрыт, администратор выключил отображение интерфейса приложения в политике.

Значок приложения выполняет следующие функции:

- служит индикатором работы приложения;
- обеспечивает доступ к контекстному меню значка приложения и главному окну приложения.

Для отображения информации о работе приложения предназначены следующие статусы значка приложения:

- Значок означает, что работа критически важных компонентов защиты приложения включена. Kaspersky Endpoint Security покажет предупреждение, если от пользователя требуется выполнить действие, например, перезагрузить компьютер после обновления приложения.
- Значок означает, что работа критически важных компонентов защиты приложения выключена или нарушена. Работа компонентов защиты может быть нарушена, например, если срок действия лицензии истек или произошел сбой в работе приложения. Kaspersky Endpoint Security покажет предупреждение с описанием проблемы в защите компьютера.

Контекстное меню значка приложения содержит следующие пункты:

- **Kaspersky Endpoint Security для Windows**. Открывает главное окно приложения. В этом окне вы можете регулировать работу компонентов и задач приложения, просматривать статистику об обработанных файлах и обнаруженных угрозах.
- **Приостановить защиту** / **Возобновить защиту**. Приостановка работы всех компонентов защиты и контроля, не отмеченных в политике замком (). Перед выполнением этой операции рекомендуется выключить политику Kaspersky Security Center.

  Перед приостановкой работы компонентов защиты и контроля приложение запрашивает пароль доступа к Kaspersky Endpoint Security (пароль учетной записи или временный пароль). Далее вы можете выбрать период приостановки: на указанное время, до перезагрузки или по требованию пользователя.

  Этот пункт контекстного меню доступен, если включена Защита паролем. Для возобновления работы компонентов защиты и контроля выберите пункт **Возобновить защиту** в контекстном меню приложения.

Приостановка работы компонентов защиты и контроля не влияет на выполнение задач обновления и поиска вредоносного ПО. Также приложение продолжает использование Kaspersky Security Network.

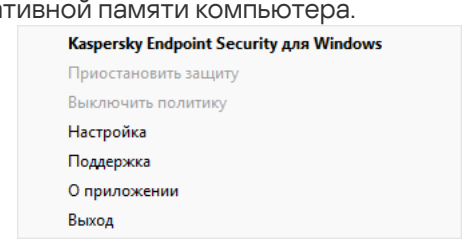
- **Выключить политику** / **Включить политику**. Выключение политики Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком (). При выключении политики приложение запрашивает пароль доступа к Kaspersky Endpoint Security (пароль учетной записи или временный пароль). Этот пункт контекстного меню доступен, если включена Защита паролем. Для включения политики выберите пункт **Включить политику** в контекстном меню приложения.

- **Настройка**. Открывает окно настройки параметров приложения.

- **Поддержка**. Открывает окно, содержащее информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".

- **О приложении**. Открывает информационное окно со сведениями о приложении.

- **Выход**. Завершает работу Kaspersky Endpoint Security. Если вы выбрали этот пункт контекстного меню, приложение выгружается из оперативной памяти компьютера.



Контекстное меню значка приложения

Упрощенный интерфейс приложения

Если к клиентскому компьютеру, на котором установлено приложение Kaspersky Endpoint Security, применена политика Kaspersky Security Center, в которой настроено отображение упрощенного интерфейса приложения, то на этом клиентском компьютере недоступно главное окно приложения. По правой клавише мыши пользователь может открыть контекстное меню значка Kaspersky Endpoint Security (см. рис. ниже), содержащее следующие пункты:

- **Выключить политику** / **Включить политику**. Выключение политики Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком (). При выключении политики приложение запрашивает пароль доступа к Kaspersky Endpoint Security (пароль учетной записи или временный пароль). Этот пункт контекстного меню доступен, если включена Защита паролем. Для включения политики выберите пункт **Включить политику** в контекстном меню приложения.

- **Задачи**. Раскрывающийся список, содержащий следующие элементы:

  - **Проверка целостности приложения**.

  - **Откат к предыдущей версии баз**.

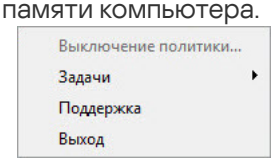
  - **Полная проверка**.

  - **Выборочная проверка**.

- **Проверка важных областей**.
- **Обновление**.

- **Поддержка**. Открывает окно, содержащее информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".

- **Выход**. Завершает работу Kaspersky Endpoint Security. Если вы выбрали этот пункт контекстного меню, приложение выгружается из оперативной памяти компьютера.



Контекстное меню значка приложения при отображении упрощенного интерфейса приложения

Настройка отображения интерфейса приложения

Вы можете настроить отображение интерфейса приложения для пользователя компьютера. Пользователь может взаимодействовать с приложением следующими способами:

- **Упрощенный**. На клиентском компьютере недоступно главное окно приложения, а доступен только значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять ограниченный список операций с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает над значком приложения только уведомления, требующие действий со стороны пользователя компьютера.

- **Полный**. На клиентском компьютере доступно главное окно Kaspersky Endpoint Security и значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает уведомления над значком приложения.

- **Не отображать пользовательский интерфейс**. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security. Также недоступны значок в области уведомлений Windows и уведомления.

Как настроить отображение интерфейса приложения в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Интерфейс**.

4. В блоке **Взаимодействие с пользователем** настройте отображение интерфейса приложения:

   - **Отображать пользовательский интерфейс**. На клиентском компьютере доступно главное окно Kaspersky Endpoint Security и значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает уведомления над значком приложения. При необходимости вы можете включить функцию **Скрыть раздел Мониторинг активности приложений**, чтобы скрыть данные об активности приложений на компьютере, ограничив доступ пользователя к инструменту Мониторинг активности приложений.

   - **Отображать упрощенный интерфейс**. На клиентском компьютере недоступно главное окно приложения, а доступен только значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять ограниченный список операций с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает над значком приложения только уведомления, требующие действий со стороны пользователя компьютера.

   - **Не отображать пользовательский интерфейс**. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security. Также недоступны значок в области уведомлений Windows и уведомления.

5. Сохраните внесенные изменения.

Как настроить отображение интерфейса приложения в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки** → **Взаимодействие с пользователем**.

5. В блоке **Отображение для пользователей** настройте отображение интерфейса приложения:

   - **Отображать пользовательский интерфейс**. Если функция выключена, на клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security. Также недоступны значок в области уведомлений Windows и уведомления.

   - **Упрощенный**. На клиентском компьютере недоступно главное окно приложения, а доступен только значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять ограниченный список операций с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает над значком приложения только уведомления, требующие действий со стороны пользователя компьютера.

   - **Полный**. На клиентском компьютере доступно главное окно Kaspersky Endpoint Security и значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает уведомления над значком приложения.

   - **Скрыть раздел Мониторинг активности приложений**. Если вы хотите скрыть данные об активности приложений на компьютере пользователя, вы можете ограничить доступ пользователя к инструменту Мониторинг активности приложений.

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Подготовка приложения к работе

После развертывания приложения на клиентских компьютерах для работы с Kaspersky Endpoint Security из Kaspersky Security Center вам нужно выполнить следующие действия:

- Создать и настроить политику.

  При помощи политик вы можете установить одинаковые значения параметров работы приложения Kaspersky Endpoint Security для всех клиентских компьютеров, входящих в состав группы администрирования. Мастер первоначальной настройки Kaspersky Security Center создает политику для Kaspersky Endpoint Security автоматически.

- Создать задачи *Обновление баз и модулей приложения* и *Поиск вредоносного ПО*.

  Задача *Обновление баз и модулей приложения* требуется для поддержания защиты компьютера в актуальном состоянии. При выполнении задачи Kaspersky Endpoint Security обновляет антивирусные базы и модули приложения. Задача *Обновление баз и модулей приложения* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление баз и модулей приложения* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.

  Задача *Поиск вредоносного ПО* требуется для своевременного обнаружения вирусов и других приложений, представляющих угрозу. Задачу *Поиск вредоносного ПО* вам нужно создать вручную.

  Как создать задачу Поиск вредоносного ПО в Консоли администрирования (MMC)

  1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

     Откроется список задач.

  2. Нажмите на кнопку **Новая задача**.

     Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Поиск вредоносного ПО**.

Шаг 2. Область проверки

Создайте список объектов, которые Kaspersky Endpoint Security будет проверять во время выполнения задачи проверки.

Шаг 3. Действие Kaspersky Endpoint Security

Выберите действие при обнаружении угрозы:

- **Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.

- **Лечить. Информировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security добавляет информацию об обнаруженных зараженных файлах в список активных угроз.

- **Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз.

- **Выполнять лечение активного заражения немедленно**. Если флажок установлен, Kaspersky Endpoint Security использует технологию лечения активного заражения во время проверки.

  Технология лечения активного заражения направлена на лечение операционной системы от вредоносных приложений, которые уже запустили свои процессы в оперативной памяти и мешают Kaspersky Endpoint Security удалить их с помощью других методов. В результате угроза нейтрализуется. В процессе процедуры лечения активного заражения не рекомендуется запускать новые процессы или редактировать реестр операционной системы. Технология лечения активного заражения требует значительных ресурсов операционной системы, что может замедлить работу других приложений. После окончания процедуры лечения активного заражения Kaspersky Endpoint Security перезагружает компьютер без запроса у пользователя подтверждения.

- **Выполнять только во время простоя компьютера**. Отложенный запуск задачи, если ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка. Если вы прервали выполнение задачи и, например, разблокировали компьютер, Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана. Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.

Шаг 4. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.

- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 5. Выбор учетной записи для запуска задачи

Выберите учетную запись для запуска задачи *Поиск вредоносного ПО*. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя. Если в область проверки входят сетевые диски или другие объекты, доступ к которым ограничен, выберите учетную запись пользователя с необходимыми правами доступа.

Шаг 6. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или после загрузки антивирусных баз в хранилище.

Шаг 7. Определение названия задачи

Введите название задачи, например, *Полная проверка каждый день*.

Шаг 8. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи. В результате на компьютерах пользователей будет выполняться поиск вредоносного ПО в соответствии с установленным расписанием.

Как создать задачу Поиск вредоносного ПО в Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Поиск вредоносного ПО**.

   c. В поле **Название задачи** введите короткое описание, например, *Еженедельная проверка*.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

5. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.

6. Завершите работу мастера.

   В списке задач отобразится новая задача.

7. Для настройки расписания выполнения задачи перейдите в свойства задачи.

   Рекомендуется настроить расписание выполнения задачи минимум раз в неделю.

8. Установите флажок напротив задачи.

9. Нажмите на кнопку **Запустить**.

   Вы можете отслеживать статус задачи, количество устройств, на которых задача выполнена успешно или завершилась с ошибкой.

В результате на компьютерах пользователей будет выполняться поиск вредоносного ПО в соответствии с установленным расписанием.

- Оптимизировать производительность Kaspersky Endpoint Security.

Управление политиками

Политика – это набор параметров работы приложения, определенный для группы администрирования. Для одного приложения можно настроить несколько политик с различными значениями. Для разных групп администрирования параметры работы приложения могут быть различными. В каждой группе администрирования может быть создана собственная политика для приложения.

Каждый параметр, представленный в политике, имеет атрибут ("замок"). От статуса данного атрибута зависит, будет ли параметр передан на управляемые устройства, входящие в группу администрирования:

- Если "замок" открыт (), значение данного параметра не будет передаваться на управляемые устройства. Параметр будет доступен для изменения в локальном интерфейсе приложения. Такие параметры называются *разблокированными*.

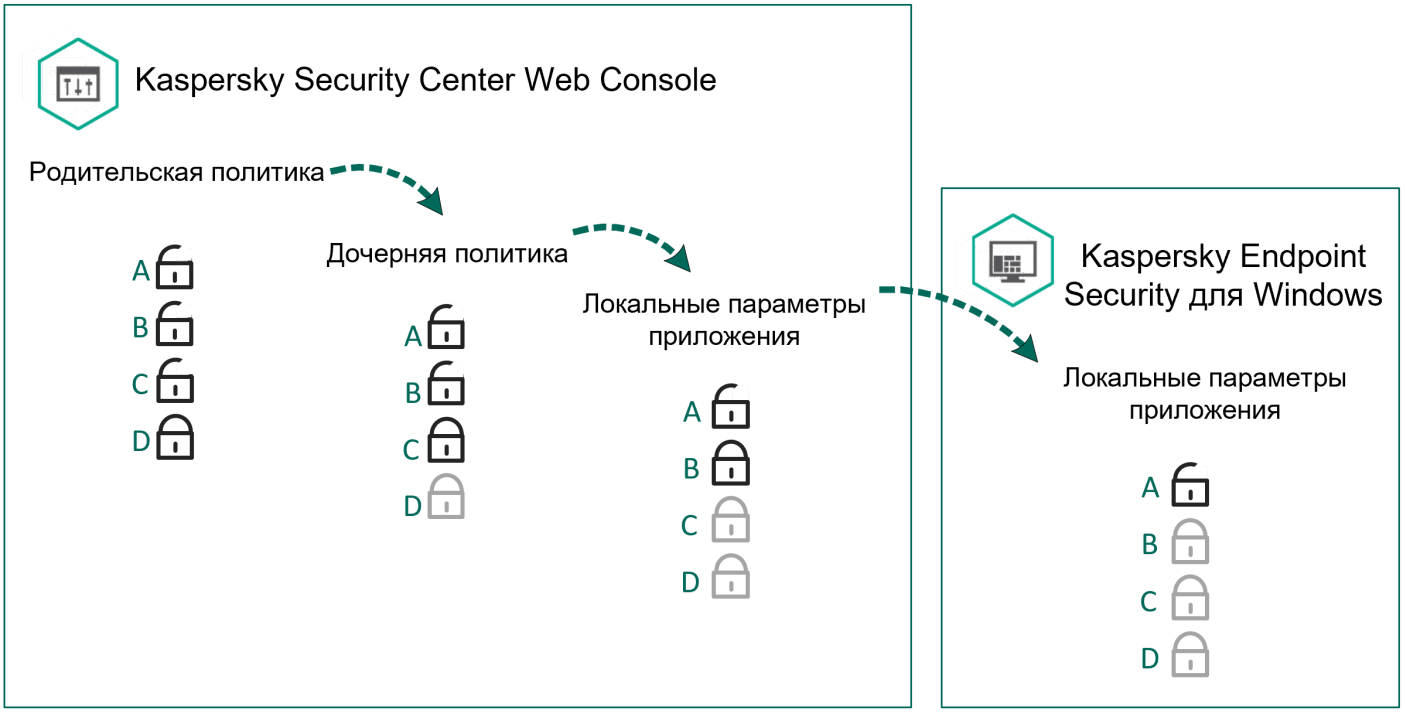
- Если "замок" закрыт (), значение данного параметра будет передано и применено на управляемых устройствах. Такие параметры называются *заблокированными*. Заблокированные параметры недоступны для изменения в локальном интерфейсе приложения.

Параметры политики передаются на клиентские компьютеры с помощью Агента администрирования при *синхронизации*. По умолчанию Сервер администрирования выполняет синхронизацию сразу после изменения параметров политики. Синхронизация выполняется через UDP-порт 15000 на клиентском компьютере. Сервер администрирования по умолчанию выполняет синхронизацию каждые 15 минут. Если синхронизация после изменения параметров политики не удалась, следующая попытка синхронизации будет выполнена по настроенному расписанию.

Наследование параметров

Политики, как и группы администрирования, имеют иерархию. *Дочерняя политика* – политика вложенного уровня иерархии, т.е. политика для вложенных групп администрирования и подчиненных Серверов администрирования.

По умолчанию дочерняя политика наследует параметры родительской политики. Если параметр в родительской политике имеет атрибут (замок закрыт), то в дочерних политиках и локальных параметрах приложения значение данного параметра будет переназначено в соответствии с родительской политикой, и параметр будет заблокирован. При необходимости вы можете выключить наследование параметров из родительской политики. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.



Наследование параметров

Права на доступ к параметрам политики (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, и отдельно для каждой функциональной области Kaspersky Endpoint Security. Для настройки прав доступа к параметрам политики перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center (по умолчанию этот раздел скрыт в интерфейсе консоли).

Ревизии политики

Kaspersky Security Center отслеживает изменения политики и создает ревизии. *Ревизия* – набор измененных параметров, сохраненные пользователем. С помощью ревизий вы можете сравнивать и откатывать изменения параметров политики. Кроме набора измененных параметров ревизия включает в себя данные о пользователе, который изменил параметры политики, а также время, IP-адрес компьютера, комментарий пользователя и другие данные.

Для просмотра журнала ревизий вам нужно открыть свойства политики и перейти в раздел **История ревизий**. Подробнее о работе с ревизиями см. в справке Kaspersky Security Center.

Создание политики

При создании политики мастер предлагает настроить параметры, которые важны для выбранного режима использования. Например, для работы приложения в режиме Легкого агента необходимо обязательно добавить Сервер защиты (SVM). При использовании приложения для защиты SQL-сервера необходимо добавить предустановленные исключения из проверки для стабильной работы сервера. Мастер предлагает настроить соответствующие параметры политики после выбора режима использования приложения. Далее вы можете изменить эти параметры в свойствах политики.

Как создать политику в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят интересующие вас клиентские компьютеры.
3. В рабочей области выберите вкладку **Политики**.
4. Нажмите на кнопку **Новая политика**.

   Запустится мастер создания политики.
5. Следуйте указаниям мастера создания политики.

Шаг 1. Выбор приложения для создания групповой политики

Выберите приложение **Kaspersky Endpoint Security для Windows (14.3)**.

Шаг 2. Определение названия для групповой политики

Введите имя групповой политики, например, *Политика для офиса*.

Вы также можете создавать новые политики на основе имеющихся с помощью мастера создания политики. Для этого на шаге ввода названия групповой политики требуется установить флажок **Использовать параметры политики для предыдущей версии приложения**. Мастер также позволяет создать политику Kaspersky Endpoint Security (KES) на основании политики других решений, например, Kaspersky Security для Windows Server (KSWS) или Kaspersky Security для виртуальных сред Легкий агент для Windows

Шаг 3. Участие в Kaspersky Security Network

Прочитайте и примите условия Положения о Kaspersky Security Network (KSN).

Шаг 4. Выбор режима использования приложения на компьютерах

В зависимости от назначения Kaspersky Endpoint Security вы можете настроить политику для следующих режимов работы приложения:

- Стандартный режим для защиты устройств.

  В этом режиме вы можете выбрать способ настройки политики:

  - **Создать политику с настройками по умолчанию**. Параметры политики по умолчанию считаются оптимальными. Эти параметры рекомендованы специалистами "Лаборатории Касперского". Параметры по умолчанию обеспечивают рекомендуемый уровень защиты и оптимальное потребление ресурсов компьютера.

  - **Изменить настройки политики в мастере**. Этот способ позволяет выполнять пошаговую настройку параметров политики в мастере. Также вы можете настроить параметры политики с помощью конфигурационного файла приложения (см. следующий шаг).

- Агент Endpoint Detection and Response для защиты от сложных угроз и целевых атак.

  Агент Endpoint Detection and Response – приложение, которое устанавливается на отдельные рабочие станции и серверы IT-инфраструктуры организации, для работы решений Detection and Response от "Лаборатории Касперского". На следующем шаге вам нужно выбрать решение для интеграции EDR-агента.

- Легкий агент для защиты виртуальных сред.

  Для работы приложения в режиме Легкого агента необходимо настроить соединение с виртуальной машиной SVM. Эти параметры являются обязательными для работы приложения в режиме Легкого агента.

Kaspersky Endpoint Security предоставляет единую политику для всех режимов использования приложения и типов ОС. То есть политика содержит полный набор параметров. При этом некоторые параметры политики приложение может игнорировать, так как Kaspersky Endpoint Security развернуто в режиме, в котором недоступны некоторые функции. Например, при использовании приложения в режиме Агента Endpoint Detection and Response доступны только параметры интеграции с решениями Detection and Response от "Лаборатории Касперского" и параметры интеграции с KUMA.

Рекомендуется использовать разные политики для разных режимов использования и разных типов операционных систем.

Шаг 5. Импорт настроек

Этот шаг доступен, если на шаге 4 вы выбрали настройку параметров политики вручную.

Вы можете создать политику на основе параметров Kaspersky Endpoint Security из конфигурационного файла CFG. Мастер создания политики не поддерживает зашифрованные конфигурационные файлы. При экспорте конфигурационного файла пропустите шаг шифрования файла.

При импорте конфигурационного файла CFG приложения мастеру доступны не все параметры политики. Например, в параметрах приложения отсутствуют профили политики. Если вы хотите перенести в политику все параметры и профили, вы можете использовать импорт другой политики из KLP-файла.

При импорте конфигурационного файла Kaspersky Endpoint Security не переносит пароли криптоконтейнеров. Если вы используете двустороннюю аутентификацию для подключения к серверам, вам нужно заново указать пароли к криптоконтейнерам.

Шаг 6 - 10. Настройка параметров политики

Этот шаг доступен, если на шаге 4 вы выбрали настройку параметров политики вручную.

Настройте параметры политики по шагам.

Шаг 11. Настройка доверенной зоны

Настройте доверенную зону. Вы можете добавить предустановленные исключения из проверки и доверенные приложения. Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах. Также предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в режиме Легкого агента в виртуальных средах Citrix и VMware.

Шаг 12. Выбор состояния политики

- **Активна**. После следующей синхронизации политика будет использоваться на компьютере в качестве действующей.

  Параметры активной политики во время синхронизации сохраняются на клиентских компьютерах. К одному компьютеру нельзя одновременно применить несколько политик, поэтому в каждой группе активной может быть только одна политика.

- **Неактивна**. Резервная политика. При необходимости неактивную политику можно сделать активной.

  Вы можете создать неограниченное количество неактивных политик. Неактивная политика не влияет на параметры приложения на компьютерах в сети. Неактивные политики предназначены для подготовки к нештатным ситуациям, например, в случае вирусной атаки. В случае атаки через флеш-накопители вы можете активировать политику, блокирующую доступ к флеш-накопителям. При этом активная политика автоматически становится неактивной.

- **Для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организации.

Завершите работу мастера.

Как создать политику в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.
3. Выберите приложение Kaspersky Endpoint Security и нажмите **Далее**.
4. Выберите режим использования приложения:

   - Стандартный режим для защиты рабочих станций и серверов.
   - Агент Endpoint Detection and Response для защиты от сложных угроз и целевых атак.

     Если вы выбрали этот режим, вы можете создать политику для интеграции компьютера с решениями Detection and Response от "Лаборатории Касперского". Мастер последовательно предложит настроить параметры интеграции для решений Kaspersky Managed Detection and Response и Kaspersky Anti Targeted Attack Platform (EDR).
   - Легкий агент для защиты виртуальных сред.

     Если вы выбрали этот режим, на следующем шаге вам нужно настроить параметры подключения к Серверу защиты (SVM). Эти параметры являются обязательными для работы приложения в режиме Легкого агента.

   Kaspersky Endpoint Security предоставляет единую политику для всех режимов использования приложения и типов ОС. То есть политика содержит полный набор параметров. При этом некоторые параметры политики приложение может игнорировать, так как Kaspersky Endpoint Security развернуто в режиме, в котором недоступны некоторые функции. Например, при использовании приложения в режиме Агента Endpoint Detection and Response доступны только параметры интеграции с решениями Detection and Response от "Лаборатории Касперского" и параметры интеграции с KUMA.

   > Рекомендуется использовать разные политики для разных режимов использования и разных типов операционных систем.
5. Настройте Защиту паролем для безопасности приложения.

   Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы приложения). Задайте пароль для учетной записи KLAdmin и подтвердите его. Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем.
6. Прочитайте и примите условия Положения о Kaspersky Security Network (KSN) и нажмите **Далее**.
7. Настройте доверенную зону. Вы можете добавить предустановленные исключения из проверки и доверенные приложения. Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах. Также предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в режиме Легкого агента в виртуальных средах Citrix и VMware.

8. Настройте дополнительные параметры политики:

   a. На вкладке **Общие** вы можете выполнить следующие действия:

   - Изменить имя политики.
   - Выбрать состояние политики:
     - **Активна**. После следующей синхронизации политика будет использоваться на компьютере в качестве действующей.
     - Параметры активной политики во время синхронизации сохраняются на клиентских компьютерах. К одному компьютеру нельзя одновременно применить несколько политик, поэтому в каждой группе активной может быть только одна политика.
     - **Неактивна**. Резервная политика. При необходимости неактивную политику можно сделать активной.
     - Вы можете создать неограниченное количество неактивных политик. Неактивная политика не влияет на параметры приложения на компьютерах в сети. Неактивные политики предназначены для подготовки к нештатным ситуациям, например, в случае вирусной атаки. В случае атаки через флеш-накопители, вы можете активировать политику, блокирующую доступ к флеш-накопителям. При этом активная политика автоматически становится неактивной.
     - **Для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организации.
   - Настроить наследование параметров:
     - **Наследовать параметры родительской политики**. Если переключатель включен, значения параметров политики наследуются из политики верхнего уровня иерархии. Параметры политики недоступны для изменения, если в родительской политике установлен.
     - **Обеспечить принудительное наследование параметров для дочерних политик**. Если переключатель включен, значения параметров политики будут распространены на дочерние политики. В свойствах дочерней политики будет автоматически включен и недоступен для выключения переключатель **Наследовать параметры родительской политики**. Параметры дочерней политики наследуются из родительской политики, кроме параметров с. Параметры дочерних политик недоступны для изменения, если в родительской политике установлен.

   b. На вкладке **Параметры приложения** вы можете настроить параметры политики Kaspersky Endpoint Security.

9. Завершите работу мастера.

В результате параметры Kaspersky Endpoint Security будут настроены на клиентских компьютерах при следующей синхронизации. Вы можете просмотреть информацию о политике, которая применена к компьютеру, в интерфейсе Kaspersky Endpoint Security по кнопке на главном экране (например, имя политики). Для этого в параметрах политики Агента администрирования нужно включить получение расширенных данных политики. Подробнее о политике Агента администрирования см. в справке Kaspersky Security Center.

Экспорт и импорт политики

Kaspersky Endpoint Security позволяет экспортировать политику, ее параметры и профили в файл формата KLP. Вы можете использовать функцию экспорта / импорта политики для резервного копирования политик, переноса политик на другой сервер или, например, для переноса политик из Kaspersky Security Center Windows в Kaspersky Security Center Linux. Подробнее об управлении политиками см. в справке Kaspersky Security Center.

Как экспортировать / импортировать политику в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите вкладку **Политики**.
4. Для экспорта политики выполните следующие действия:
   a. Выберите политику, которую вы хотите экспортировать.
   b. Нажмите на ссылку **Экспортировать политику в файл** в правой части окна.
   c. В открывшемся окне введите имя файла формата KLP, в который вы хотите экспортировать политику, а также выберите папку для сохранения файла.
   d. Сохраните файл.
5. Для импорта политики выполните следующие действия:
   a. Нажмите на кнопку **Импортировать политику из файла**.
   b. В открывшемся окне выберите KLP-файл политики, который вы хотите импортировать.
   c. Откройте файл.

В результате будет добавлена новая политика со статусом *Неактивная политика*.

Как экспортировать / импортировать политику в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Для экспорта политики выполните следующие действия:
   a. Установите флажок рядом с политикой, которую вы хотите экспортировать.
   b. Нажмите на кнопку **Экспортировать.**
   c. В открывшемся окне введите имя файла формата KLP, в который вы хотите экспортировать политику, а также выберите папку для сохранения файла.
   d. Сохраните файл.

3. Для импорта политики выполните следующие действия:

   a. Нажмите на кнопку **Импортировать**.

   b. Выберите KLP-файл политики, который вы хотите импортировать.

   c. После успешной обработки политики выберите группу администрирования, к которой вы хотите применить политику.

   d. Нажмите на кнопку **Завершить**, чтобы завершить импорт политики.

В результате будет добавлена новая политика со статусом *Неактивна*.

Индикатор уровня защиты

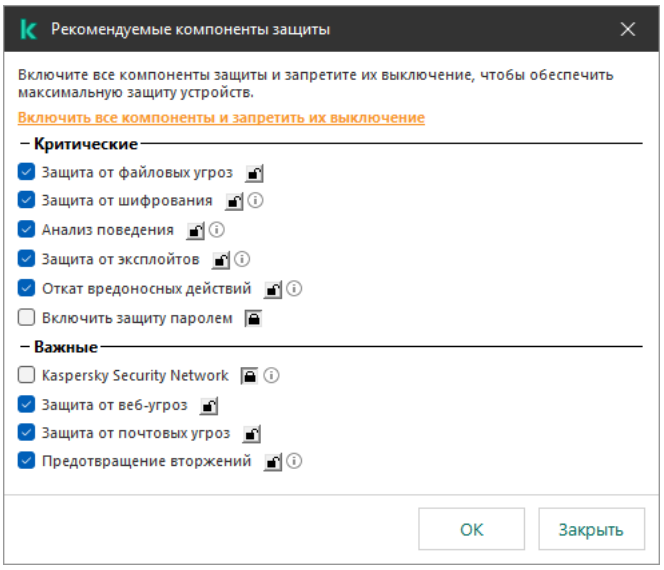
В верхней части окна свойств политики отображается индикатор уровня защиты. Индикатор может принимать одно из следующих значений:

- **Уровень защиты высокий**. Индикатор принимает это значение и цвет индикатора изменяется на зеленый, если включены все компоненты, относящиеся к следующим категориям:
  - **Критические**. Категория включает следующие компоненты:
    - Защита от файловых угроз.
    - Анализ поведения.
    - Защита от эксплойтов.
    - Откат вредоносных действий.
    - Защита служб приложения от внешнего управления.
  - **Важные**. Категория включает следующие компоненты:
    - Kaspersky Security Network.
    - Защита от веб-угроз.
    - Защита от почтовых угроз.
    - Предотвращение вторжений.
    - Защита паролем.
- **Уровень защиты средний**. Индикатор принимает это значение и цвет индикатора изменяется на желтый, если отключен один важный компонент.

- **Уровень защиты низкий**. Индикатор принимает это значение и цвет индикатора изменяется на красный в одном из следующих случаев:
  - отключены один или несколько критических компонентов;
  - отключены два или более важных компонента.

Если отображается индикатор со значением **Уровень защиты средний** или **Уровень защиты низкий**, то справа от индикатора доступна ссылка, по которой открывается окно **Рекомендуемые компоненты защиты**. В этом окне вы можете включить любой из рекомендованных компонентов защиты.

После обновления версии приложения индикатор уровня защиты может показать более низкий уровень защиты, чем до обновления. Это связано с тем, что в новой версии приложения добавлены новые компоненты или функции, важные для безопасности компьютера. После обновления версии приложения настройте новые параметры в соответствии с высоким уровнем защиты.



Индикатор уровня защиты политики

Управление задачами

Для работы с Kaspersky Endpoint Security через Kaspersky Security Center вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного клиентского компьютера;
- групповые задачи, определенные для клиентских компьютеров, входящих в группы администрирования;
- задачи для выборки компьютеров.

Вы можете создавать любое количество групповых задач, задач для выборки компьютеров и локальных задач. Подробнее о работе с группами администрирования и выборками компьютеров см. в справке Kaspersky Security Center.

Kaspersky Endpoint Security поддерживает выполнение следующих задач:

- **Поиск вредоносного ПО**. Kaspersky Endpoint Security проверяет на вирусы и другие приложения, представляющие угрозу, области компьютера, указанные в параметрах задачи. Задача *Поиск вредоносного ПО* является обязательной для работы Kaspersky Endpoint Security и создается во время работы мастера первоначальной настройки. Рекомендуется настроить расписание выполнения задачи минимум раз в неделю.

- **Добавление ключа**. Kaspersky Endpoint Security добавляет ключ для активации приложения, в том числе дополнительный. Перед выполнением задачи убедитесь, что количество компьютеров, на которых будет выполняться задача, не превышает количество компьютеров, на которые рассчитана лицензия.

- **Изменение состава компонентов приложения**. Kaspersky Endpoint Security устанавливает или удаляет на клиентских компьютерах компоненты согласно списку компонентов, указанному в параметрах задачи. Компонент Защита от файловых угроз удалить невозможно. Оптимальный состав компонентов Kaspersky Endpoint Security позволяет экономить ресурсы компьютера.

- **Инвентаризация**. Kaspersky Endpoint Security получает информацию обо всех исполняемых файлах приложений, хранящихся на компьютерах. Задачу *Инвентаризация* выполняет компонент Контроль приложений. Если компонент Контроль приложений не установлен, задача завершит работу с ошибкой.

- **Обновление баз и модулей приложения**. Kaspersky Endpoint Security обновляет базы и модули приложения. Задача *Обновление баз и модулей приложения* является обязательной для работы Kaspersky Endpoint Security и создается во время работы мастера первоначальной настройки. Рекомендуется настроить расписание выполнения задачи минимум раз в день.

- **Удаление данных**. Kaspersky Endpoint Security удаляет файлы и папки с компьютеров пользователей немедленно или при длительном отсутствии связи с Kaspersky Security Center.

- **Откат обновления**. Kaspersky Endpoint Security откатывает последнее обновление баз и модулей приложения. Это может понадобиться, например, если новые базы содержат некорректные данные, из-за которых Kaspersky Endpoint Security может блокировать безопасное приложение.

- **Проверка целостности приложения**. Kaspersky Endpoint Security анализирует файлы приложения, проверяет файлы на наличие повреждений или изменений и проверяет цифровые подписи файлов приложения.

- **Управление учетными записями Агента аутентификации**. Kaspersky Endpoint Security настраивает параметры учетных записей Агента аутентификации. Агент аутентификации нужен для работы с зашифрованными дисками. Перед загрузкой операционной системы пользователю нужно пройти аутентификацию с помощью агента.

Если приложение работает в составе решения Endpoint Detection and Response от "Лаборатории Касперского", вы можете запускать дополнительные задачи в качестве действий по реагированию на обнаружение (responses). Например, вы можете удаленно завершать процессы с помощью задачи *Завершение процесса*.

Запуск задач на компьютере выполняется только в том случае, если запущено приложение Kaspersky Endpoint Security.

Создание задачи

Как создать задачу в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** дерева Консоли администрирования.
3. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.

Как создать задачу в Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите задачу, которую вы хотите запустить на компьютерах пользователей.

   c. В поле **Название задачи** введите короткое описание.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.
4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.
5. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.
6. Завершите работу мастера.

В списке задач отобразится новая задача. Задача будет иметь параметры по умолчанию. Для настройки параметров задачи вам нужно перейти в свойства задачи. Для выполнения задачи вам нужно установить флажок напротив задачи и нажать на кнопку **Запустить**. После запуска задачи вы можете остановить задачу и возобновить выполнение задачи позже.

В списке задач вы можете контролировать результат выполнения задачи: статус задачи и статистику выполнения задачи на компьютерах. Также вы можете создать выборку событий для контроля за выполнением задач (**Мониторинг → Выборки событий**). Подробнее о выборке событий см. в справке Kaspersky Security Center. Также результаты выполнения задач сохраняются локально на компьютере в журнале событий Windows и в отчетах Kaspersky Endpoint Security.

Управление доступом к задачам

Права на доступ к задачам Kaspersky Endpoint Security (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, через параметры доступа к функциональным областям Kaspersky Endpoint Security. Для настройки доступа к функциональным областям Kaspersky Endpoint Security перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center. Подробнее о концепции управления задачами через Kaspersky Security Center см. в справке Kaspersky Security Center.

Вы можете настроить права доступа к задачам для пользователей компьютеров с помощью политики (*режим работы с задачами*). Например, вы можете скрыть групповые задачи в интерфейсе Kaspersky Endpoint Security.

Как настроить режим работы с задачами в интерфейсе Kaspersky Endpoint Security через Консоль администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Локальные задачи** → **Управление задачами**.
4. Настройте режим работы с задачами (см. таблицу ниже).
5. Сохраните внесенные изменения.

Как настроить режим работы с задачами в интерфейсе Kaspersky Endpoint Security через Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Взаимодействие с пользователем**.
5. В блоке **Разрешенные действия** настройте режим работы с задачами (см. таблицу ниже).
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Параметры управления задачами

Параметр	Описание
Доступ к локальным задачам	Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь, при отсутствии дополнительных ограничений политики, может настраивать и запускать задачи. При этом параметры расписания запуска задачи остаются недоступными для пользователя. Пользователь может запускать задачи только вручную. Если флажок снят, то локальные задачи скрыты в интерфейсе приложения. В этом режиме локальные задачи не запускаются по расписанию. Задачи недоступны для запуска и настройки в локальном интерфейсе Kaspersky Endpoint Security, а также при работе с командной строкой. Пользователь по-прежнему может запустить проверку файла или папки, выбрав пункт **Проверить на вирусы** в контекстном меню файла или папки. При этом задача проверки запустится со значениями параметров, установленными по умолчанию для задачи выборочной проверки.

Параметр	Описание
Просмотр групповых задач	Если флажок установлен, то групповые задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь может просмотреть полный список задач в интерфейсе приложения. Если флажок снят, Kaspersky Endpoint Security показывает пустой список задач.
Управление групповыми задачами	Если флажок установлен, пользователь может запускать и останавливать заданные в консоли Kaspersky Security Center групповые задачи. Пользователь может запускать и останавливать задачи в интерфейсе приложения или в упрощенном интерфейсе приложения. Если флажок снят, Kaspersky Endpoint Security запускает задачи автоматически по расписанию, или администратор запускает задачи вручную в консоли Kaspersky Security Center.

Настройка локальных параметров приложения

В Kaspersky Security Center вы можете настроить параметры Kaspersky Endpoint Security на конкретном компьютере – *локальные параметры приложения*. Некоторые параметры могут быть недоступны для изменения. Эти параметры заблокированы атрибутом в свойствах политики.

Как настроить локальные параметры приложения в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите вкладку **Устройства**.
4. Откройте свойства компьютера двойным щелчком мыши.
5. В окне свойств компьютера выберите раздел **Приложения**.
6. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows (14.3)** и откройте свойства приложения двойным щелчком мыши.
7. В разделе **Общие настройки** настройте параметры работы Kaspersky Endpoint Security, а также параметры отчетов и хранилищ.

   Остальные разделы окна свойств приложения стандартны для Kaspersky Security Center. Описание этих разделов вы можете прочитать в справке для Kaspersky Security Center.

   > Если для приложения создана политика, в которой запрещено изменение некоторых параметров, то во время настройки параметров приложения в разделе **Общие настройки** их изменение недоступно.

8. Сохраните внесенные изменения.

Как настроить локальные параметры приложения в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.

3. Выберите вкладку **Приложения**.

4. Нажмите на **Kaspersky Endpoint Security для Windows 14.2**.

   Откроются локальные параметры приложения.

5. Выберите вкладку **Параметры приложения**.

6. Настройте локальные параметры приложения.

7. Сохраните внесенные изменения.

Локальные параметры приложения повторяют параметры политики, кроме параметров шифрования.

Разделение доступа к функциям программы по пользовательским ролям

По умолчанию пользователи с ролью "Администратор Kaspersky Endpoint Security" в системе администрирования Kaspersky Security Center имеют доступ ко всем функциям Kaspersky Endpoint Security.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Endpoint Security один из следующих предустановленных уровней доступа к функциям Kaspersky Endpoint Security:

- **Чтение** – возможность просматривать общие параметры работы Kaspersky Endpoint Security и параметры работы компонентов Kaspersky Endpoint Security.
- **Изменение** – возможность просматривать и изменять общие параметры работы Kaspersky Endpoint Security и параметры работы компонентов Kaspersky Endpoint Security.
- **Выполнение** – возможность запускать и останавливать задачи Kaspersky Endpoint Security.
- **Выполнение операций с выборками устройств** – возможность запускать и останавливать задачи Kaspersky Endpoint Security для выборки устройств.

Также вы можете выполнять расширенную настройку прав доступа: разрешать или запрещать доступ к функциям Kaspersky Endpoint Security.

Права доступа к функциям Kaspersky Endpoint Security

Функциональная область	Компонент Kaspersky Endpoint Security
Адаптивный контроль аномалий	Адаптивный контроль аномалий.
Антивирусная функциональность	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз Защита от сетевых угроз Сетевой экран AMSI-защита Защита от эксплойтов Анализ поведения Откат вредоносных действий
Контроль программ	Контроль приложений

Функциональная область	Компонент Kaspersky Endpoint Security
Базовая функциональность	Поиск вредоносного ПО Обновление баз / Откат обновления баз Проверка целостности Удаление данных Добавление ключа Установка Изменение состава компонентов Управление учетными записями Агента аутентификации
Обнаружение и реагирование	Endpoint Detection and Response (KATA) Network Detection and Response (KATA) Endpoint Detection and Response Optimum Endpoint Detection and Response Expert Kaspersky Sandbox Managed Detection and Response
Контроль устройств	Контроль устройств
Шифрование	Шифрование диска Kaspersky Шифрование диска BitLocker Шифрование файлов Шифрование съемных дисков
Предотвращение вторжений	Предотвращение вторжений
Исключения	Угрозы и исключения
Веб-Контроль	Веб-Контроль

Запуск и остановка Kaspersky Endpoint Security

После установки Kaspersky Endpoint Security на компьютер пользователя запуск приложения выполняется автоматически. Далее по умолчанию запуск Kaspersky Endpoint Security выполняется сразу после операционной системы. Настроить автоматический запуск приложения в параметрах операционной системы невозможно.

Загрузка антивирусных баз Kaspersky Endpoint Security после загрузки операционной системы занимает до двух минут, в зависимости от производительности (технических возможностей) компьютера. В течение этого времени уровень защиты компьютера снижен. Загрузка антивирусных баз при запуске приложения Kaspersky Endpoint Security в уже запущенной операционной системе не вызывает снижения уровня защиты компьютера.

Как настроить запуск Kaspersky Endpoint Security в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Настройки приложения**.
4. С помощью флажка **Запускать приложение при включении компьютера (рекомендуется)** настройте запуск приложения.
5. Сохраните внесенные изменения.

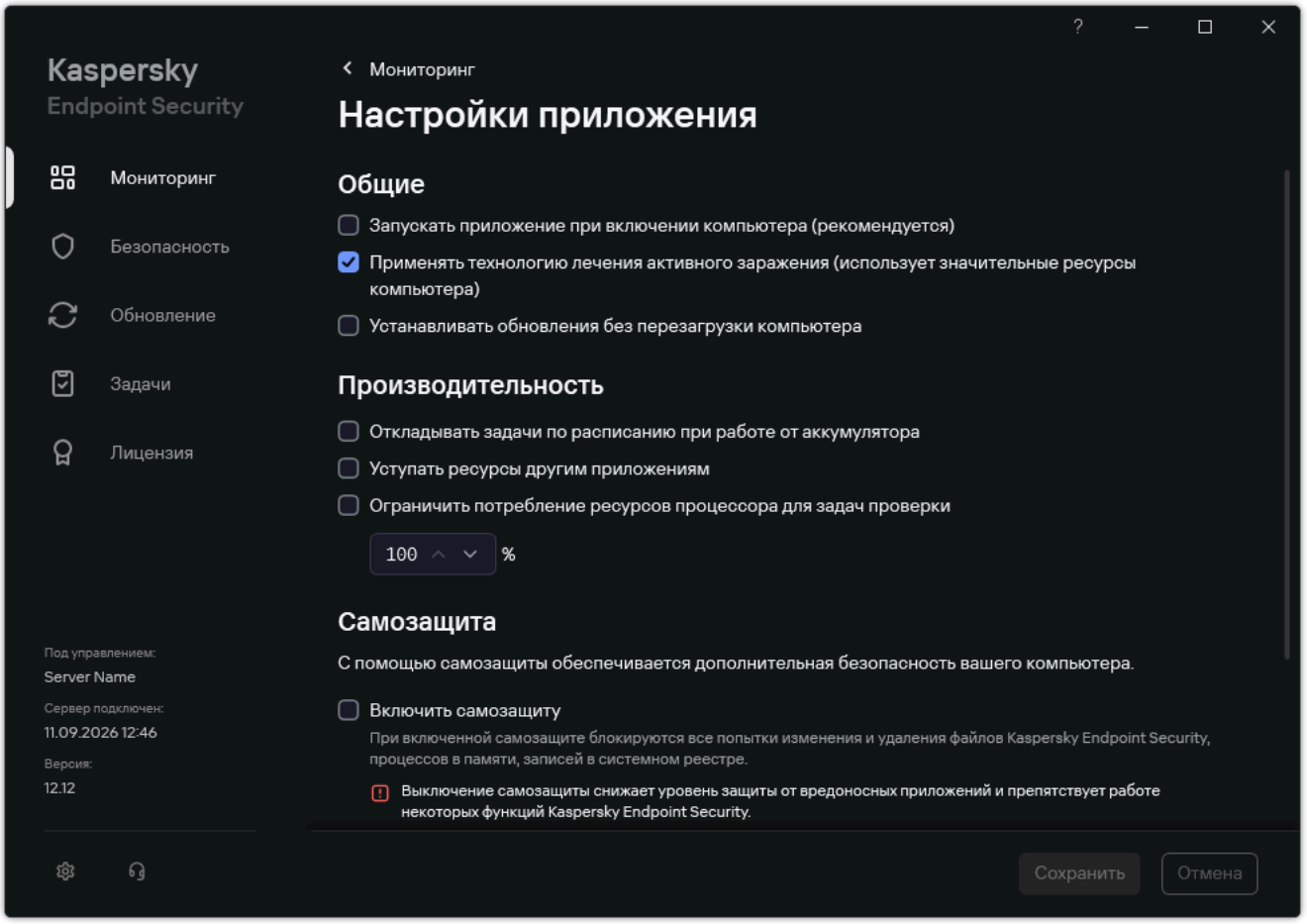
Как настроить запуск Kaspersky Endpoint Security в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Взаимодействие с пользователем**.
5. С помощью флажка **Запускать Kaspersky Endpoint Security при включении компьютера (рекомендуется)** настройте запуск приложения.
6. Сохраните внесенные изменения.

Как настроить запуск Kaspersky Endpoint Security в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.



Параметры приложения Kaspersky Endpoint Security для Windows

3. С помощью флажка **Запускать приложение при включении компьютера (рекомендуется)** настройте запуск приложения.

4. Сохраните внесенные изменения.

Специалисты "Лаборатории Касперского" рекомендуют не завершать работу Kaspersky Endpoint Security, поскольку в этом случае защита компьютера и ваших данных окажется под угрозой. Если требуется, вы можете приостановить защиту компьютера на необходимый срок, не завершая работу приложения.

Вы можете контролировать статус работы приложения с помощью виджета **Состояние защиты**.

Как запустить или остановить Kaspersky Endpoint Security в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите вкладку **Устройства**.

4. Откройте свойства компьютера двойным щелчком мыши.

5. В окне свойств компьютера выберите раздел **Приложения**.

6. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows (14.3)** и откройте свойства приложения двойным щелчком мыши.

7. Выполните одно из следующих действий:

   - Если вы хотите запустить приложение, справа от списка приложений "Лаборатории Касперского" нажмите на кнопку .
   - Если вы хотите остановить работу приложения, справа от списка приложений "Лаборатории Касперского" нажмите на кнопку .

Как запустить или остановить Kaspersky Endpoint Security в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.

2. Нажмите на имя компьютера, на котором вы хотите запустить или остановить Kaspersky Endpoint Security. Откроется окно свойств компьютера.

3. Выберите вкладку **Приложения**.

4. Установите флажок напротив приложения **Kaspersky Endpoint Security для Windows**.

5. Нажмите на кнопку **Запустить** или **Остановить**.

Как запустить или остановить Kaspersky Endpoint Security через командную строку

1. Запустите интерпретатор командной строки cmd от имени администратора.

2. Перейдите в папку, в которой расположен исполняемый файл klpsm.exe.

3. Для запуска приложения в командной строке введите `klpsm.exe start_avp_service`.

4. Для остановки приложения в командной строке введите `klpsm.exe stop_avp_service`.

> Для завершения работы приложения из командной строки необходимо включить внешнее управление системными службами.



Запуск и завершение работы приложения из командной строки

Приостановка и возобновление защиты и контроля компьютера

Приостановка защиты и контроля компьютера означает выключение на некоторое время всех компонентов защиты и всех компонентов контроля Kaspersky Endpoint Security.

Состояние приложения отображается с помощью значка приложения в области уведомлений панели задач:

- значок свидетельствует о приостановке защиты и контроля компьютера;
- значок свидетельствует о том, что защита и контроль компьютера включены.

Приостановка и возобновление защиты и контроля компьютера не оказывает влияния на выполнение задач проверки и задачи обновления.

Если в момент приостановки и возобновления защиты и контроля компьютера были установлены сетевые соединения, на экран выводится уведомление о разрыве этих сетевых соединений.

Чтобы приостановить защиту и контроль компьютера, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка приложения, который расположен в области уведомлений панели задач.

2. В контекстном меню выберите пункт **Приостановить защиту** (см. рисунок ниже).

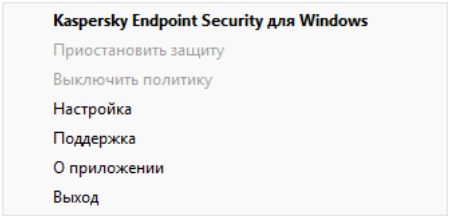
   Этот пункт контекстного меню доступен, если включена Защита паролем.

3. Выберите один из следующих вариантов:

   - **Приостановить на <период времени>** – защита и контроль компьютера включатся через интервал времени, указанный в раскрывающемся списке ниже.
   - **Приостановить до перезапуска приложения** – защита и контроль компьютера включатся после перезапуска приложения или перезагрузки операционной системы. Для использования этой возможности должен быть включен автоматический запуск приложения.
   - **Приостановить** – защита и контроль компьютера включатся тогда, когда вы решите возобновить их.

4. Нажмите на кнопку **Приостановить защиту**.

   Kaspersky Endpoint Security приостановит работу всех компонентов защиты и контроля, не отмеченных в политике замком (🔒). Перед выполнением этой операции рекомендуется выключить политику Kaspersky Security Center.



Контекстное меню значка приложения

Чтобы возобновить защиту и контроль компьютера, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка приложения, который расположен в области уведомлений панели задач.
2. В контекстном меню выберите пункт **Возобновить защиту**.

Вы можете возобновить защиту и контроль компьютера в любой момент, независимо от того, какой вариант приостановки защиты и контроля компьютера вы выбрали ранее.

Создание и использование конфигурационного файла

Конфигурационный файл с параметрами работы Kaspersky Endpoint Security позволяет решить следующие задачи:

- Выполнить локальную установку Kaspersky Endpoint Security через командную строку с заранее заданными параметрами.
- Выполнить удаленную установку Kaspersky Endpoint Security через Kaspersky Security Center с заранее заданными параметрами.
- Перенести параметры работы приложения в политику.
- Перенести параметры работы Kaspersky Endpoint Security с одного компьютера на другой (см. инструкцию ниже).

Экспорт конфигурационного файла

Начиная с Kaspersky Endpoint Security версии 14.2 доступна функция шифрования конфигурационного файла при экспорте. Так как конфигурационный файл может содержать данные учетных записей, мы рекомендуем зашифровать файл. Внести изменения в зашифрованный файл невозможно. Любые попытки внести изменения в файл приведут к его повреждению.

Шифрование конфигурационного файла имеет следующие особенности:

- Kaspersky Endpoint Security позволяет импортировать зашифрованные файлы только в интерфейсе приложения или в командной строке. Использовать такой файл в консоли Kaspersky Security Center для настройки политики или удаленной установки приложения невозможно. Для добавления файла в политику или инсталляционый пакет пропустите шаг шифрование файла.
- Восстановить пароль от зашифрованного конфигурационного файла невозможно.
- Kaspersky Endpoint Security версий ниже 14.1 не поддерживают импорт зашифрованных конфигурационных файлов. Для импорта файла в более ранней версии приложения пропустите шаг шифрования файла.

Чтобы создать конфигурационный файл, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Управление настройками**.
3. Нажмите на кнопку **Экспортировать**.
4. Для сохранения конфигурационного файла должна быть включена Защита паролем. Пользователь должен иметь разрешение **Экспорт настроек**.
5. В открывшемся окне укажите путь, по которому вы хотите сохранить конфигурационный файл, и введите его имя.

   Чтобы использовать конфигурационный файл для локальной или удаленной установки Kaspersky Endpoint Security, необходимо назвать его install.cfg.

6. Если требуется, включите переключатель **Зашифровать экспортируемый файл** и введите пароль для шифрования конфигурационного файла.

   Сохраните пароль в защищённом хранилище. Восстановить пароль невозможно.

7. Сохраните файл.

В результате приложение создаст конфигурационный файл.

Импорт конфигурационного файла

При импорте конфигурационного файла Kaspersky Endpoint Security не переносит пароли криптоконтейнеров. Если вы используете двустороннюю аутентификацию для подключения к серверам, вам нужно заново указать пароли к криптоконтейнерам.

Чтобы импортировать параметры работы Kaspersky Endpoint Security из конфигурационного файла, выполните следующие действия:

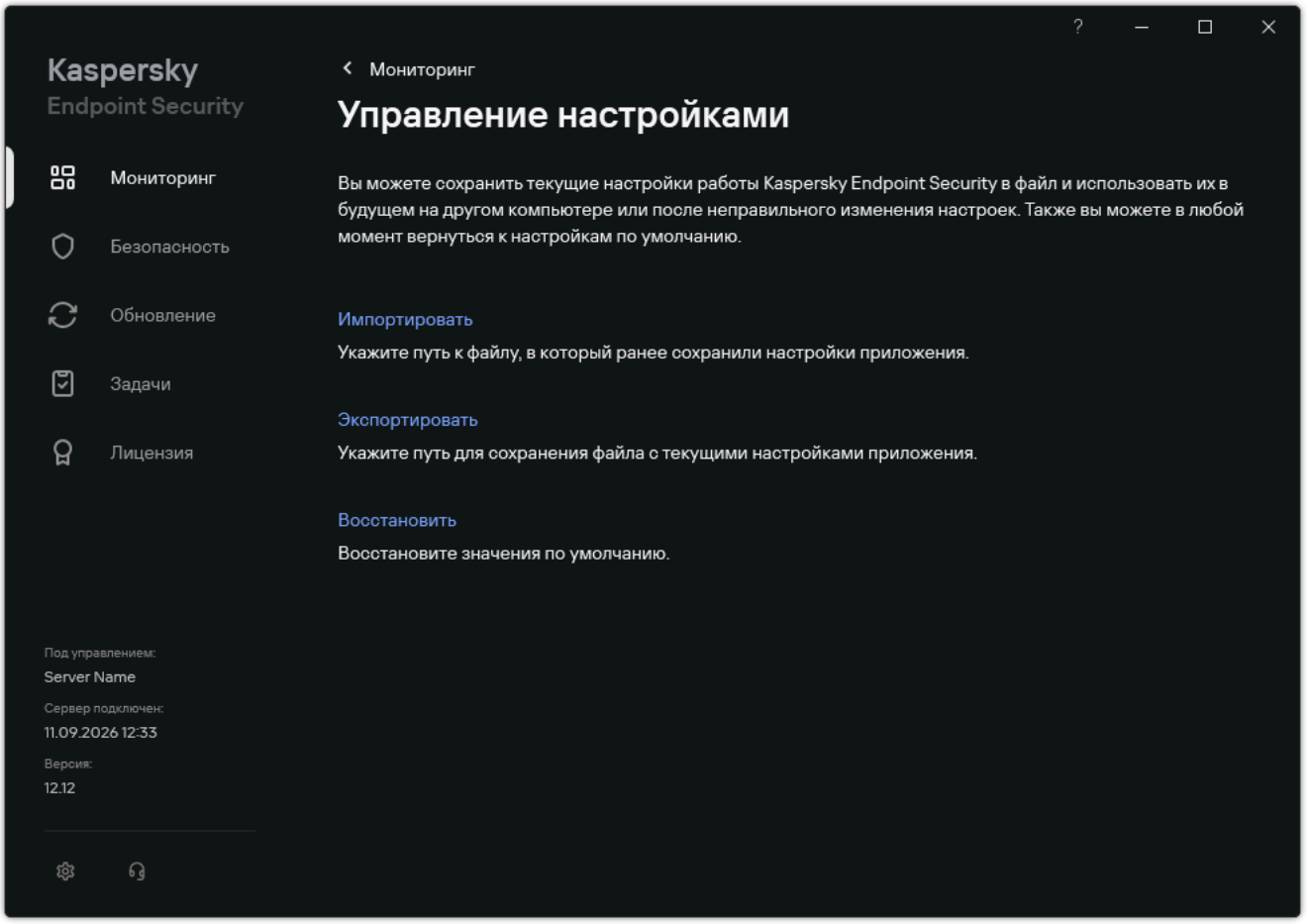
1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Управление настройками**.
3. Нажмите на кнопку **Импортировать**.
4. В открывшемся окне укажите путь к конфигурационному файлу.

5. Если конфигурационный файл зашифрован, введите пароль, который вы задали при экспорте.

Если вы забыли пароль для шифрования конфигурационного файла, восстановить пароль невозможно. В этом случае необходимо повторно выполнить процедуру экспорта конфигурационного файла.

6. Откройте файл.

Все значения параметров Kaspersky Endpoint Security будут установлены в соответствии с выбранным конфигурационным файлом.



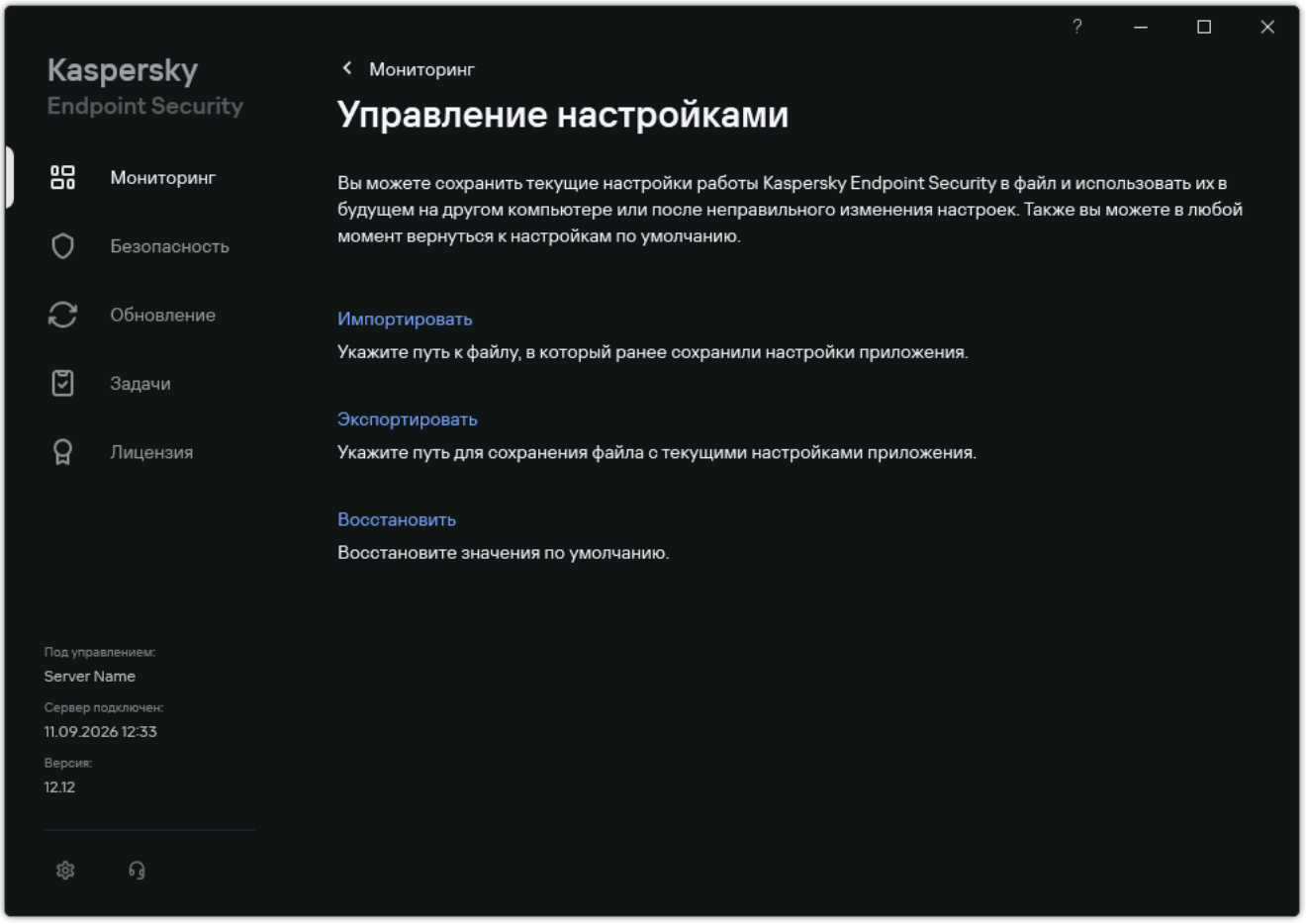
Управление настройками приложения

Восстановление параметров приложения по умолчанию

Вы в любое время можете восстановить настройки приложения, рекомендуемые "Лабораторией Касперского". В результате восстановления настроек для всех компонентов защиты будет установлен уровень безопасности **Рекомендуемый**.

Чтобы восстановить параметры приложения по умолчанию, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Управление настройками**.
3. Нажмите на кнопку **Восстановить**.
4. Сохраните внесенные изменения.



Управление настройками приложения

Производительность Kaspersky Endpoint Security и совместимость с другими приложениями

Под производительностью Kaspersky Endpoint Security подразумевается количество обнаруживаемых типов объектов, которые могут нанести вред компьютеру, а также потребление энергии и ресурсов компьютера.

Выбор типов обнаруживаемых объектов

Kaspersky Endpoint Security позволяет гибко настраивать защиту компьютера и выбирать типы объектов, которые приложение обнаруживает в ходе работы. Kaspersky Endpoint Security всегда проверяет операционную систему на наличие вирусов, червей и троянских приложений. Вы не можете выключить проверку этих типов объектов. Такие приложения могут нанести значительный вред компьютеру пользователя. Чтобы обеспечить большую безопасность компьютера, вы можете расширить список обнаруживаемых типов объектов, включив контроль действий легальных приложений, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Использование режима энергосбережения

Во время работы на портативных компьютерах потребление приложениями энергоресурсов имеет особое значение. Зачастую задачи, которые Kaspersky Endpoint Security выполняет по расписанию, требуют значительного количества ресурсов. При питании компьютера от аккумулятора для экономии его заряда вы можете использовать режим энергосбережения.

Режим энергосбережения позволяет автоматически откладывать выполнение задач, для которых установлен запуск по расписанию:

- задача полной проверки;
- задача проверки важных областей;
- задача выборочной проверки;
- задача проверки целостности.

Независимо от того, включен режим энергосбережения или нет, Kaspersky Endpoint Security приостанавливает выполнение задач шифрования при переходе портативного компьютера в режим работы от аккумулятора. При выходе портативного компьютера из режима работы от аккумулятора в режим работы от сети приложение возобновляет выполнение задач шифрования.

Передача ресурсов компьютера другим приложениям

Потребление ресурсов компьютера при проверке компьютера может увеличить нагрузку на центральный процессор и дисковые подсистемы. Чтобы решить проблему совместной работы при увеличении нагрузки на процессор и дисковые подсистемы, Kaspersky Endpoint Security может уступать ресурсы другим приложениям.

Применение технологии лечения активного заражения

Современные вредоносные приложения могут внедряться на самые нижние уровни операционной системы, что делает их удаление практически невозможным. Обнаружив вредоносную активность в операционной системе, Kaspersky Endpoint Security выполняет расширенную процедуру лечения, применяя специальную технологию лечения активного заражения. *Технология лечения активного заражения* направлена на лечение операционной системы от вредоносных приложений, которые уже запустили свои процессы в оперативной памяти и мешают Kaspersky Endpoint Security удалить их с помощью других методов. В результате угроза нейтрализуется. В процессе процедуры лечения активного заражения не рекомендуется запускать новые процессы или редактировать реестр операционной системы. Технология лечения активного заражения требует значительных ресурсов операционной системы, что может замедлить работу других приложений.

После окончания процедуры лечения активного заражения на компьютере под управлением операционной системы Microsoft Windows для рабочих станций Kaspersky Endpoint Security запрашивает у пользователя разрешение на перезагрузку компьютера. После перезагрузки компьютера Kaspersky Endpoint Security удаляет файлы вредоносного программного обеспечения и запускает облегченную полную проверку компьютера.

Запрос перезагрузки на компьютере под управлением операционной системы Microsoft Windows для серверов невозможен из-за особенностей приложения Kaspersky Endpoint Security. Незапланированная перезагрузка файлового сервера может повлечь за собой проблемы, связанные с временным отказом доступа к данным файлового сервера или потерей несохраненных данных. Перезагрузку файлового сервера рекомендуется выполнять строго по расписанию. Поэтому по умолчанию технология лечения активного заражения для файловых серверов выключена.

В случае обнаружения активного заражения на файловом сервере, на Kaspersky Security Center передается событие о необходимости лечения активного заражения. Для лечения активного заражения на сервере требуется включить технологию лечения активного заражения для серверов и запустить групповую задачу *Поиск вредоносного ПО* в удобное для пользователей сервера время.

Включение и выключение режима энергосбережения

Режим энергосбережения – это функция, позволяющая снизить нагрузку на ресурсы ноутбука и продлить время работы от аккумулятора без существенного ухудшения уровня защиты. В режиме энергосбережение приложения ограничивает запуск задач расписанию. Таким образом, режим энергосбережения позволяет обеспечить баланс между уровнем защиты и длительностью автономной работы ноутбука.

Если включен режим энергосбережения, при работе от аккумулятора не запускаются следующие задачи, даже если для них задан запуск по расписанию:

- *Полная проверка*;
- *Проверка важных областей*;
- *Выборочная проверка*;
- *Проверка целостности приложения*;

- *Поиск IOC*;
- *Обновление баз и модулей приложения* (только патчи).

Приложение пропускает обновление антивирусных баз по расписанию только в том случае когда ноутбук работает от аккумулятора и уровень заряда аккумулятора ниже 30% (значение по умолчанию). Вы можете изменить минимальный уровень заряда аккумулятора, при котором приложение пропускает обновление антивирусных баз по расписанию, через реестр (см. инструкции ниже). В остальных случаях Kaspersky Endpoint Security обновляет антивирусные базы по расписанию независимо от того, подключен ноутбук к сети или работает от аккумулятора, а также от статуса режима энергосбережения приложения.

Как включить или выключить режим энергосбережения в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Общие настройки** → **Настройки приложения**.
5. В блоке **Производительность** используйте флажок **Откладывать задачи по расписанию при работе от аккумулятора**, чтобы включить или выключить режим энергосбережения.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

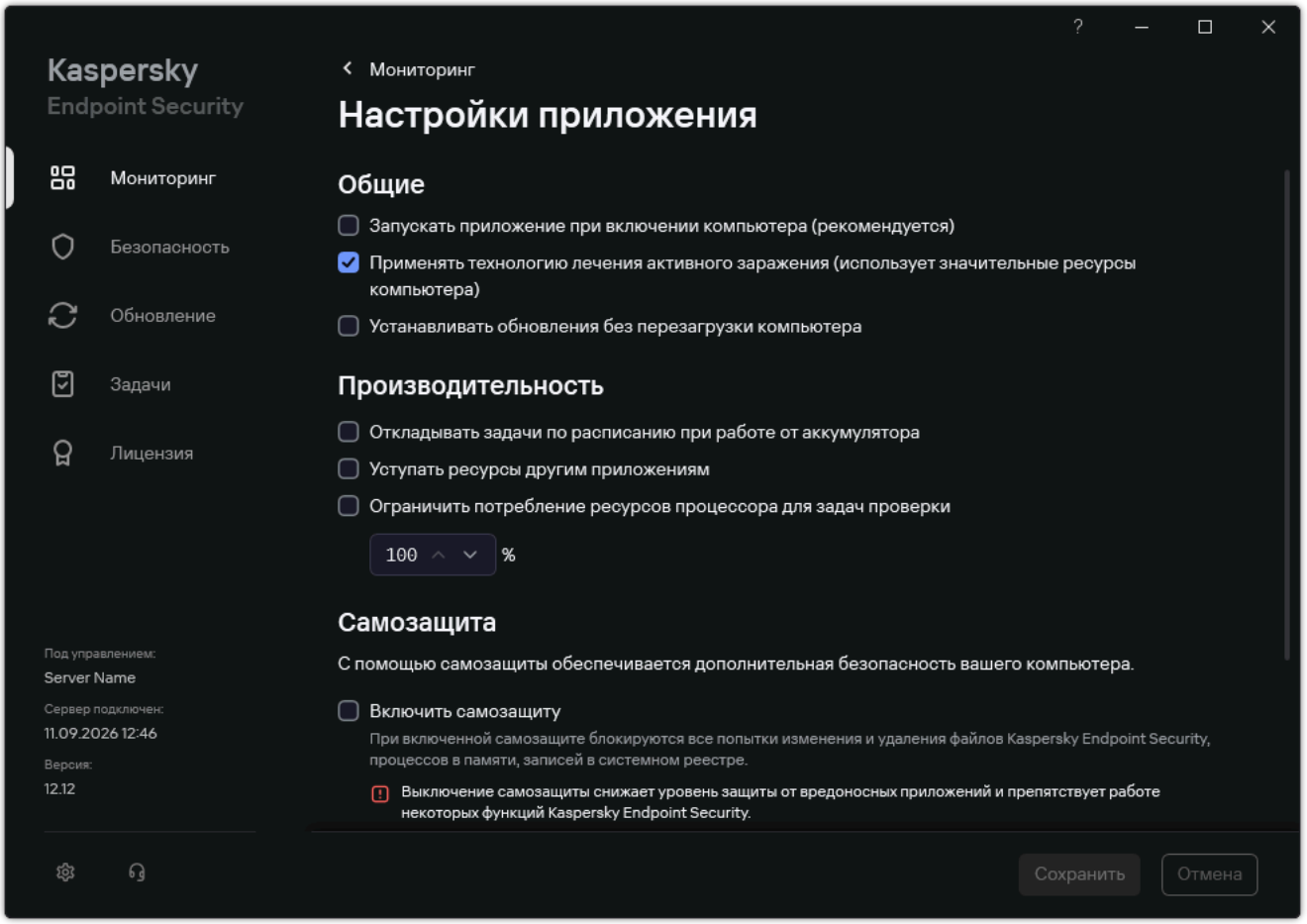
Как включить или выключить режим энергосбережения в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Производительность**.
5. В блоке **Откладывать или пропускать задачи по расписанию при работе от аккумулятора** используйте флажок **Откладывать или пропускать задачи по расписанию при работе от аккумулятора**, чтобы включить или выключить режим энергосбережения.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить режим энергосбережения в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.



Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Производительность** используйте флажок **Откладывать задачи по расписанию при работе от аккумулятора**, чтобы включить или выключить режим энергосбережения.
4. Сохраните внесенные изменения.

Как изменить минимальный уровень заряда, при котором приложение пропускает обновление антивирусных баз по расписанию

1. Откройте редактор реестра на компьютере.
2. В редакторе реестра перейдите в раздел:
   - для 64-битных операционных систем: `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.3\environment]`
   - для 32-битных операционных систем: `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.3\environment]`.
3. Откройте параметр `UpdaterAccumulatorThreshold` на редактирование.
4. Укажите минимальный уровень заряда аккумулятора, при котором приложение пропускает обновление антивирусных баз по расписанию.

Включение и выключение режима передачи ресурсов другим приложениям

Потребление ресурсов компьютера Kaspersky Endpoint Security при проверке компьютера может увеличить нагрузку на центральный процессор и дисковые подсистемы. Это может замедлить работу других приложений. Для оптимизации производительности в Kaspersky Endpoint Security предусмотрен *режим передачи ресурсов другим приложениям*. В этом режиме операционная система может понизить приоритет потоков задач проверки Kaspersky Endpoint Security при высокой нагрузке на центральный процессор. Это позволит перераспределить ресурсы операционной системы для других приложений. То есть задачи проверки получат меньше процессорного времени. В результате Kaspersky Endpoint Security будет проверять компьютер дольше. По умолчанию режим передачи ресурсов другим приложениям включен.

Как включить или выключить режим передачи ресурсов другим приложениям в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Настройки приложения**.
4. В блоке **Производительность** используйте флажок **Уступать ресурсы другим приложениям**, чтобы включить или выключить режим передачи ресурсов другим приложениям.
5. Сохраните внесенные изменения.

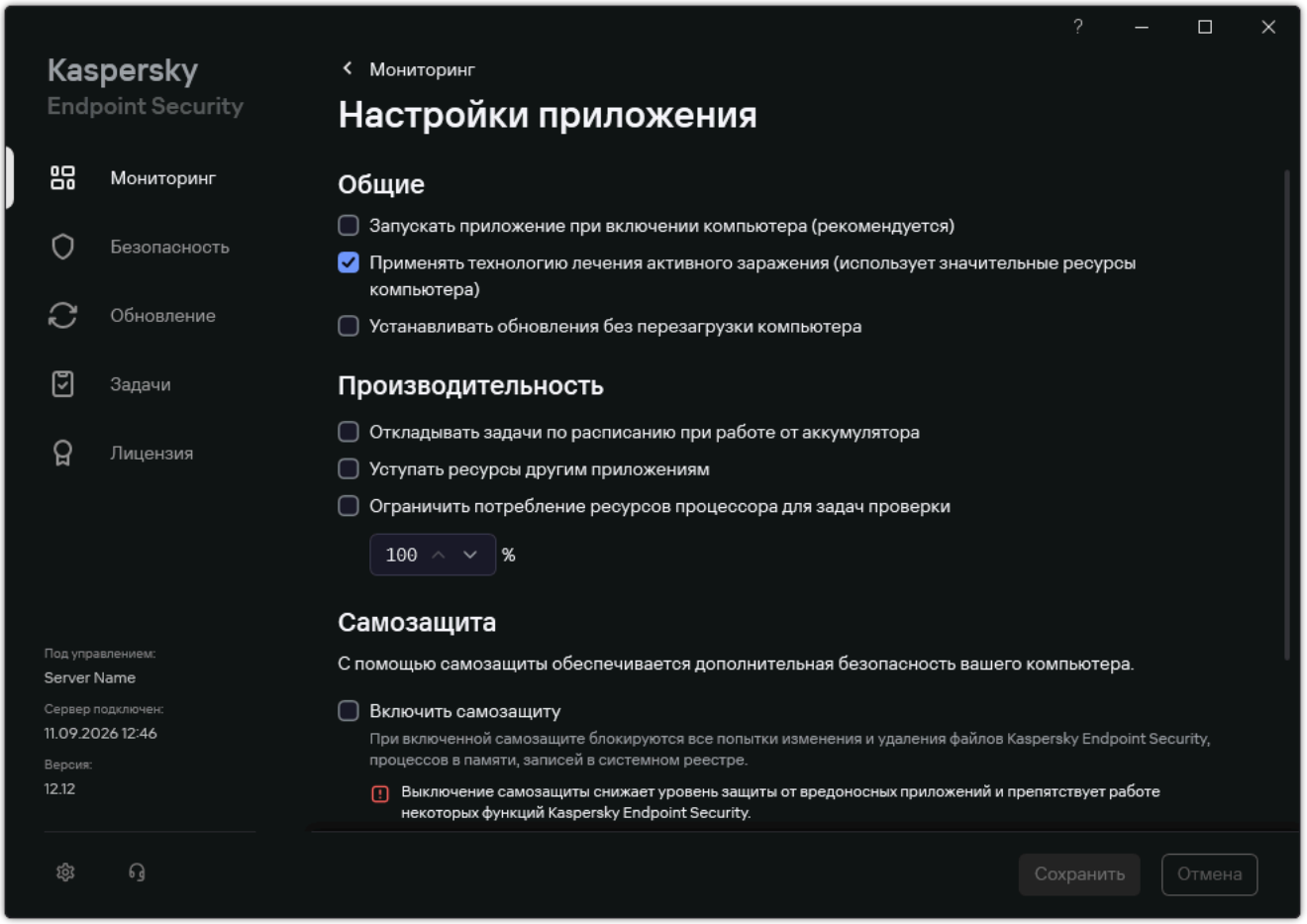
Как включить или выключить режим передачи ресурсов другим приложениям в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Производительность**.
5. В блоке **Уступать ресурсы другим приложениям** используйте переключатель **Уступать ресурсы другим приложениям**, чтобы включить или выключить режим передачи ресурсов другим приложениям.
6. Сохраните внесенные изменения.

Как включить или выключить режим передачи ресурсов другим приложениям в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.



Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Производительность** используйте флажок **Уступать ресурсы другим приложениям**, чтобы включить или выключить режим передачи ресурсов другим приложениям.
4. Сохраните внесенные изменения.

Лучшие практики по оптимизации производительности Kaspersky Endpoint Security

При развертывании Kaspersky Endpoint Security для Windows вы можете использовать следующие рекомендации для настройки защиты компьютеров и оптимизации производительности. Также при проблемах производительности компьютера см. базу знаний Службы технической поддержки.

Общее

Настройте общие параметры приложения в соответствии со следующими рекомендациями:

1. Обновите Kaspersky Endpoint Security до последней версии.

   В новых версиях приложения исправлены ошибки, повышена стабильность работы, а также оптимизирована производительность.

2. Включите компоненты защиты с параметрами по умолчанию.

   Параметры приложения по умолчанию считаются оптимальными. Эти параметры рекомендованы специалистами "Лаборатории Касперского". Параметры по умолчанию обеспечивают рекомендуемый уровень защиты и оптимальное потребление ресурсов компьютера. Если требуется, вы можете восстановить параметры приложения по умолчанию.

3. Включите функции оптимизации производительности приложения.

   Приложение имеет функции оптимизации производительности: режим энергосбережения и режим передачи ресурсов другим приложениям. Убедитесь, что эти режимы включены.

Поиск вредоносного ПО на рабочих станциях

Для поиска вредоносного ПО на рабочих станциях рекомендуется использовать фоновую проверку. *Фоновая проверка* – это режим проверки Kaspersky Endpoint Security без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security проверяет объекты автозапуска, загрузочного сектора, системной памяти и системного раздела. Параметры фоновой проверки считаются оптимальными. Эти параметры рекомендованы специалистами "Лаборатории Касперского". Таким образом, для поиска вредоносного ПО вы можете использовать только режим фоновой проверки и не использовать другие задачи проверки.

Если фоновая проверка вам не подходит, настройте параметры задачи *Поиск вредоносного ПО* в соответствии со следующими рекомендациями:

1. Установите ограничение на потребление ресурсов процессора при проверке компьютера.

   Вы можете ограничить потребление ресурсов процессора при выполнении задачи *Поиск вредоносного ПО*. Для этого вам нужно в параметрах приложения установить максимальное значение нагрузки на все ядра процессора при проверке компьютера в процентах. При этом время проверки компьютера может увеличиться.

2. Настройте оптимальное расписание проверки компьютера.

   Вы можете настроить запуск задачи во время, когда компьютер наименее нагружен. Например, вы можете настроить запуск задачи ночью или в выходные дни.

   Если пользователи выключают компьютер в нерабочее время, вы можете включить функцию Wake-on-LAN. Функция Wake-on-LAN позволяет удаленно включать компьютер с помощью отправки специального сигнала через локальную сеть. Для использования этой функции необходимо включить Wake-on-LAN в параметрах BIOS компьютера. Также вы можете включить автоматическое выключение компьютера после выполнения проверки.

Если настроить оптимальное расписание проверки не удалось, включите выполнение задачи во время простоя компьютера. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка. Если вы прервали выполнение задачи и, например, разблокировали компьютер, Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана.

3. Сформируйте область проверки.

   Выберите следующие объекты для проверки (минимальный набор областей проверки):

   - память ядра;
   - запущенные процессы и объекты автозапуска;
   - загрузочные секторы;
   - %systemroot% (не включая вложенные папки);
   - %systemroot%\System (не включая вложенные папки);
   - %systemroot%\System32 (не включая вложенные папки);
   - %systemroot%\System32\drivers (не включая вложенные папки);
   - %systemroot%\SysWOW64 (не включая вложенные папки);
   - %systemroot%\SysWOW64\drivers (не включая вложенные папки).

4. Включите использование технологий iSwift и iChecker.

   - Технология iSwift.

     Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.

   - Технология iChecker.

     Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

   Вы можете включить использование технологий iSwift и iChecker только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security. Включить использование технологий в Kaspersky Security Center Web Console невозможно.

5. Выключите проверку архивов, защищенных паролем.

   Если проверка архивов, защищенных паролем, включена, перед проверкой архива на экран выводится запрос пароля. Так как есть рекомендация по настройке расписания запуска задачи в нерабочее время, пользователь не может ввести пароль. Вы можете проверять архивы, защищенные паролем, вручную.

6. Выключите запуск нескольких задач проверки одновременно.

   Kaspersky Endpoint Security ставит новые задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер.

Поиск вредоносного ПО на серверах

Настройте параметры задачи *Поиск вредоносного ПО* в соответствии со следующими рекомендациями:

1. Установите ограничение на потребление ресурсов процессора при проверке компьютера.

   Вы можете ограничить потребление ресурсов процессора при выполнении задачи *Поиск вредоносного ПО*. Для этого вам нужно в параметрах приложения установить максимальное значение нагрузки на все ядра процессора при проверке компьютера в процентах. При этом время проверки компьютера может увеличиться.

2. Настройте оптимальное расписание проверки компьютера.

   Вы можете настроить запуск задачи во время, когда компьютер наименее нагружен. Например, вы можете настроить запуск задачи ночью или в выходные дни.

3. Включите использование технологий iSwift и iChecker.

   - Технология iSwift.

     Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.

   - Технология iChecker.

     Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

   Вы можете включить использование технологий iSwift и iChecker только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security. Включить использование технологий в Kaspersky Security Center Web Console невозможно.

4. Выключите проверку архивов, защищенных паролем.

   Если проверка архивов, защищенных паролем, включена, перед проверкой архива на экран выводится запрос пароля. Так как есть рекомендация по настройке расписания запуска задачи в нерабочее время, пользователь не может ввести пароль. Вы можете проверять архивы, защищенные паролем, вручную.

5. Выключите запуск нескольких задач проверки одновременно.

   Kaspersky Endpoint Security ставит новые задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер.

Kaspersky Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть Kaspersky Security Network.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, приложение Kaspersky Endpoint Security получает от служб KSN сведения о репутации проверяемых веб-адресов, а также сведения о категории и репутации проверяемых файлов.

Настройте параметры Kaspersky Security Network в соответствии со следующими рекомендациями:

1. Выключите расширенный режим KSN.

   Расширенный режим KSN – режим работы приложения, при котором Kaspersky Endpoint Security передает в "Лабораторию Касперского" дополнительные данные.

2. Настройте использование Kaspersky Private Security Network.

   Kaspersky Private Security Network (KPSN) – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров.

3. Включите облачный режим.

   Облачный режим – режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию антивирусных баз. Работу приложения с облегченными антивирусными базами обеспечивает Kaspersky Security Network. Облегченная версия антивирусных баз позволяет снизить нагрузку на оперативную память компьютера примерно в два раза. Если вы не участвуете в Kaspersky Security Network или облачный режим выключен, Kaspersky Endpoint Security загружает полную версию антивирусных баз с серверов "Лаборатории Касперского".

Поиск вредоносного ПО

Проверка на наличие вредоносного ПО является важным фактором для обеспечения безопасности компьютера. Требуется регулярно выполнять поиск вредоносного ПО, чтобы исключить возможность распространения вредоносных приложений, которые не были обнаружены компонентами защиты, например, из-за установленного низкого уровня защиты или по другим причинам.

Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive, и создает в журнале записи о том, что эти файлы не были проверены.

Полная проверка

Тщательная проверка всей системы. Kaspersky Endpoint Security проверяет следующие объекты:

- память ядра;
- объекты, загрузка которых осуществляется при запуске операционной системы;
- загрузочные секторы;
- резервное хранилище операционной системы;
- все жесткие и съемные диски.

Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задачи *Полная проверка*.

Для экономии ресурсов компьютера рекомендуется вместо задачи полной проверки использовать задачу фоновой проверки. Уровень защиты компьютера при этом не изменится.

Проверка важных областей

По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задачи *Проверка важных областей*.

Выборочная проверка

Kaspersky Endpoint Security проверяет объекты, выбранные пользователем. Вы можете проверить любой объект из следующего списка:

- системная память;
- объекты, загрузка которых осуществляется при запуске операционной системы;
- резервное хранилище операционной системы;
- жесткие, съемные и сетевые диски;
- любой выбранный файл.

Фоновая проверка

Фоновая проверка – это режим проверки Kaspersky Endpoint Security без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security проверяет объекты автозапуска, загрузочного сектора, системной памяти и системного раздела.

Проверка целостности приложения

Kaspersky Endpoint Security проверяет модули приложения на наличие повреждений или изменений.

Проверка компьютера

Проверка является важным фактором для обеспечения безопасности компьютера. Требуется регулярно выполнять поиск вредоносного ПО, чтобы исключить возможность распространения вредоносных приложений, которые не были обнаружены компонентами защиты, например, из-за установленного низкого уровня защиты или по другим причинам. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

В Kaspersky Endpoint Security предустановлены стандартные задачи *Полная проверка*, *Проверка важных областей*, *Выборочная проверка*. Если в вашей организации развернута система администрирования Kaspersky Security Center, вы можете создать задачу *Поиск вредоносного ПО* и настроить параметры проверки.

Как запустить проверку в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.

3. Выберите задачу проверки и откройте свойства задачи двойным щелчком мыши.

   Если требуется, создайте задачу *Поиск вредоносного ПО*.

4. В окне свойств задачи выберите раздел **Настройки**.

5. Настройте параметры задачи проверки (см. таблицу ниже).

   Если требуется, настройте расписание запуска задачи проверки.

6. Сохраните внесенные изменения.

7. Запустите задачу проверки.

Kaspersky Endpoint Security запустит проверку компьютера. Если пользователь прервал выполнение задачи (например, выключил компьютер), Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана.

Как запустить проверку в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

   Откроется список задач.

2. Нажмите на задачу проверки.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. Настройте параметры задачи проверки (см. таблицу ниже).

   Если требуется, настройте расписание запуска задачи проверки.

5. Сохраните внесенные изменения.

6. Запустите задачу проверки.

Kaspersky Endpoint Security запустит проверку компьютера. Если пользователь прервал выполнение задачи (например, выключил компьютер), Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана.

Как запустить проверку в интерфейсе приложения

1. В главном окне приложения перейдите в раздел **Задачи**.

2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.

> Если задача проверки не отображается, администратор запретил использование локальных задач в политике.

> В интерфейсе приложения можно настроить только локальные задачи проверки: *Полная проверка*, *Проверка важных областей*, *Выборочная проверка*. Настроить параметры групповых задач, добавленных через консоль Kaspersky Security Center, в интерфейсе приложения невозможно. Для групповых задач приложение скрывает кнопку ⚙.

3. Настройте параметры задачи проверки (см. таблицу ниже).

   Если требуется, настройте расписание запуска задачи проверки.

4. Сохраните внесенные изменения.

5. Запустите задачу проверки.

   Kaspersky Endpoint Security запустит проверку компьютера. Приложение покажет процесс проверки, количество проверенных файлов и оставшиеся время. Вы можете остановить выполнение задачи в любое время по кнопке **Стоп**.

Для оптимизации производительности Kaspersky Endpoint Security во время проверки компьютера вы можете настроить дополнительные параметры задачи *Полная проверка* и ограничить потребление ресурсов процессора.

Также в Kaspersky Security Center доступна задача *Фоновая проверка*, которую можно использовать вместо задачи *Полная проверка* для оптимизации производительности приложения. Уровень защиты компьютера при этом не изменится. Настроить параметры фоновой проверки невозможно.

В результате Kaspersky Endpoint Security проверит компьютер и при обнаружении угроз выполнит действие, заданное в параметрах приложения. Обычно приложение пытается вылечить зараженные файлы. При этом зараженные файлы могут получать следующие статусы:

- **Отложено**. Вылечить зараженный файл не удалось. Приложение удалит зараженный файл после перезагрузки компьютера.
- **Записано в отчет**. Вылечить зараженный файл не удалось. Приложение добавит информацию об обнаруженных зараженных файлах в список активных угроз.
- **Запись не поддерживается** или **Ошибка записи**. Вылечить зараженный файл не удалось. У приложения нет прав на запись.
- **Обработка уже выполнена**. Приложение обнаружило зараженный файл ранее. Приложение вылечит или удалит зараженный файл после перезагрузки компьютера.

Параметры проверки

Параметр	Описание
Уровень безопасности	Для проверки Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Высокий**. Приложение Kaspersky Endpoint Security проверяет файлы всех типов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Глубокий**. • **Рекомендуемый**. Приложение Kaspersky Endpoint Security проверяет файлы всех типов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Средний**. • **Низкий**. Приложение Kaspersky Endpoint Security проверяет только файлы определенных форматов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Поверхностный**. Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

Параметр	Описание
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл. **Лечить. Информировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security добавляет информацию об обнаруженных зараженных файлах в список активных угроз. **Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз. Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить. При обнаружении зараженных файлов, являющихся частью приложения Windows Store, Kaspersky Endpoint Security пытается удалить файл.
Выполнять лечение активного заражения немедленно *(доступен только в консоли Kaspersky Security Center)*	Лечение активного заражения в ходе выполнения задачи поиска вирусов на компьютере осуществляется только в том случае, если в свойствах примененной к этому компьютеру политики включена функция лечения активного заражения. Если флажок установлен, Kaspersky Endpoint Security лечит активное заражение сразу после его обнаружения в ходе выполнения задачи поиска вирусов. После лечения активного заражения Kaspersky Endpoint Security перезагружает компьютер, не запрашивая подтверждение у пользователя. Если флажок снят, Kaspersky Endpoint Security не лечит активное заражение сразу после его обнаружения в ходе выполнения задачи поиска вирусов. Приложение формирует события об активном заражении в локальных отчетах приложения и на стороне Kaspersky Security Center. Лечение активного заражения возможно при повторном запуске задачи поиска вирусов с включенной функцией лечения активного заражения. Таким образом, системный администратор имеет возможность выбрать подходящее время для лечения активного заражения компьютеров и их последующей автоматической перезагрузки.
Область проверки	Список объектов, которые Kaspersky Endpoint Security проверяет во время выполнения задачи проверки. Объектом проверки может быть память ядра, запущенные процессы, загрузочные секторы, системное резервное хранилище, жесткий, съемный или сетевой диск, папка или файл. В Kaspersky Endpoint Security для Windows версии 12.12 почта исключена из области проверки приложения. Проверку входящих и исходящих сообщений выполняет компонент Защита от почтовых угроз. Если вы используете плагин управления более ранней версии, то приложение исключает почту из области проверки, даже если эта область включена в политике.
Расписание проверки	**Вручную**. Режим запуска, при котором вы запускаете проверку вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.
Отложить запуск после старта приложения на N минут	Отложенный запуск задачи проверки после старта приложения. После старта операционной системы запускается множество процессов, поэтому удобно запускать задачу проверки не сразу после запуска Kaspersky Endpoint Security, а через некоторое время.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Endpoint Security запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.

Параметр	Описание
Выполнять только во время простоя компьютера	Отложенный запуск задачи, если ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка. Если вы прервали выполнение задачи и, например, разблокировали компьютер, Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана. Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.
Запускать проверку с правами	По умолчанию задача проверки запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Область защиты может включать сетевые диски или другие объекты, для доступа к которым нужны специальные права. Вы можете указать пользователя, обладающего этими правами, в параметрах приложения, и запускать задачу проверки от имени этого пользователя.
Типы файлов Файлы без расширения приложение Kaspersky Endpoint Security считает исполняемыми. Приложение проверяет исполняемые файлы всегда, независимо от того, файлы какого типа вы выбрали для проверки. **Все файлы**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений). **Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла. **Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения. По умолчанию Kaspersky Endpoint Security проверяет файлы по формату. Проверять файлы по расширению менее безопасно, так как вредоносный файл может иметь расширение, которое не входит в список потенциально заражаемых (например, `.123`).	
Проверять только новые и измененные файлы	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Пропускать файл, если его проверка длится более N секунд	Ограничение длительности проверки файла. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку текущего файла и начинает проверку следующего. Это ускоряет проверку компьютера, но снижает уровень защиты. По умолчанию Kaspersky Endpoint Security прекращает проверку файла по истечении 30 секунд.
Не запускать несколько задач проверки одновременно	Отложенный запуск задач проверки, запланированных по расписанию, если запущенная ранее проверка по расписанию еще выполняется. Kaspersky Endpoint Security ставит запланированные задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, вы запланировали запуск задач проверки в 18:00 и в 20:00. Kaspersky Endpoint Security отложит запуск задачи проверки в 20:00, если задача проверки, запущенная в 18:00, еще выполняется. Приложение запустит проверку после завершения задачи, запущенной в 18:00. Kaspersky Endpoint Security запускает задачу проверки немедленно, даже если запущена другая задача проверки, в следующих случаях: • Проверка съемного диска при подключении. • Проверка из контекстного меню. • Проверка важных областей, запущенная в результате обнаружения индикатора компрометации (IOC). Если флажок снят, Kaspersky Endpoint Security позволяет запускать несколько задач проверки одновременно. Запуск нескольких задач проверки требует больше ресурсов компьютера.
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	Проверка дистрибутивов сторонних приложений.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.

Параметр	Описание
Проверять файлы почтовых форматов	Проверка файлов почтовых форматов, а также почтовой базы данных. Приложение проверяет PST- и OST-файлы, которые используют почтовые клиенты MS Outlook / Windows Mail, и EML-файлы. Kaspersky Endpoint Security не поддерживает работу с 64-битной версией почтового клиента Microsoft Outlook. То есть, Kaspersky Endpoint Security не проверяет файлы, связанные с работой 64-битной версии почтового клиента Microsoft Outlook (PST- и OST-файлы), даже если почта включена в область проверки. Если флажок установлен, Kaspersky Endpoint Security разбирает файл почтового формата на составляющие части (заголовок, тело, вложения) и анализирует их на наличие угроз. Если флажок снят, Kaspersky Endpoint Security проверяет файл почтового формата как единый файл. При обнаружении вредоносного объекта в PST- и OST-файлах Kaspersky Endpoint Security обезвреживает его в соответствии с выбранным действием (например, лечение или удаление файла). При обнаружении вредоносных объектов в файлах других почтовых клиентов (например, Mozilla Thunderbird), Kaspersky Endpoint Security не выполняет лечение или удаление таких файлов во избежание нежелательного удаления ваших сообщений электронной почты. Приложение только добавляет информацию об обнаруженных объектах в список активных угроз. Вам необходимо самостоятельно в интерфейсе почтового клиента удалить письма с вредоносными файлами во вложении. Если удаление писем с вредоносными объектами по какой-то причине в данный момент недоступно, вы можете обработать данные угрозы в интерфейсе Kaspersky Endpoint Security, добавив обнаруженные объекты в список исключений из проверки.
Проверять архивы, защищенные паролем	Если флажок установлен, приложение проверяет архивы, защищенные паролем. Перед проверкой файлов, содержащихся в архиве, на экран выводится запрос пароля. Если флажок не установлен, приложение пропускает проверку защищенных паролем архивов.
Не распаковывать составные файлы большого размера	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.
Машинное обучение и сигнатурный анализ	При методе проверки Машинное обучение и сигнатурный анализ используются базы Kaspersky Endpoint Security, содержащие описания известных угроз и методы их устранения. Защиту с использованием этого метода проверки обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.
Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Технология iSwift *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
Технология iChecker *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Проверка съемных дисков при подключении к компьютеру

Kaspersky Endpoint Security проверяет все файлы, которые вы запускаете или копируете, даже если файл расположен на съемном диске (компонент Защита от файловых угроз). Для предотвращения распространения вирусов и других приложений, представляющих угрозу, вы можете настроить автоматическую проверку съемных дисков при подключении к компьютеру. При обнаружении угрозы Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет. Компонент обеспечивает защиту компьютера с помощью следующих методов проверки: машинное обучение, эвристический анализ (высокий уровень) и сигнатурный анализ. Также Kaspersky Endpoint Security использует технологии оптимизации проверки iSwift и iChecker. Технологии включены постоянно и выключить их невозможно.

Как настроить запуск проверки съемных дисков в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Локальные задачи** → **Проверка съемных дисков**.
4. В раскрывающемся списке **Действие при подключении съемного диска** выберите **Подробная проверка** или **Быстрая проверка**.
5. Настройте дополнительные параметры проверки съемных дисков (см. таблицу ниже).
6. Сохраните внесенные изменения.

Как настроить запуск проверки съемных дисков в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Проверка съемных дисков**.
5. Используйте переключатель **Проверка съемных дисков ВКЛЮЧЕНА**, чтобы включить или выключить компонент.
6. В блоке **Тип проверки** выберите **Подробная проверка** или **Быстрая проверка**.
7. Настройте дополнительные параметры проверки съемных дисков (см. таблицу ниже).
8. Сохраните внесенные изменения.

Как настроить запуск проверки съемных дисков в интерфейсе приложения

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.
3. Используйте переключатель **Проверка съемных дисков**, чтобы включить или выключить проверку съемных дисков при подключении к компьютеру.
4. Настройте дополнительные параметры проверки съемных дисков (см. таблицу ниже).
5. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет запускать проверку съемных дисков, размер которых не превышает указанный максимальный размер. Если задача *Проверка съемных дисков* не отображается, администратор запретил использование локальных задач в политике.

Параметры задачи Проверка съемных дисков

Параметр	Описание
Тип проверки	**Подробная проверка**. Если выбран этот вариант, то после подключения съемного диска Kaspersky Endpoint Security проверяет все файлы, расположенные на съемном диске, в том числе вложенные файлы внутри составных объектов, архивы, дистрибутивы, файлы офисных форматов. Kaspersky Endpoint Security не проверяет файлы почтовых форматов и защищенные паролем архивы. **Быстрая проверка**. Если выбран этот вариант, то после подключения съемного диска Kaspersky Endpoint Security проверяет только файлы определенных форматов, наиболее подверженные заражению, а также не распаковывает составные объекты.
Максимальный размер диска (МБ)	Если флажок установлен, то Kaspersky Endpoint Security выполняет выбранное действие над съемными дисками, размер которых не превышает указанный максимальный размер. Если размер съемного диска превышает указанное значение, Kaspersky Endpoint Security пропускает проверку. Если флажок снят, то Kaspersky Endpoint Security выполняет выбранное действие над съемными дисками любого размера.
Скрыть индикатор выполнения задачи проверки	Если флажок установлен, то Kaspersky Endpoint Security отображает ход проверки съемных дисков в отдельном окне, а также в разделе **Задачи**. Если флажок снят, то Kaspersky Endpoint Security выполняет проверку съемных дисков в фоновом режиме.
Запретить пользователям останавливать задачу проверки	Если флажок установлен, то в локальном интерфейсе Kaspersky Endpoint Security для задачи проверки съемных дисков недоступны кнопка **Стоп** в разделе **Задачи** и кнопка **Стоп** в окне проверки съемного диска.

Фоновая проверка

Фоновая проверка – это режим проверки Kaspersky Endpoint Security без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security проверяет объекты автозапуска, загрузочного сектора, системной памяти и системного раздела.

Для экономии ресурсов компьютера рекомендуется вместо задачи полной проверки использовать задачу фоновой проверки. Уровень защиты компьютера при этом не изменится. Область проверки для этих задач одинаковая. Для оптимизации нагрузки на компьютер приложение не запускает задачи полной проверки и фоновой проверки одновременно. Если вы запустили задачу полной проверки, Kaspersky Endpoint Security не будет запускать задачу фоновой проверки в течение семи дней после выполнения полной проверки.

Фоновая проверка запускается в следующих случаях:

- после обновления антивирусных баз;
- через 30 минут после запуска Kaspersky Endpoint Security;
- каждые шесть часов;
- при простое компьютера в течение пяти и более минут (компьютер заблокирован или включена экранная заставка).

Фоновая проверка при простое компьютера прерывается при выполнении любого из следующих условий:

- Компьютер перешел в активный режим.

  Если фоновая проверка не выполнялась более десяти дней, проверка не прерывается.

- Компьютер (ноутбук) перешел в режим питания от батареи.

При выполнении фоновой проверки Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.

Как включить фоновую проверку в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Локальные задачи** → **Фоновая проверка**.
4. Используйте флажок **Включить фоновую проверку**, чтобы включить или выключить фоновую проверку.
5. Сохраните внесенные изменения.

Как включить фоновую проверку в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Защита от файловых угроз**.
5. В блоке **Фоновая проверка** используйте переключатель **Фоновая проверка ВКЛЮЧЕНА**, чтобы включить или выключить фоновую проверку.
6. Сохраните внесенные изменения.

Как включить фоновую проверку в интерфейсе приложения

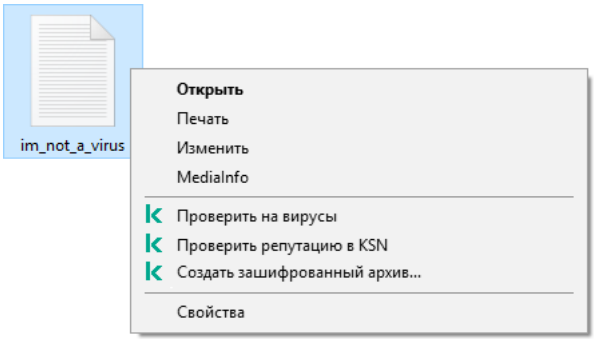
1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.
3. Используйте переключатель **Фоновая проверка**, чтобы включить или выключить фоновую проверку.
4. Сохраните внесенные изменения.

Если задача *Фоновая проверка* не отображается, администратор запретил использование локальных задач в политике.

Проверка из контекстного меню

Kaspersky Endpoint Security позволяет проверять отдельные файлы на вирусы и другие приложения, представляющие угрозу, из контекстного меню (см. рис. ниже).

При выполнении проверки из контекстного меню Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.



Проверка из контекстного меню

Как настроить параметры проверки из контекстного меню в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Локальные задачи** → **Проверка из контекстного меню**.
4. Настройте параметры проверки из контекстного меню (см. таблицу ниже).
5. Сохраните внесенные изменения.

Как настроить параметры проверки из контекстного меню в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз → Защита от файловых угроз**.

5. В блоке **Проверка из контекстного меню** настройте параметры проверки из контекстного меню (см. таблицу ниже).

6. Сохраните внесенные изменения.

Как настроить параметры проверки из контекстного меню в интерфейсе приложения

1. В главном окне приложения перейдите в раздел **Задачи**.

2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.

3. Настройте параметры проверки из контекстного меню (см. таблицу ниже).

4. Сохраните внесенные изменения.

Если задача *Проверка из контекстного меню* не отображается, администратор запретил использование локальных задач в политике.

Параметры задачи Проверка из контекстного меню

Параметр	Описание
Уровень безопасности	Для проверки Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Высокий**. Приложение Kaspersky Endpoint Security проверяет файлы всех типов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Глубокий**. • **Рекомендуемый**. Приложение Kaspersky Endpoint Security проверяет файлы всех типов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Средний**. • **Низкий**. Приложение Kaspersky Endpoint Security проверяет только файлы определенных форматов. Во время проверки составных файлов приложение проверяет архивы, дистрибутивы, файлы офисных форматов, но не проверяет архивы, защищенные паролем. Когда установлен этот уровень безопасности, приложение использует эвристический анализ с уровнем детализации **Поверхностный**.
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл. **Лечить. Информировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security добавляет информацию об обнаруженных зараженных файлах в список активных угроз. **Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз.
Типы файлов	Файлы без расширения приложение Kaspersky Endpoint Security считает исполняемыми. Приложение проверяет исполняемые файлы всегда, независимо от того, файлы какого типа вы выбрали для проверки. **Все файлы**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений). **Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла. **Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения. По умолчанию Kaspersky Endpoint Security проверяет файлы по формату. Проверять файлы по расширению менее безопасно, так как вредоносный файл может иметь расширение, которое не входит в список потенциально заражаемых (например, `.123`).

Параметр	Описание
Проверять только новые и измененные файлы	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Пропускать файл, если его проверка длится более N секунд	Ограничение длительности проверки файла. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку текущего файла и начинает проверку следующего. Это ускоряет проверку компьютера, но снижает уровень защиты. По умолчанию Kaspersky Endpoint Security прекращает проверку файла по истечении 30 секунд.
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Проверять файлы почтовых форматов	Проверка файлов почтовых форматов, а также почтовой базы данных. Приложение проверяет PST- и OST-файлы, которые используют почтовые клиенты MS Outlook / Windows Mail, и EML-файлы. Kaspersky Endpoint Security не поддерживает работу с 64-битной версией почтового клиента Microsoft Outlook. То есть, Kaspersky Endpoint Security не проверяет файлы, связанные с работой 64-битной версии почтового клиента Microsoft Outlook (PST- и OST-файлы), даже если почта включена в область проверки. Если флажок установлен, Kaspersky Endpoint Security разбирает файл почтового формата на составляющие части (заголовок, тело, вложения) и анализирует их на наличие угроз. Если флажок снят, Kaspersky Endpoint Security проверяет файл почтового формата как единый файл. При обнаружении вредоносного объекта в PST- и OST-файлах Kaspersky Endpoint Security обезвреживает его в соответствии с выбранным действием (например, лечение или удаление файла). При обнаружении вредоносных объектов в файлах других почтовых клиентов (например, Mozilla Thunderbird), Kaspersky Endpoint Security не выполняет лечение или удаление таких файлов во избежание нежелательного удаления ваших сообщений электронной почты. Приложение только добавляет информацию об обнаруженных объектах в список активных угроз. Вам необходимо самостоятельно в интерфейсе почтового клиента удалить письма с вредоносными файлами во вложении. Если удаление писем с вредоносными объектами по какой-то причине в данный момент недоступно, вы можете обработать данные угрозы в интерфейсе Kaspersky Endpoint Security, добавив обнаруженные объекты в список исключений из проверки.
Проверять архивы, защищенные паролем	Если флажок установлен, приложение проверяет архивы, защищенные паролем. Перед проверкой файлов, содержащихся в архиве, на экран выводится запрос пароля. Если флажок не установлен, приложение пропускает проверку защищенных паролем архивов.
Не распаковывать составные файлы большого размера	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.
Машинное обучение и сигнатурный анализ	При методе проверки Машинное обучение и сигнатурный анализ используются базы Kaspersky Endpoint Security, содержащие описания известных угроз и методы их устранения. Защиту с использованием этого метода проверки обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.
Эвристический анализ	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

Параметр	Описание
Технология iSwift	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
Технология iChecker	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Проверка целостности приложения

Kaspersky Endpoint Security проверяет модули приложения на наличие повреждений или изменений. Например, если библиотека приложения имеет некорректную цифровую подпись, то такая библиотека считается поврежденной. Для проверки файлов приложения предназначена задача *Проверка целостности приложения*. Запускайте задачу *Проверка целостности приложения*, если приложение Kaspersky Endpoint Security обнаружило вредоносный объект и не обезвредило его.

Вы можете создать задачу *Проверка целостности приложения* в Kaspersky Security Center Web Console и Консоли администрирования. Создать задачу в приложении Kaspersky Security Center Cloud Console невозможно.

Нарушения целостности приложения могут, например, возникать в следующих случаях:

- Вредоносный объект внес изменения в файлы Kaspersky Endpoint Security. В этом случае выполните процедуру восстановления Kaspersky Endpoint Security средствами операционной системы. После восстановления запустите полную проверку компьютера и повторите проверку целостности.
- Истек срок действия цифровой подписи. В этом случае обновите Kaspersky Endpoint Security.

Как выполнить проверку целостности приложения через Консоль администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Проверка целостности приложения**.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 3. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или при обнаружении вирусной атаки.

Шаг 4. Определение названия задачи

Введите название задачи, например, *Проверка целостности приложения после заражения компьютера*.

Шаг 5. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи. В результате Kaspersky Endpoint Security выполнит проверку целостности приложения. Вы также можете настроить расписание проверки целостности приложения в свойствах задачи (см. таблицу ниже).

Как выполнить проверку целостности приложения через Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Проверка целостности приложения**.

c. В поле **Название задачи** введите короткое описание, например, *Проверка целостности приложения после заражения компьютера*.

d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

5. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.

6. Завершите работу мастера.

   В списке задач отобразится новая задача.

7. Установите флажок напротив задачи.

В результате Kaspersky Endpoint Security выполнит проверку целостности приложения. Вы также можете настроить расписание проверки целостности приложения в свойствах задачи (см. таблицу ниже).

Как выполнить проверку целостности в интерфейсе приложения

1. В главном окне приложения перейдите в раздел **Задачи**.

2. В открывшемся списке задач выберите задачу *Проверка целостности приложения* и нажмите на кнопку **Запустить**.

В результате Kaspersky Endpoint Security выполнит проверку целостности приложения. Вы также можете настроить расписание проверки целостности приложения в свойствах задачи (см. таблицу ниже). Если задача *Проверка целостности приложения* не отображается, администратор запретил использование локальных задач в политике.

Параметры задачи Проверка целостности

Параметр	Описание
Расписание проверки	**Вручную**. Режим запуска, при котором вы запускаете проверку вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Endpoint Security запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.
Выполнять только во время простоя компьютера	Отложенный запуск задачи, если ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка. Если вы прервали выполнение задачи и, например, разблокировали компьютер, Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана. Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.

Формирование области проверки

Область проверки – список путей к папкам и файлам, которые Kaspersky Endpoint Security проверяет во время выполнения задачи. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

Для формирования области проверки рекомендуется использовать задачу *Выборочная проверка*. Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задач *Полная проверка* и *Проверка важных областей*.

В Kaspersky Endpoint Security предустановлены следующие объекты для формирования области проверки:

- **Системная память**.
- **Запущенные процессы и объекты автозапуска**.

  Память, занятая процессами, и исполняемые файлы приложения, которые запускаются при старте операционной системы.
- **Загрузочные секторы**.

  Загрузочные секторы жестких и съемных дисков.
- **Системное резервное хранилище**.

  Содержимое папки System Volume Information.
- **Все внешние устройства**.
- **Все жесткие диски**.
- **Все сетевые диски**.

  В Kaspersky Endpoint Security для Windows версии 12.12 почта исключена из области проверки приложения. Проверку входящих и исходящих сообщений выполняет компонент Защита от почтовых угроз. Если вы используете плагин управления более ранней версии, то приложение исключает почту из области проверки, даже если эта область включена в политике.

  Для проверки сетевых дисков или сетевых папок рекомендуется создавать отдельную задачу проверки. В параметрах задачи *Поиск вредоносного ПО* укажите пользователя, у которого есть права на запись на этом диске, для устранения обнаруженных угроз. Если на сервере, на котором расположен сетевой диск, установлены собственные инструменты защиты, запускать задачу проверки на этом диске не требуется. Это позволит не проверять объекты дважды и повысит производительность сервера.

Для исключения папок или файлов из области проверки вам нужно добавить папку или файл в доверенную зону.

Как сформировать область проверки в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.
3. Выберите задачу проверки и откройте свойства задачи двойным щелчком мыши.

   Если требуется, создайте задачу *Поиск вредоносного ПО*.
4. В окне свойств задачи выберите раздел **Настройки**.
5. В разделе **Область проверки** нажмите на кнопку **Настройка**.
6. В открывшемся окне выберите объекты, которые вы хотите добавить в область проверки или исключить из нее.
7. Если вы хотите добавить новый объект в область проверки, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   b. В поле **Объект** введите путь к папке или файлу.

   Используйте маски:

   - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.
   - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.
   - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

   Вы можете использовать маски в любом месте пути к файлу или папке. Например, если вы хотите включить в область проверки папку Загрузки для всех учетных записей пользователей компьютера, введите маску `C:\Users\*\Downloads\`.

   Объект **Этот компьютер** в списке файловых ресурсов компьютера включает в себя следующие объекты: **Все жесткие диски**, **Все сетевые диски** и **Все съемные диски**.

   Вы можете исключить объект из проверки, не удаляя его из списка объектов области проверки. Для этого снимите флажок рядом с ним.
8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как сформировать область проверки в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Задачи**.

   Откроется список задач.

2. Нажмите на задачу проверки.

   Откроется окно свойств задачи. Если требуется, создайте задачу *Поиск вредоносного ПО*.

3. Выберите вкладку **Параметры приложения**.

4. В разделе **Область проверки** выберите объекты, которые вы хотите добавить в область проверки или исключить из нее.

5. Если вы хотите добавить новый объект в область проверки, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   b. Введите путь к папке или файлу.

      Используйте маски:

      - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

      - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

      - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

      Вы можете использовать маски в любом месте пути к файлу или папке. Например, если вы хотите включить в область проверки папку Загрузки для всех учетных записей пользователей компьютера, введите маску `C:\Users\*\Downloads\`.

   Вы можете исключить объект из проверки, не удаляя его из списка объектов области проверки. Для этого выключите переключатель рядом с ним.

6. Сохраните внесенные изменения.

Как сформировать область проверки в интерфейсе приложения

1. В главном окне приложения перейдите в раздел **Задачи**.

2. В открывшемся списке задач выберите задачу *Выборочная проверка* и нажмите на кнопку **Выбрать**.

   Вы также можете изменить область проверки для других задач. Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задач *Полная проверка* и *Проверка важных областей*.

3. В открывшемся окне выберите объекты, которые вы хотите добавить в область проверки.

4. Сохраните внесенные изменения.

Если задача проверки не отображается, администратор запретил использование локальных задач в политике.

Запуск проверки по расписанию

Проверка на наличие вредоносного ПО с помощью задачи *Поиск вредоносного ПО* может занимать длительное время и увеличивает потребление Kaspersky Endpoint Security ресурсов компьютера. В связи с этим рекомендуется выбрать оптимальное время для запуска задачи, чтобы минимизировать влияние на производительность других приложений.

Например, если сотрудники вашей организации работают по фиксированному графику, вы можете настроить запуск проверки компьютера ночью или в выходные дни. Если по каким-либо причинам запуск задачи невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи проверки, как только это станет возможным. Данной функцией необходимо пользоваться с осторожностью, так как это может замедлить работу приложений на компьютере пользователя когда он с утра включит компьютер.

Если подобрать оптимальное расписание проверки исходя из ваших потребностей не удалось, вы можете настроить запуск проверки компьютера при выполнении следующих специальных условий:

- После обновления баз.

  Kaspersky Endpoint Security запускает проверку компьютера с обновленными базами сигнатур.

- При запуске приложения.

  Kaspersky Endpoint Security запускает проверку компьютера через заданное время после запуска приложения. После старта операционной системы запускается множество процессов, поэтому удобно запускать задачу проверки не сразу после запуска Kaspersky Endpoint Security, а через некоторое время.

- Функция Wake-on-LAN.

  Kaspersky Endpoint Security запускает проверку компьютера по расписанию даже если компьютер выключен. Для этого приложение использует функцию операционной системы Wake-on-LAN. Функция Wake-on-LAN позволяет удаленно включать компьютер с помощью отправки специального сигнала через локальную сеть. Для использования этой функции необходимо включить Wake-on-LAN в параметрах BIOS компьютера.

  Вы можете настроить запуск проверки компьютера с функцией Wake-on-LAN только для задачи *Поиск вредоносного ПО* в Kaspersky Security Center. Включить функцию Wake-on-LAN для проверки компьютера в интерфейсе приложения невозможно.

- При простое компьютера.

  Kaspersky Endpoint Security запускает проверку компьютера по расписанию, если включена экранная заставка или компьютер заблокирован. Если пользователь разблокировал компьютер, Kaspersky Endpoint Security приостанавливает проверку компьютера. В таком случае полная проверка компьютера может занимать несколько дней.

- Если задача была пропущена.

  Kaspersky Endpoint Security запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени.

Как настроить расписание проверки компьютера в Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на задачу проверки.

   Откроется окно свойств задачи.

3. В окне свойств задачи выберите вкладку **Расписание**.

4. Настройте расписание запуска задачи проверки.

5. В зависимости от выбранной периодичности настройте дополнительные параметры, которые уточняют расписание запуска задачи (см. таблицу ниже).

6. Сохраните внесенные изменения.

Как настроить расписание проверки компьютера в интерфейсе приложения

Вы можете настроить расписание проверки, только если к компьютеру не применена политика. Для компьютеров под политикой вы можете настроить расписание запуска задачи *Поиск вредоносного ПО* в Kaspersky Security Center.

1. В главном окне приложения перейдите в раздел **Задачи**.

2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.

   Вы можете настроить расписание для запуска полной проверки, проверки важных областей и проверки целостности. Выборочную проверку вы можете запускать только вручную.

3. Нажмите на кнопку **Расписание проверки**.

4. В открывшемся окне настройте расписание запуска задачи проверки.

5. В зависимости от выбранной периодичности настройте дополнительные параметры, которые уточняют расписание запуска задачи (см. таблицу ниже).

6. Сохраните внесенные изменения.

Параметры расписания проверки

Параметр	Описание
Расписание проверки	**Вручную**. Режим запуска, при котором вы запускаете проверку вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.
Отложить запуск после старта приложения на N минут	Отложенный запуск задачи проверки после старта приложения. После старта операционной системы запускается множество процессов, поэтому удобно запускать задачу проверки не сразу после запуска Kaspersky Endpoint Security, а через некоторое время.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Endpoint Security запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.

Параметр	Описание
Выполнять только во время простоя компьютера	Отложенный запуск задачи, если ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка. Если вы прервали выполнение задачи и, например, разблокировали компьютер, Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана. Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.
Использовать автоматическое определение случайного интервала между запусками задачи *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, задача запускается на компьютерах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит распределенный запуск задачи. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества компьютеров, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако, когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Использовать случайную задержку запуска задачи в интервале (мин)	Если флажок установлен, задача запускается на компьютерах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Остановить, если задача выполняется дольше (мин) *(доступен только в консоли Kaspersky Security Center)*	Ограничение длительности выполнения задачи. По истечении заданного времени Kaspersky Endpoint Security останавливает выполнение задачи. При этом задача не будет завершена. Следующий запуск задачи Kaspersky Endpoint Security выполнит сначала и по расписанию. Чтобы уменьшить время выполнения задачи, вы можете, например, настроить область проверки или оптимизировать проверку.
Активировать устройства перед запуском задачи функцией Wake-on-LAN за (мин) *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, операционная система на компьютере будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут. Установите флажок, если вы хотите запустить выполнение задачи на всех компьютерах, включая компьютеры, которые выключены.
Выключать устройства после выполнения задачи *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, компьютер будет выключен после выполнения задачи. Например, вы можете включить эту функцию для проверки компьютера в пятницу после рабочего дня. После завершения работы задачи приложение выключает компьютер на выходные.
Приостановить задачу	Вы можете задавать временной интервал, в течение которого выполнение ранее запущенной по расписанию задачи будет приостановлено. По окончании заданного периода времени выполнение задачи будет возобновлено. Это может понадобиться, например, для снижения влияния Kaspersky Endpoint Security на производительность компьютера в период наиболее активного его использования.
Выключить расписание с	Если флажок установлен, Kaspersky Endpoint Security прекратит выполнение задачи по расписанию начиная с указанной даты. Для задачи будет установлен режим запуска **Вручную**.

Запуск проверки с правами другого пользователя

По умолчанию задача проверки запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Область защиты может включать сетевые диски или другие объекты, для доступа к которым нужны специальные права. Вы можете указать пользователя, обладающего этими правами, в параметрах приложения, и запускать задачу проверки от имени этого пользователя.

Вы можете запускать проверку с правами другого пользователя для следующих типов проверки:

- Проверка важных областей.
- Полная проверка.
- Выборочная проверка.
- Проверка из контекстного меню.

Настроить права пользователя для запуска проверки съемных дисков, фоновой проверки и проверки целостности невозможно.

Как запустить проверку с правами другого пользователя в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите вкладку **Задачи**.
4. Выберите задачу проверки и откройте свойства задачи двойным щелчком мыши.
5. В окне свойств задачи выберите раздел **Учетная запись**.
6. Введите учетные данные пользователя, права которого требуется использовать для запуска задачи проверки.
7. Сохраните внесенные изменения.

Как запустить проверку с правами другого пользователя в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

   Откроется список задач.
2. Нажмите на задачу проверки.

   Откроется окно свойств задачи.
3. Выберите вкладку **Параметры**.
4. В блоке **Учетная запись** нажмите на кнопку **Параметры**.
5. Введите учетные данные пользователя, права которого требуется использовать для запуска задачи проверки.
6. Сохраните внесенные изменения.

Как запустить проверку с правами другого пользователя в интерфейсе приложения

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.
3. В свойствах задачи выберите **Расширенная настройка** → **Запускать проверку с правами**.
4. В открывшемся окне введите учетные данные пользователя, права которого требуется использовать для запуска задачи проверки.
5. Сохраните внесенные изменения.

Если задача проверки не отображается, администратор запретил использование локальных задач в политике.

Оптимизация проверки

Контроль потребления ресурсов процессора при проверке компьютера

Вы можете ограничить потребление ресурсов процессора при выполнении задачи *Поиск вредоносного ПО*. При этом время проверки компьютера может увеличиться.

Как ограничить потребление ресурсов процессора при проверке компьютера в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Настройки приложения**.
4. В блоке **Производительность** установите флажок **Ограничить потребление ресурсов процессора для задач проверки** и введите среднее значение потребления ресурсов процессора в процентах.
5. Сохраните внесенные изменения.

Как ограничить потребление ресурсов процессора при проверке компьютера в Web Console

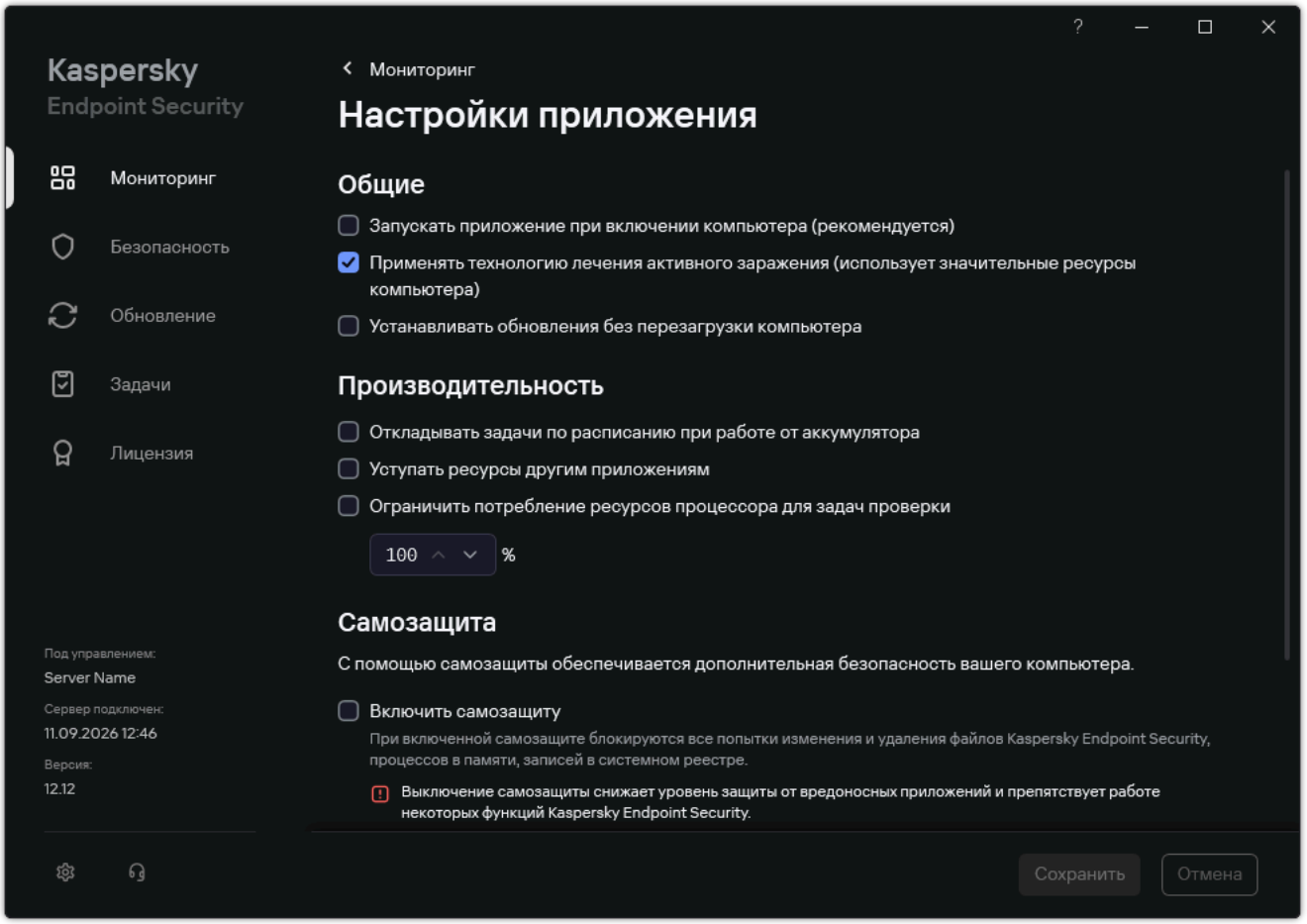
1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Производительность**.
5. В блоке **Ограничить потребление ресурсов процессора для задач проверки** установите переключатель **Ограничить потребление ресурсов процессора для задач проверки** и введите среднее значение потребления ресурсов процессора в процентах.
6. Сохраните внесенные изменения.

Как ограничить потребление ресурсов процессора при проверке компьютера в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.



Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Производительность** установите флажок **Ограничить потребление ресурсов процессора для задач проверки** и введите среднее значение потребления ресурсов процессора в процентах.

4. Сохраните внесенные изменения.

Настройка дополнительных параметров задачи Поиск вредоносного ПО

Вы можете оптимизировать проверку файлов: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы. Вы можете также ограничить длительность проверки одного файла. По истечении заданного времени Kaspersky Endpoint Security исключает файл из текущей проверки (кроме архивов и объектов, в состав которых входит несколько файлов).

Распространенной практикой сокрытия вирусов и других приложений, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие приложения, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить типы проверяемых составных файлов, таким образом увеличив скорость проверки.

Вы также можете включить использование технологий iChecker и iSwift. Технологии iChecker и iSwift позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

Как оптимизировать проверку в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.
3. Выберите задачу проверки и откройте свойства задачи двойным щелчком мыши.

   Если требуется, создайте задачу *Поиск вредоносного ПО*.
4. В окне свойств задачи выберите раздел **Настройки**.
5. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно настройки задачи проверки.
6. В блоке **Оптимизация** настройте параметры проверки:

   - **Проверять только новые и измененные файлы**. Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.

     Вы также можете настроить проверку новых файлов по типам. Например, вы можете запускать проверку всех дистрибутивов и проверку только новых архивов и файлов офисных форматов.

   - **Пропускать файлы, если их проверка длится более N сек**. Ограничение длительности проверки файла. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку текущего файла и начинает проверку следующего. Это ускоряет проверку компьютера, но снижает уровень защиты. По умолчанию Kaspersky Endpoint Security прекращает проверку файла по истечении 30 секунд.

   - **Не запускать несколько задач проверки одновременно**. Отложенный запуск задач проверки, запланированных по расписанию, если запущенная ранее проверка по расписанию еще выполняется. Kaspersky Endpoint Security ставит запланированные задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, вы запланировали запуск задач проверки в 18:00 и в 20:00. Kaspersky Endpoint Security отложит запуск задачи проверки в 20:00, если задача проверки, запущенная в 18:00, еще выполняется. Приложение запустит проверку после завершения задачи, запущенной в 18:00.
7. Нажмите на кнопку **Дополнительно**.

   Откроется окно настройки проверки составных файлов.
8. В блоке **Ограничение по размеру** установите флажок **Не распаковывать составные файлы большого размера**. Ограничение длительности проверки файла. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку текущего файла и начинает проверку следующего. Это ускоряет проверку компьютера, но снижает уровень защиты. По умолчанию Kaspersky Endpoint Security прекращает проверку файла по истечении 30 секунд.

   > Kaspersky Endpoint Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.
9. Нажмите на кнопку **OK**.

10. Перейдите на вкладку **Дополнительно**.

11. В блоке **Технологии проверки** установите флажки около названий технологий, которые вы хотите использовать во время проверки:

    - **Технология iSwift**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.

    - **Технология iChecker**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

12. Сохраните внесенные изменения.

Как оптимизировать проверку в Web Console

1. В главном окне Web Console выберите **Управление активами → Задачи**.

   Откроется список задач.

2. Нажмите на задачу проверки.

   Откроется окно свойств задачи. Если требуется, создайте задачу *Поиск вредоносного ПО*.

3. Выберите вкладку **Параметры приложения**.

4. В блоке **Действие при обнаружении угрозы** установите флажок **Проверять только новые и измененные файлы**. Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.

   Вы также можете настроить проверку новых файлов по типам. Например, вы можете запускать проверку всех дистрибутивов и проверку только новых архивов и файлов офисных форматов.

5. В блоке **Оптимизация проверки** установите флажок **Не распаковывать составные файлы большого размера**. Ограничение длительности проверки файла. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку текущего файла и начинает проверку следующего. Это ускоряет проверку компьютера, но снижает уровень защиты. По умолчанию Kaspersky Endpoint Security прекращает проверку файла по истечении 30 секунд.

   > Kaspersky Endpoint Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

6. Установить флажок **Не запускать несколько задач проверки одновременно**. Отложенный запуск задач проверки, запланированных по расписанию, если запущенная ранее проверка по расписанию еще выполняется. Kaspersky Endpoint Security ставит запланированные задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, вы запланировали запуск задач проверки в 18:00 и в 20:00. Kaspersky Endpoint Security отложит запуск задачи проверки в 20:00, если задача проверки, запущенная в 18:00, еще выполняется. Приложение запустит проверку после завершения задачи, запущенной в 18:00.

7. В блоке **Дополнительные настройки** установите флажок **Пропускать файл, если его проверка длится более (сек.)**. Ограничение длительности проверки файла. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку текущего файла и начинает проверку следующего. Это ускоряет проверку компьютера, но снижает уровень защиты. По умолчанию Kaspersky Endpoint Security прекращает проверку файла по истечении 30 секунд.

8. Сохраните внесенные изменения.

Как оптимизировать проверку в интерфейсе приложения

1. В главном окне приложения перейдите в раздел **Задачи**.

2. В открывшемся списке задач выберите задачу проверки и нажмите на кнопку ⚙.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Оптимизация** настройте параметры проверки:

   - **Проверять только новые и измененные файлы**. Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.

     Вы также можете настроить проверку новых файлов по типам. Например, вы можете запускать проверку всех дистрибутивов и проверку только новых архивов и файлов офисных форматов.

   - **Пропускать файл, если его проверка длится более N секунд**. Ограничение длительности проверки файла. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку текущего файла и начинает проверку следующего. Это ускоряет проверку компьютера, но снижает уровень защиты. По умолчанию Kaspersky Endpoint Security прекращает проверку файла по истечении 30 секунд.

   - **Не запускать несколько задач проверки одновременно**. Отложенный запуск задач проверки, запланированных по расписанию, если запущенная ранее проверка по расписанию еще выполняется. Kaspersky Endpoint Security ставит запланированные задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, вы запланировали запуск задач проверки в 18:00 и в 20:00. Kaspersky Endpoint Security отложит запуск задачи проверки в 20:00, если задача проверки, запущенная в 18:00, еще выполняется. Приложение запустит проверку после завершения задачи, запущенной в 18:00.

5. В блоке **Ограничение по размеру** установите флажок **Не распаковывать составные файлы большого размера**. Ограничение длительности проверки файла. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку текущего файла и начинает проверку следующего. Это ускоряет проверку компьютера, но снижает уровень защиты. По умолчанию Kaspersky Endpoint Security прекращает проверку файла по истечении 30 секунд.

   Kaspersky Endpoint Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

6. В блоке **Технологии проверки** установите флажки около названий технологий, которые вы хотите использовать во время проверки:

   - **Технология iSwift**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.

   - **Технология iChecker**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

7. Сохраните внесенные изменения.

Если задача проверки не отображается, администратор запретил использование локальных задач в политике.

Обновление баз и модулей приложения

Обновление баз и модулей приложения Kaspersky Endpoint Security обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие приложения, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули приложения.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) может быть недоступна в приложении на территории США.

Для регулярного обновления требуется действующая лицензия на использование приложения. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

Для успешной загрузки пакета обновлений с серверов обновлений "Лаборатории Касперского" компьютер должен быть подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, требуется настроить параметры прокси-сервера.

Загрузка обновлений осуществляется по протоколу HTTPS. Загрузка по протоколу HTTP может осуществляться в случае, когда загрузка обновлений по протоколу HTTPS невозможна.

В процессе обновления на ваш компьютер загружаются и устанавливаются следующие объекты:

- Базы Kaspersky Endpoint Security. Защита компьютера обеспечивается на основании баз данных, содержащих сигнатуры вирусов и других приложений, представляющих угрозу, и информацию о способах борьбы с ними. Компоненты защиты используют эту информацию при поиске и обезвреживании зараженных файлов на компьютере. Базы регулярно пополняются записями о появляющихся угрозах и способах борьбы с ними. Поэтому рекомендуется регулярно обновлять базы.

  Наряду с базами Kaspersky Endpoint Security обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.

- Модули приложения. Помимо баз Kaspersky Endpoint Security, можно обновлять и модули приложения. Обновления модулей приложения устраняют уязвимости Kaspersky Endpoint Security, добавляют новые функции или улучшают существующие.

В процессе обновления базы и модули приложения на вашем компьютере сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы и модули приложения отличаются от актуальной версии, на компьютер устанавливается недостающая часть обновлений.

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

Информация о текущем состоянии баз Kaspersky Endpoint Security отображается в главном окне приложения или в подсказке при наведении курсора на значок приложения в области уведомлений.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении задачи обновления, записывается в отчет Kaspersky Endpoint Security.

Если приложение работает в режиме Легкого агента, обновление баз и модулей приложения имеет особенности.

Схемы обновления баз и модулей приложения

Обновление баз и модулей приложения Kaspersky Endpoint Security обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие приложения, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули приложения.

На компьютерах пользователей обновляются следующие объекты:

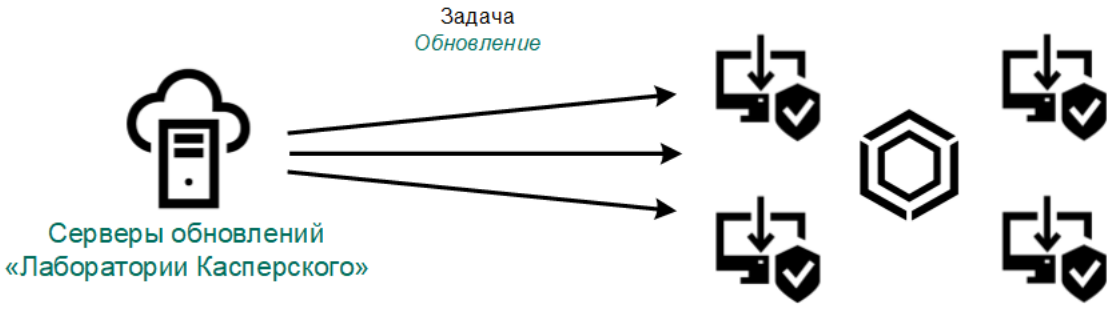
- Антивирусные базы. Антивирусные базы включают в себя базы сигнатур вредоносных приложений, описание сетевых атак, базы вредоносных и фишинговых веб-адресов, базы баннеров, спам-базы и другие данные.

- Модули приложения. Обновление модулей предназначено для устранения уязвимостей в приложении и улучшения методов защиты компьютера. Обновления модулей могут менять поведение компонентов приложения и добавлять новые возможности.

Kaspersky Endpoint Security поддерживает следующие схемы обновления баз и модулей приложения:

- Обновление с серверов "Лаборатории Касперского".

  Серверы обновлений "Лаборатории Касперского" расположены в разных странах по всему миру. Это обеспечивает высокую надежность обновления. Если обновление не может быть выполнено с одного сервера, Kaspersky Endpoint Security переключается к следующему серверу.



Обновление с серверов "Лаборатории Касперского"

- Централизованное обновление.

  Централизованное обновление обеспечивает снижение внешнего интернет-трафика, а также удобство контроля за обновлением.

  Централизованное обновление состоит из следующих этапов:

  1. Загрузка пакета обновлений в хранилище внутри сети организации.

     Загрузку пакета обновлений в хранилище обеспечивает задача Сервера администрирования *Загрузка обновлений в хранилище Сервера администрирования*.

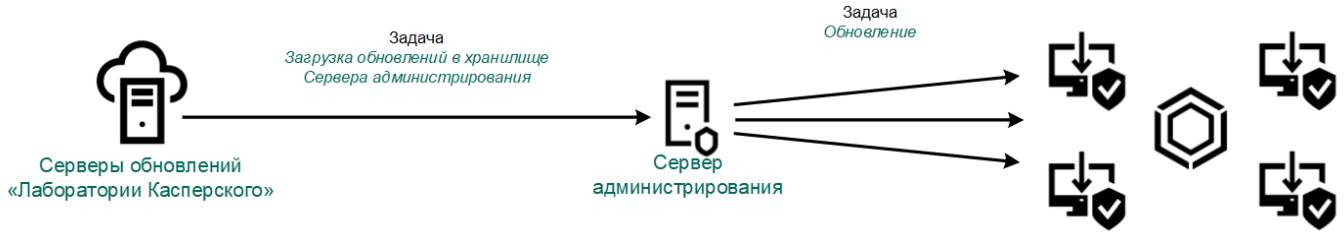
  2. Загрузка пакета обновлений в папку общего доступа (необязательно).

Загрузку пакета обновлений в папку общего доступа можно обеспечить следующими способами:

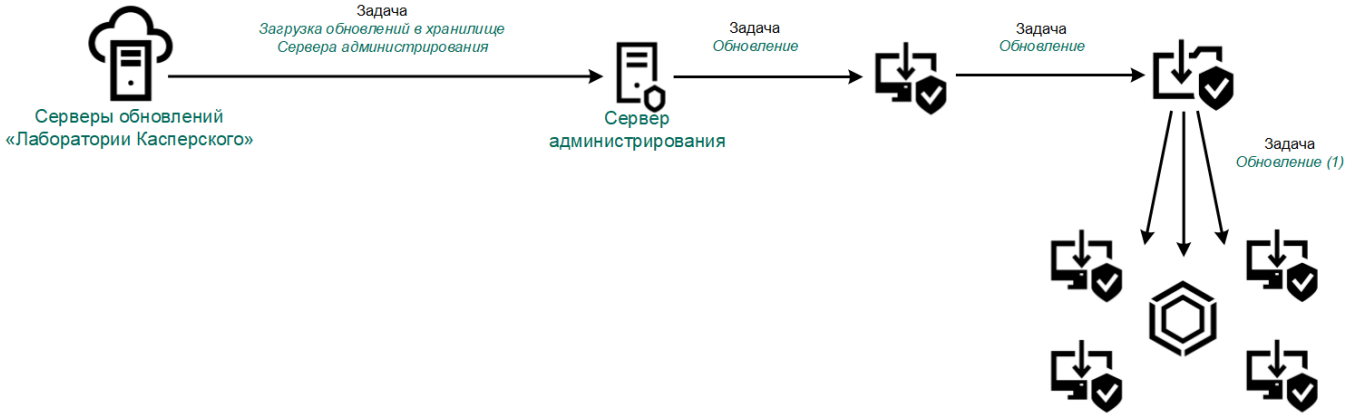
- С помощью задачи Kaspersky Endpoint Security *Обновление баз и модулей приложения*. Задача предназначена для одного из компьютеров локальной сети организации.
- С помощью Kaspersky Update Utility. Подробную информацию о работе с Kaspersky Update Utility см. в Базе знаний "Лаборатории Касперского".

3. Распространение пакета обновлений на клиентские компьютеры.

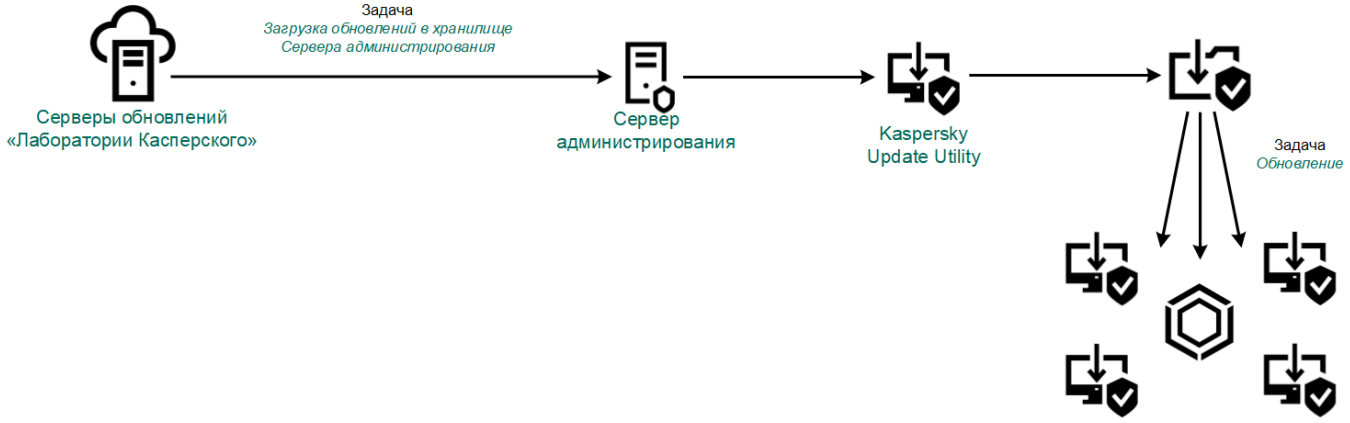
   Распространение пакета обновлений на клиентские компьютеры обеспечивает задача Kaspersky Endpoint Security *Обновление баз и модулей приложения*. Вы можете создать неограниченное количество задач обновления для каждой из групп администрирования.



Обновление с серверного хранилища



Обновление из папки общего доступа



Обновление с помощью Kaspersky Update Utility

Для Kaspersky Security Center по умолчанию список источников обновлений содержит Сервер администрирования Kaspersky Security Center и серверы обновлений "Лаборатории Касперского". Для Kaspersky Security Center Cloud Console по умолчанию список источников обновлений содержит точки распространения и серверы обновлений "Лаборатории Касперского". Подробнее о точках распространения см. в справке Kaspersky Security Center Cloud Console. Вы можете добавлять в список другие источники обновлений. В качестве источников обновлений можно указывать HTTP- или FTP-серверы, папки общего доступа. Если обновление не может быть выполнено с одного источника обновлений, Kaspersky Endpoint Security переключается к следующему.

Загрузка обновлений с серверов обновлений "Лаборатории Касперского" или с других FTP- или HTTP-серверов осуществляется по стандартным сетевым протоколам. Если для доступа к источнику обновлений требуется подключение к прокси-серверу, введите параметры прокси-сервера в свойствах политики Kaspersky Endpoint Security.

Обновление с серверного хранилища

Для экономии интернет-трафика вы можете настроить обновление баз и модулей приложения на компьютерах локальной сети организации с серверного хранилища. Для этого Kaspersky Security Center должен загружать пакет обновлений в хранилище (FTP-, HTTP-сервер, сетевая или локальная папка) с серверов обновлений "Лаборатории Касперского". В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений с серверного хранилища.

Настройка обновления баз и модулей приложения с серверного хранилища состоит из следующих этапов:

1. Настройка перемещения пакета обновлений в хранилище на Сервере администрирования (задача *Загрузка обновлений в хранилище Сервера администрирования*).

   Задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически мастером первоначальной настройки Сервера администрирования и может существовать только в единственном экземпляре. По умолчанию Kaspersky Security Center копирует пакет обновлений в папку `\\<server name>\KLSHARE\Updates`. Подробнее о загрузке обновлений в хранилище Сервера администрирования см. в справке Kaspersky Security Center.

2. Настройка обновления баз и модулей приложения из указанного серверного хранилища на остальных компьютерах локальной сети организации (задача *Обновление баз и модулей приложения*).

   Как настроить обновление Kaspersky Endpoint Security из указанного серверного хранилища в Консоли администрирования (MMC)

   1. Откройте Консоль администрирования Kaspersky Security Center.

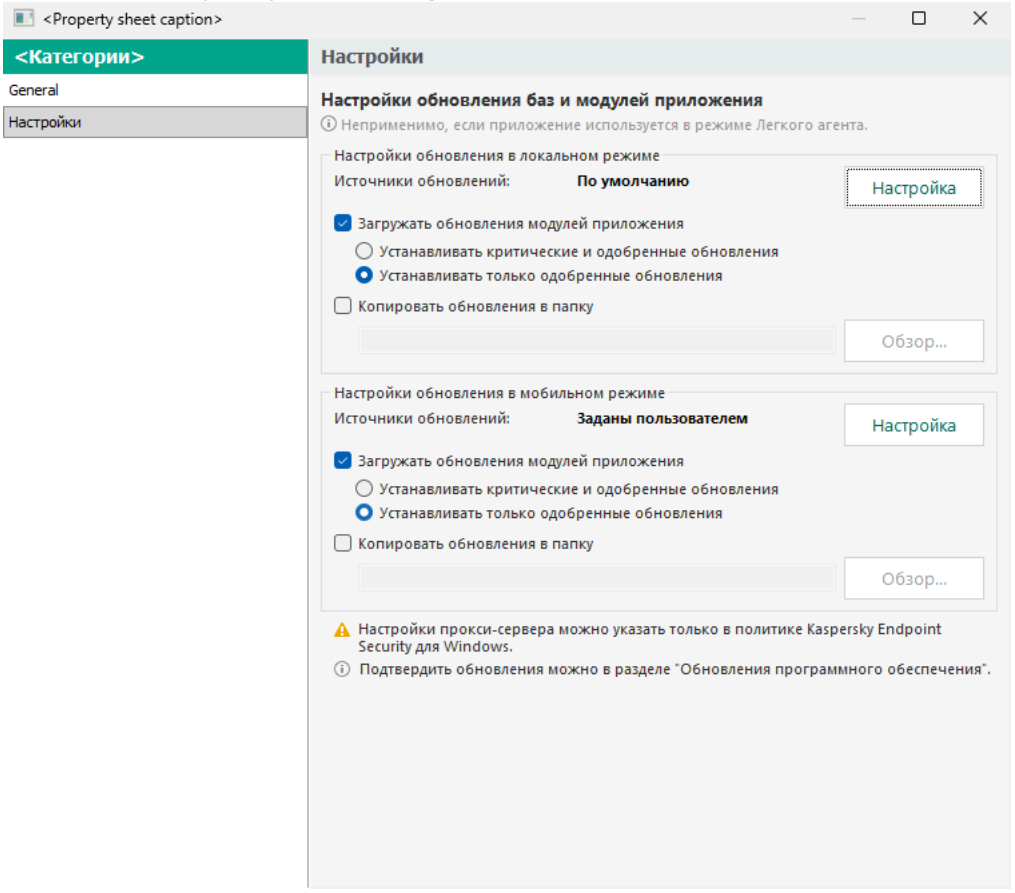
      В дереве консоли выберите папку **Задачи**.

   2. Нажмите на задачу Kaspersky Endpoint Security **Обновление баз и модулей приложения**.

      Откроется окно свойств задачи.

      Задача *Обновление баз и модулей приложения* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление баз и модулей приложения* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.

3. В окне свойств задачи выберите раздел **Настройки**.



Параметры задачи Обновление баз и модулей приложения

4. В блоке **Настройки обновления в локальном режиме** нажмите на кнопку **Настройка**.

5. В списке источников обновлений убедитесь, что обновление из источника **Kaspersky Security Center** включено. Также у источника **Kaspersky Security Center** должен быть наивысший приоритет.

6. Если требуется, добавьте источники обновлений:

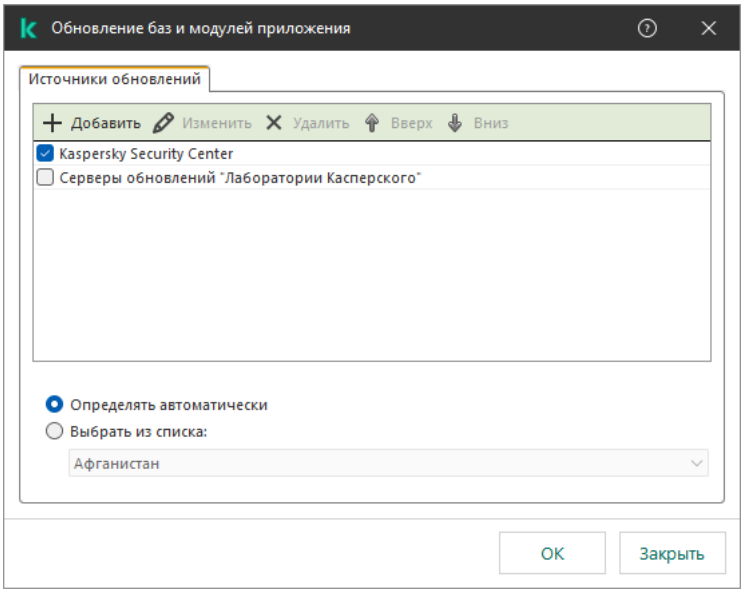
   a. В списке источников обновлений нажмите на кнопку **Добавить**.

   b. В поле **Источники обновлений** укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, в которую Kaspersky Security Center копирует пакет обновлений, полученный с серверов обновлений "Лаборатории Касперского".

   > Адрес источника должен совпадать с адресом, указанным в поле **Папка для хранения обновлений** при настройке загрузки обновлений в серверное хранилище (задача *Загрузка обновлений в хранилище Сервера администрирования*).

   c. Нажмите на кнопку **OK**.

Вы можете исключить источник обновлений, не удаляя его из списка источников. Для этого снимите флажок рядом с ним.



Источники обновлений

7. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

   Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

8. В окне свойств задачи выберите раздел **Расписание** и настройте режим запуска задачи.

9. По умолчанию Kaspersky Endpoint Security запускает задачу в ручном режиме.

10. Сохраните внесенные изменения.

Как настроить обновление Kaspersky Endpoint Security из указанного серверного хранилища в Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление**.

   Откроется окно свойств задачи.

   Задача *Обновление* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.

3. Выберите вкладку **Параметры приложения** → **Локальный режим**.

4. В списке источников обновлений убедитесь, что обновление из источника **Kaspersky Security Center** включено. Также у источника **Kaspersky Security Center** должен быть наивысший приоритет.

5. Если требуется, добавьте источники обновлений:

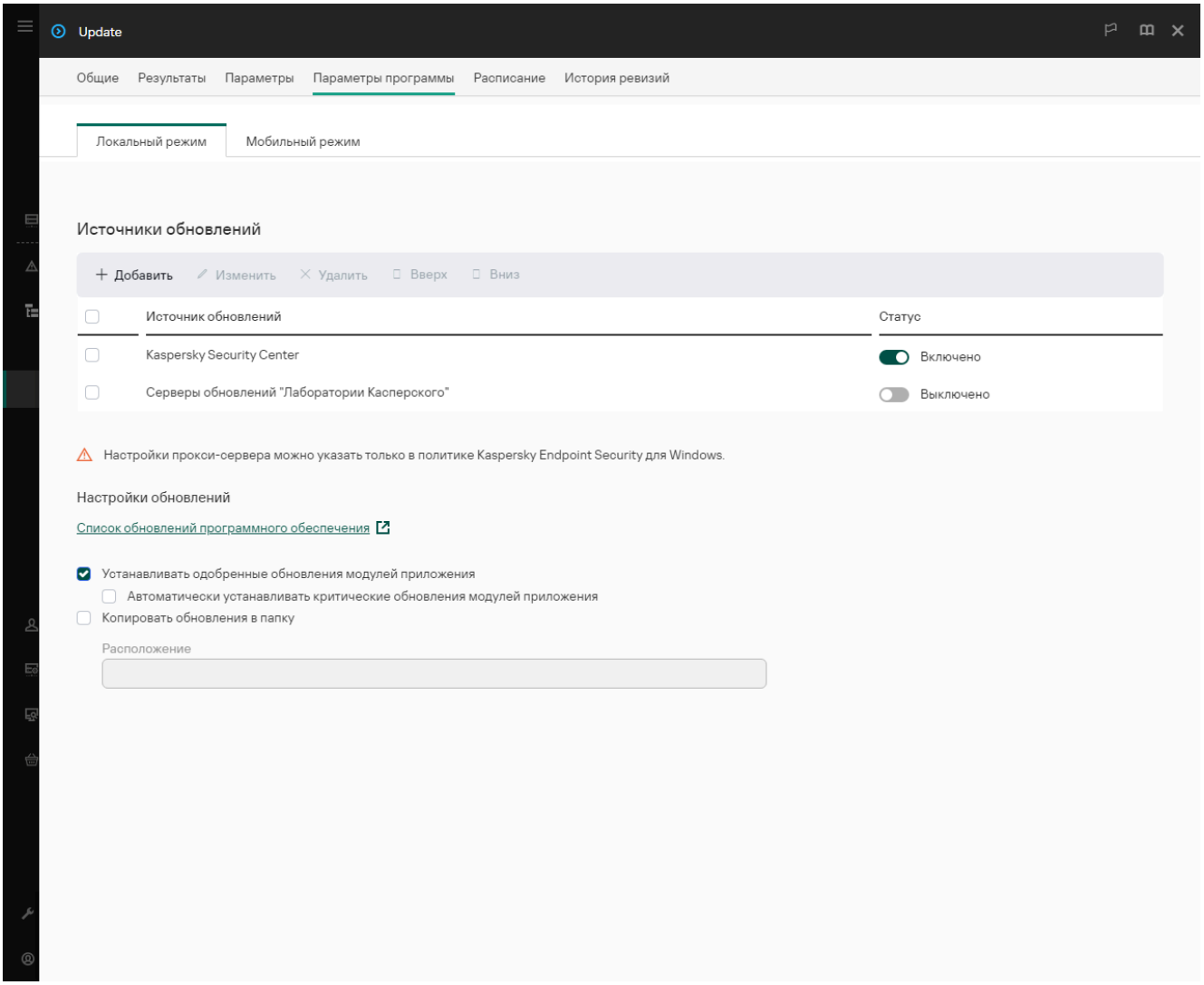
   a. В списке источников обновлений нажмите на кнопку **Добавить**.

   b. В поле **Источники обновлений** укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, в которую Kaspersky Security Center копирует пакет обновлений, полученный с серверов обновлений "Лаборатории Касперского".

      Адрес источника должен совпадать с адресом, указанным в поле **Папка для хранения обновлений** при настройке загрузки обновлений в серверное хранилище (задача *Загрузка обновлений в хранилище Сервера администрирования*).

   c. Нажмите на кнопку **Сохранить**.

Вы можете исключить источник обновлений, не удаляя его из списка источников. Для этого выключите переключатель рядом с ним.



Источники обновлений

6. Настройте приоритеты источников обновлений с помощью кнопок **Переместить вверх** и **Переместить вниз**.

   Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

7. В окне свойств задачи выберите раздел **Расписание** и настройте режим запуска задачи.

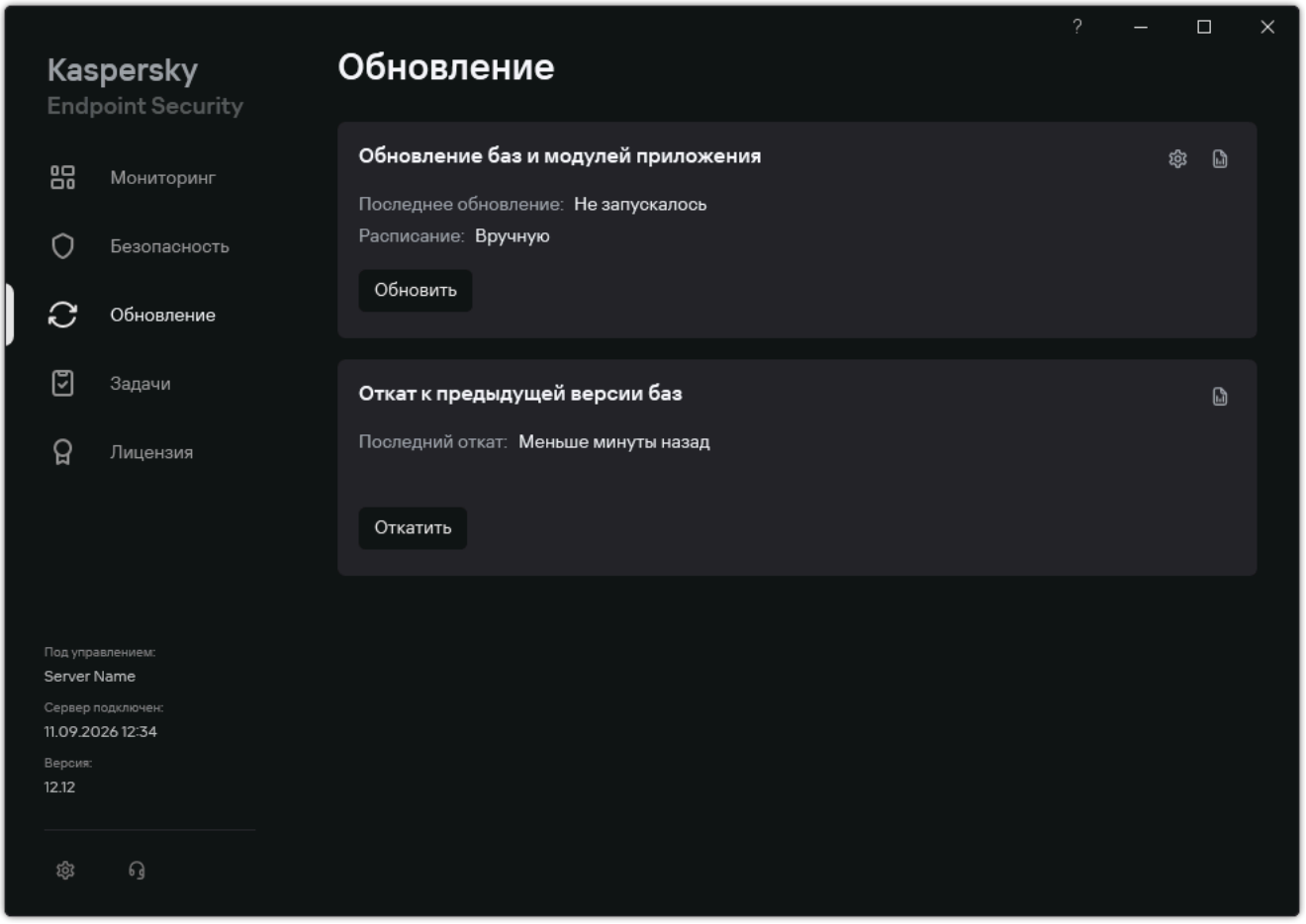
8. По умолчанию Kaspersky Endpoint Security запускает задачу в ручном режиме.

9. Сохраните внесенные изменения.

Как настроить обновление Kaspersky Endpoint Security из указанного серверного хранилища в интерфейсе приложения

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике.

1. В главном окне приложения перейдите в раздел **Обновление**.



Локальные задачи обновления

2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку ⚙.

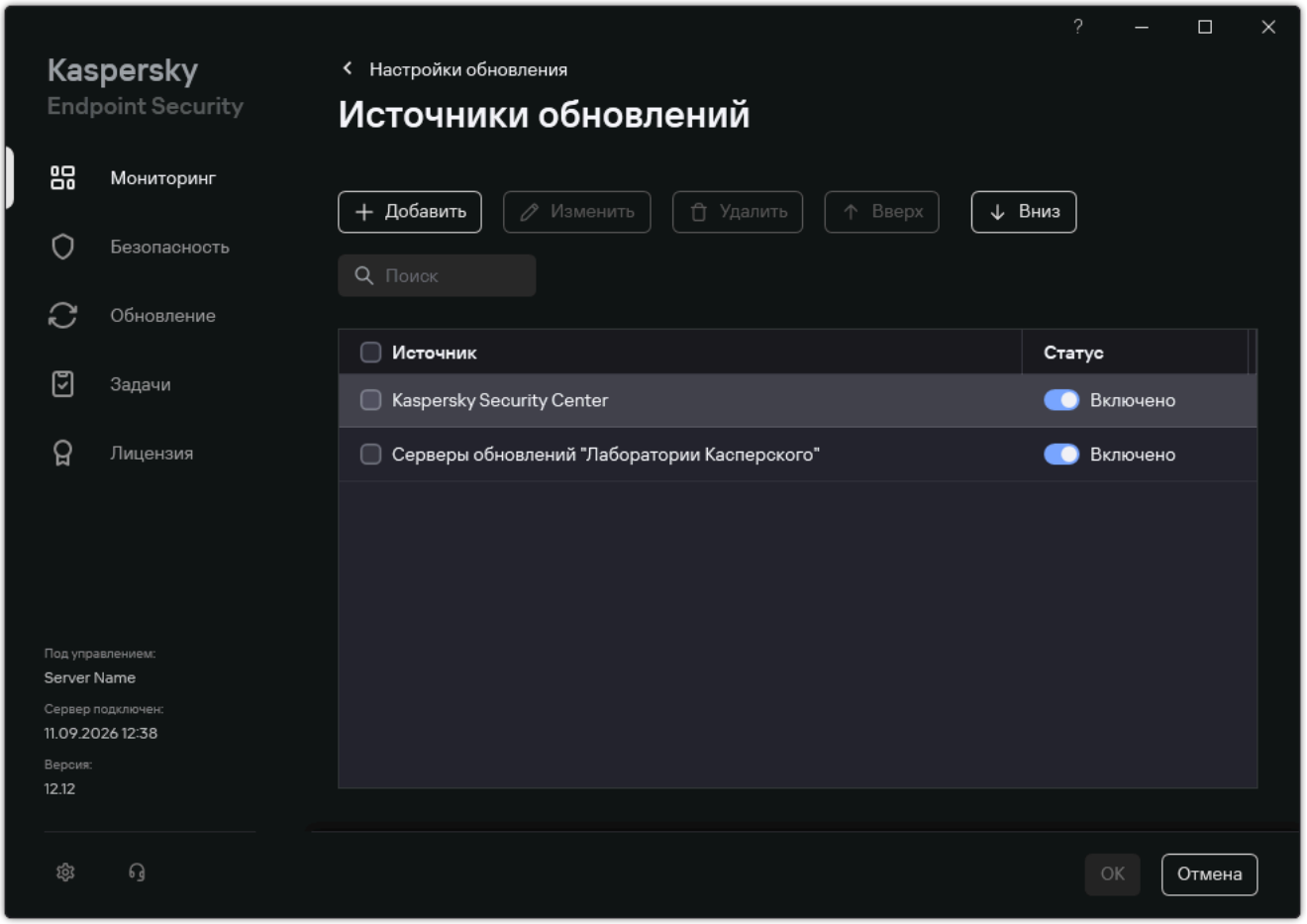
   Откроется окно свойств задачи.

3. В окне свойств задачи нажмите **Настроить источники обновлений**.

4. В списке источников обновлений убедитесь, что обновление из источника **Kaspersky Security Center** включено. Также у источника **Kaspersky Security Center** должен быть наивысший приоритет.

5. Если требуется, добавьте источники обновлений:

   a. В списке источников обновлений нажмите на кнопку **Добавить**.



Источники обновлений

   a. Укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, в которую Kaspersky Security Center копирует пакет обновлений, полученный с серверов обновлений "Лаборатории Касперского".

      Адрес источника должен совпадать с адресом, указанным в поле **Папка для хранения обновлений** при настройке загрузки обновлений в серверное хранилище (задача *Загрузка обновлений в хранилище Сервера администрирования*).

   b. Нажмите на кнопку **Выбрать**.

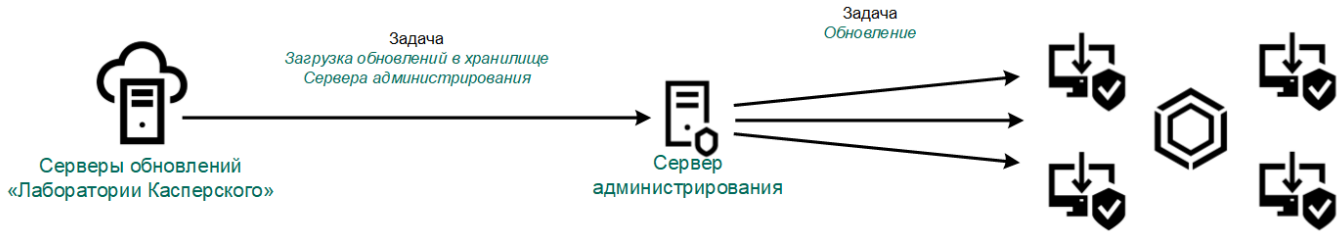
   Вы можете исключить источник обновлений, не удаляя его из списка источников. Для этого выключите переключатель рядом с ним.

6. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

   Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

Если компьютер находится под управлением Kaspersky Security Center, настроить режим запуска задачи *Обновление баз и модулей приложения* невозможно. Вы можете запустить задачу только вручную.

7. Сохраните внесенные изменения.



Обновление с серверного хранилища

Обновление из папки общего доступа

Для экономии интернет-трафика вы можете настроить обновление баз и модулей приложения на компьютерах локальной сети организации из папки общего доступа. Для этого один из компьютеров локальной сети организации должен получать пакеты обновлений с Сервера администрирования Kaspersky Security Center или серверов обновлений "Лаборатории Касперского" и копировать полученный пакет обновлений в папку общего доступа. В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений из папки общего доступа.

Версия и локализация приложения Kaspersky Endpoint Security, которое копирует пакет обновлений в папку общего доступа, и приложения, которое обновляет базы из папки общего доступа, должны совпадать. Если версия или локализация приложений не совпадает, обновление баз может завершиться с ошибкой.

Настройка обновления баз и модулей приложения из папки общего доступа состоит из следующих этапов:

1. Настройка обновления баз и модулей приложения с серверного хранилища.

2. Включение режима копирования пакета обновлений в папку общего доступа на одном из компьютеров локальной сети организации.

   Как включить режим копирования пакета обновлений в папку общего доступа в Консоли администрирования (MMC)

   1. Откройте Консоль администрирования Kaspersky Security Center.

   2. В дереве консоли выберите папку **Задачи**.

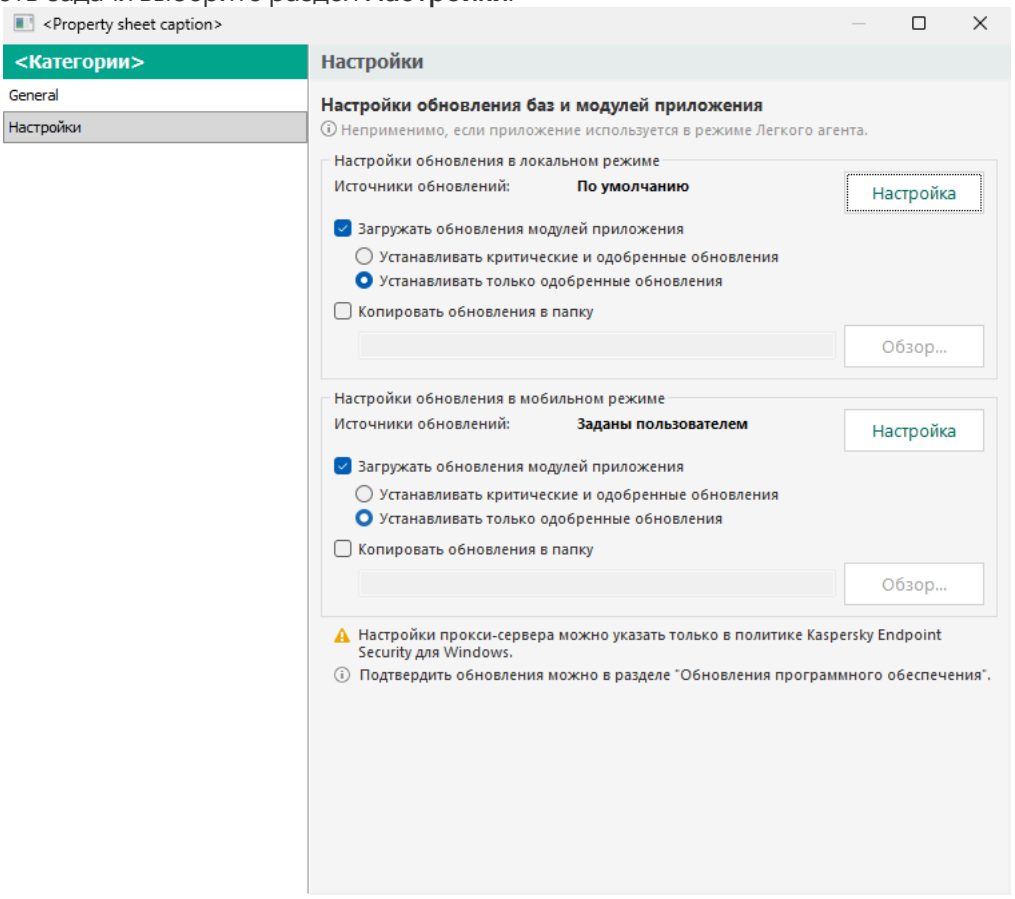
      Задача *Обновление баз и модулей приложения* должна быть назначена для одного компьютера, который будет считаться источником обновлений.

   3. Нажмите на задачу Kaspersky Endpoint Security **Обновление баз и модулей приложения**.

      Откроется окно свойств задачи.

Задача *Обновление баз и модулей приложения* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление баз и модулей приложения* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.

4. В окне свойств задачи выберите раздел **Настройки**.



Параметры задачи Обновление баз и модулей приложения

5. В блоке **Настройки обновления в локальном режиме** нажмите на кнопку **Настройка**.

6. Настройте источники обновлений.

   В качестве источников обновлений могут быть использованы серверы обновлений "Лаборатории Касперского", Сервер администрирования Kaspersky Security Center или другие FTP- или HTTP-серверы, локальные или сетевые папки.

7. Установите флажок **Копировать обновления в папку**.

8. В поле **Путь к папке** введите UNC-путь к папке общего доступа (например, `\\<server name>\KLSHARE\Updates`).

   Если оставить поле пустым, Kaspersky Endpoint Security будет копировать пакет обновлений в папку `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

9. Сохраните внесенные изменения.

Как включить режим копирования пакета обновлений в папку общего доступа в Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

Задача *Обновление* должна быть назначена для одного компьютера, который будет считаться источником обновлений.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление**.

   Откроется окно свойств задачи.

   Задача *Обновление* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.

3. Выберите вкладку **Параметры приложения** → **Локальный режим**.

4. Настройте источники обновлений.

   В качестве источников обновлений могут быть использованы серверы обновлений "Лаборатории Касперского", Сервер администрирования Kaspersky Security Center или другие FTP- или HTTP-серверы, локальные или сетевые папки.

5. Установите флажок **Копировать обновления в папку**.

6. В поле **Расположение** введите UNC-путь к папке общего доступа (например, `\\<server name>\KLSHARE\Updates`).

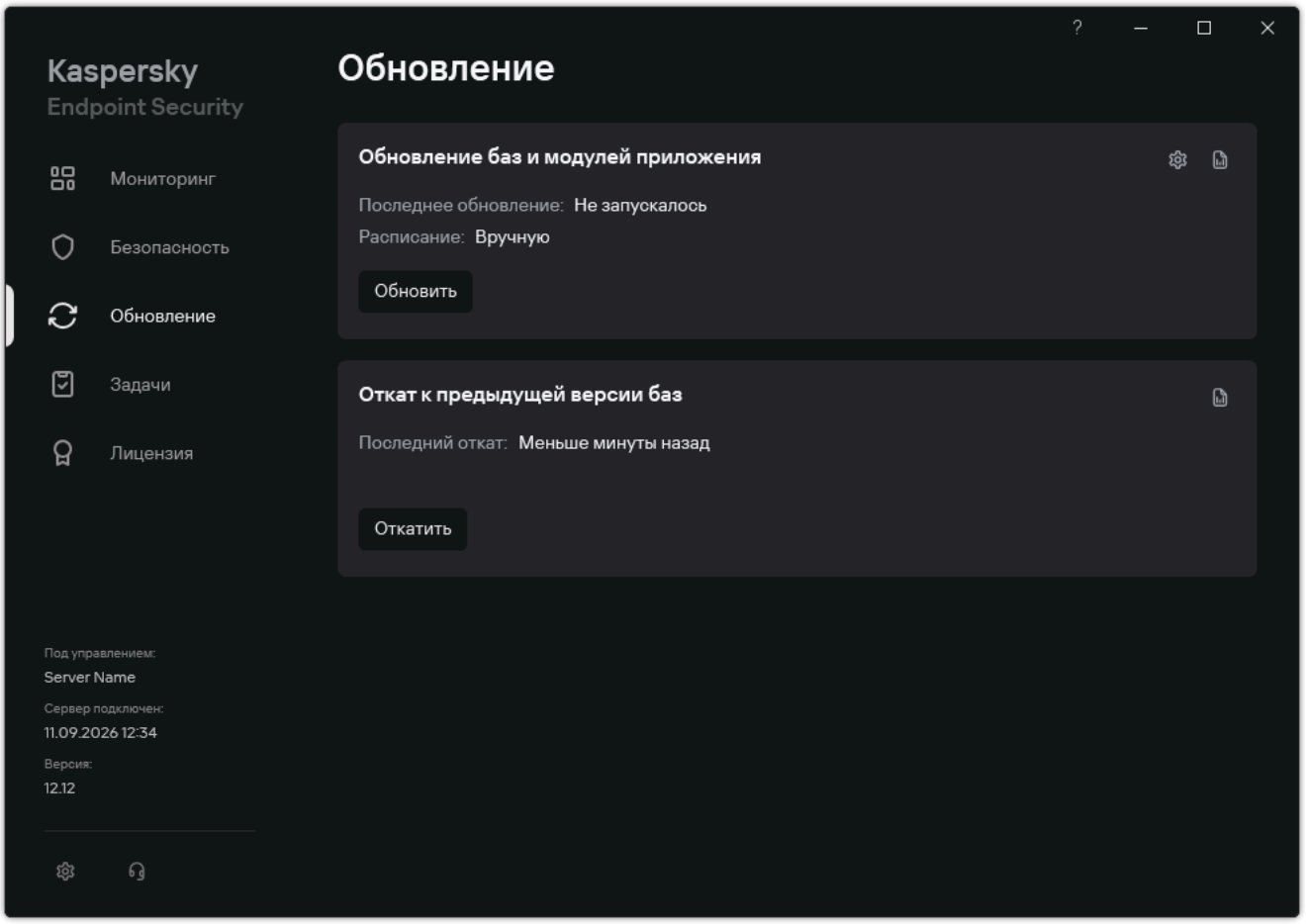
   Если оставить поле пустым, Kaspersky Endpoint Security будет копировать пакет обновлений в папку `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. Сохраните внесенные изменения.

Как включить режим копирования пакета обновлений в папку общего доступа в интерфейсе приложения

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике.

1. В главном окне приложения перейдите в раздел **Обновление**.



Локальные задачи обновления

2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку ⚙.

   Откроется окно свойств задачи.

3. В блоке **Копирование обновлений** установите флажок **Копировать обновления в папку**.

4. Введите UNC-путь к папке общего доступа (например, `\\<server name>\KLSHARE\Updates`).

5. Сохраните внесенные изменения.

3. Настройка обновления баз и модулей приложения из указанной папки общего доступа на остальных компьютерах локальной сети организации.

Как настроить обновление из папки общего доступа в Консоли администрирования (MMC)

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Обновление баз и модулей приложения**.

4. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

5. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Обновление баз и модулей приложения**.

Шаг 2. Выбор источников обновлений

Добавьте новый источник обновлений – папку общего доступа. Адрес источника должен совпадать с адресом, указанным ранее в поле **Путь к папке** при настройке режима копирования пакета обновлений в папку общего доступа. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Задача *Обновление баз и модулей приложения* должна быть назначена остальным компьютерам локальной сети организации кроме компьютера, который считается источником обновлений.

Шаг 4. Выбор учетной записи для запуска задачи

Выберите учетную запись для запуска задачи *Обновление баз и модулей приложения*. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.

Шаг 5. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или после загрузки антивирусных баз в хранилище.

Шаг 6. Определение названия задачи

Введите название задачи, например, *Обновление из папки общего доступа*.

Шаг 7. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи. В результате на компьютерах пользователей будет выполняться обновление в соответствии с установленным расписанием.

Как настроить обновление из папки общего доступа в Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Обновление**.

   c. В поле **Название задачи** введите короткое описание, например, *Обновление из папки общего доступа*.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

   > Задача *Обновление* должна быть назначена остальным компьютерам локальной сети организации кроме компьютера, который считается источником обновлений.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи и перейдите к следующему шагу.

5. Завершите работу мастера.

   В таблице задач отобразится новая задача.

6. Нажмите на созданную задачу *Обновление*.

   Откроется окно свойств задачи.

7. Выберите вкладку **Параметры приложения** → **Локальный режим**.

8. В блоке **Источники обновлений** нажмите на кнопку **Добавить**.

9. В открывшемся окне введите путь к папке общего доступа.

   > Адрес источника должен совпадать с адресом, указанным ранее в поле **Расположение** при настройке режима копирования пакета обновлений в папку общего доступа (см. инструкцию выше).

10. Нажмите на кнопку **ОК**.

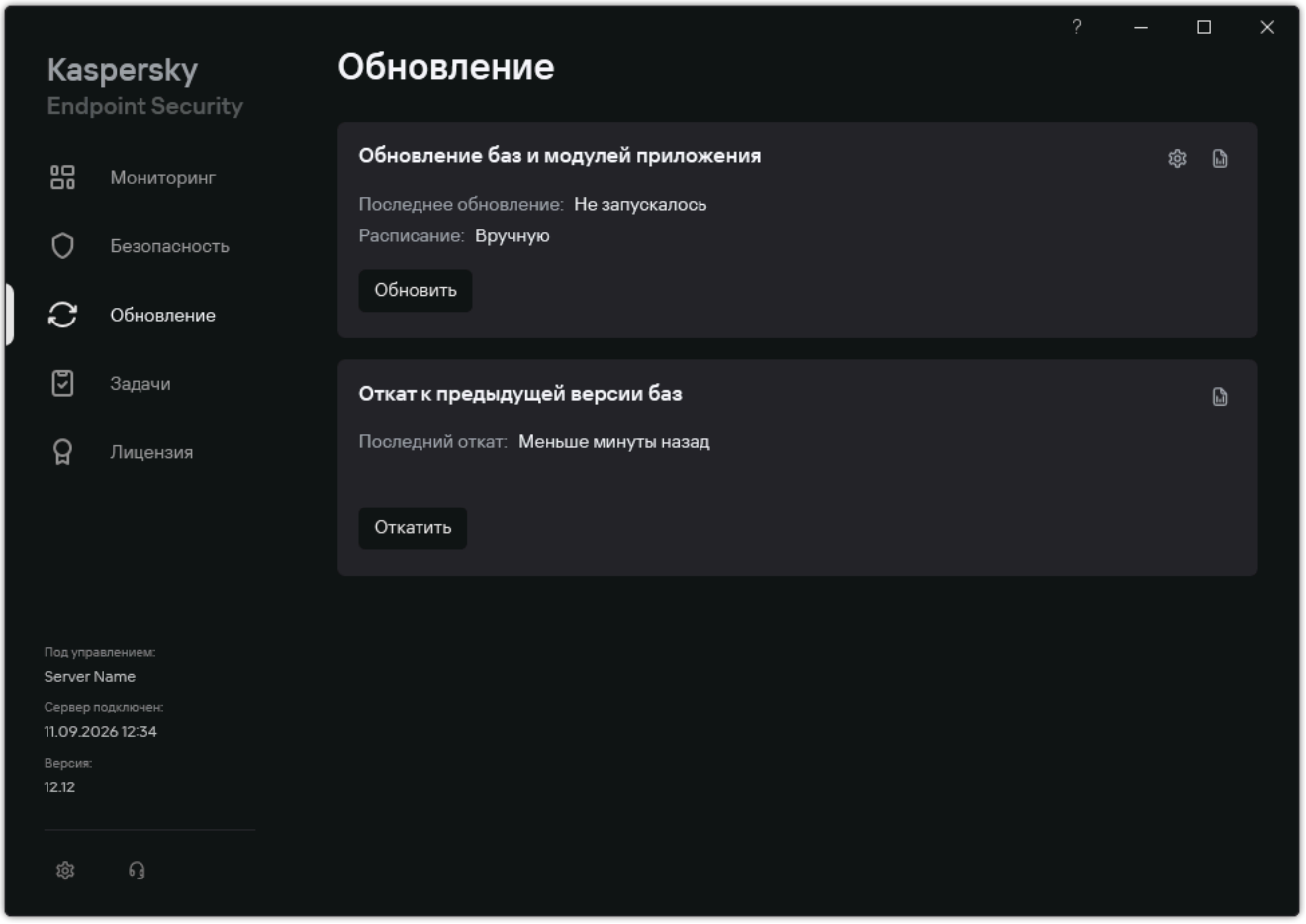
11. Настройте приоритеты источников обновлений с помощью кнопок **Переместить вверх** и **Переместить вниз**.

12. Сохраните внесенные изменения.

Как настроить обновление из папки общего доступа в интерфейсе приложения

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике.

1. В главном окне приложения перейдите в раздел **Обновление**.



Локальные задачи обновления

2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку ⚙.

   Откроется окно свойств задачи.

3. Нажмите на кнопку **Настроить источники обновлений**.

4. В открывшемся окне нажмите на кнопку **Добавить**.

5. В открывшемся окне укажите путь к папке общего доступа.

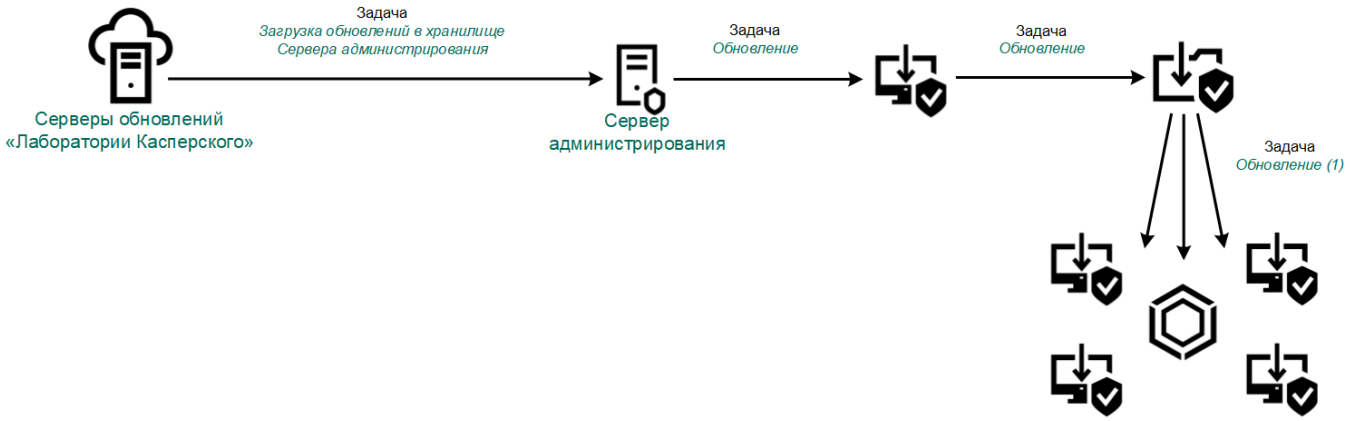
   Адрес источника должен совпадать с адресом, указанным ранее при настройке режима копирования пакета обновлений в папку общего доступа (см. инструкцию выше).

6. Нажмите на кнопку **Выбрать**.

7. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

   Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

8. Сохраните внесенные изменения.



Обновление из папки общего доступа

Обновление с помощью Kaspersky Update Utility

Для экономии интернет-трафика вы можете настроить обновление баз и модулей приложения на компьютерах локальной сети организации из папки общего доступа с помощью утилиты Kaspersky Update Utility. Для этого один из компьютеров локальной сети организации должен получать пакеты обновлений с Сервера администрирования Kaspersky Security Center или серверов обновлений "Лаборатории Касперского" и копировать полученные пакеты обновлений в папку общего доступа с помощью утилиты. В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений из папки общего доступа.

Версия и локализация приложения Kaspersky Endpoint Security, которое копирует пакет обновлений в папку общего доступа, и приложения, которое обновляет базы из папки общего доступа, должны совпадать. Если версия или локализация приложений не совпадает, обновление баз может завершиться с ошибкой.

Настройка обновления баз и модулей приложения из папки общего доступа состоит из следующих этапов:

1. Настройка обновления баз и модулей приложения с серверного хранилища.

2. Установка Kaspersky Update Utility на одном из компьютеров локальной сети организации.

3. Настройка копирования пакета обновлений в папку общего доступа в параметрах Kaspersky Update Utility.

   Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта Службы технической поддержки "Лаборатории Касперского". После установки утилиты выберите источник обновлений (например, хранилище Сервера администрирования) и папку общего доступа, в которую Kaspersky Update Utility будет копировать пакеты обновлений. Подробную информацию о работе с Kaspersky Update Utility см. в Базе знаний "Лаборатории Касперского".

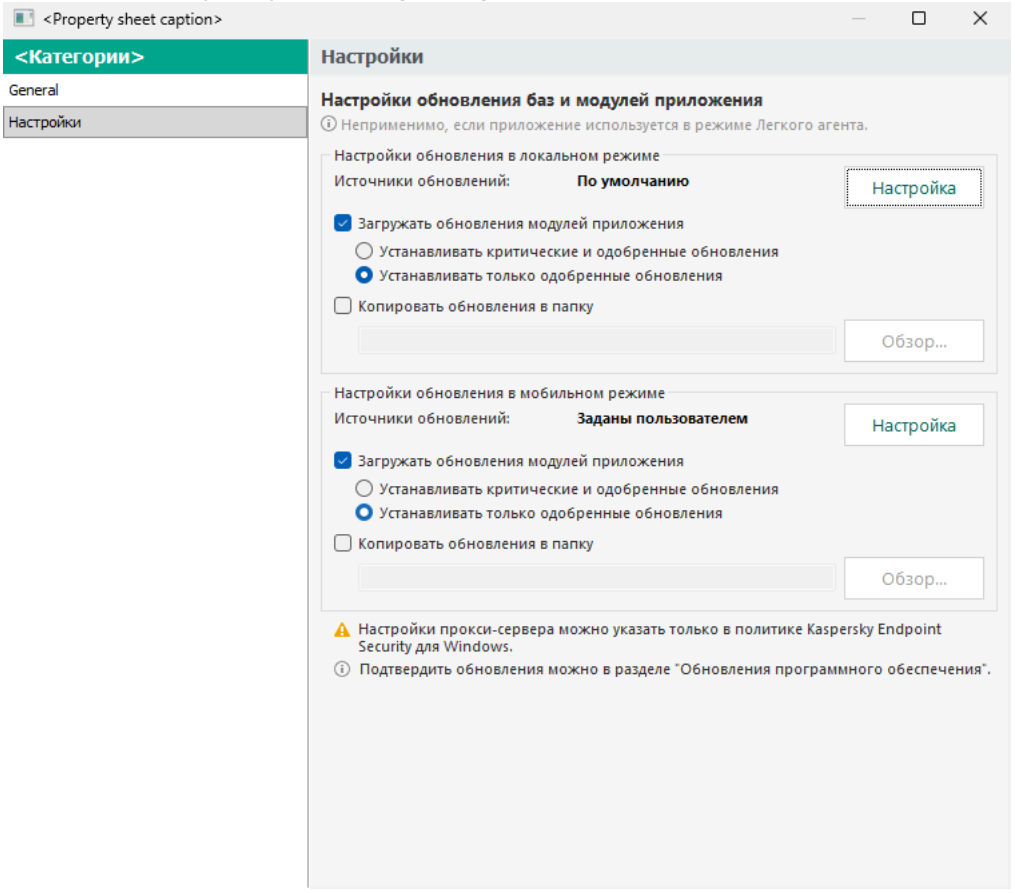
4. Настройка обновления баз и модулей приложения из указанной папки общего доступа на остальных компьютерах локальной сети организации.

Как настроить обновление из папки общего доступа в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.
3. Нажмите на задачу Kaspersky Endpoint Security **Обновление баз и модулей приложения**.

   Откроется окно свойств задачи.

   Задача *Обновление баз и модулей приложения* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление баз и модулей приложения* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.
4. В окне свойств задачи выберите раздел **Параметры**.



Параметры задачи Обновление баз и модулей приложения

5. В блоке **Настройки обновления в локальном режиме** нажмите на кнопку **Настройка**.
6. В списке источников обновлений нажмите на кнопку **Добавить**.
7. В открывшемся окне введите UNC-путь к папке общего доступа (например, `\\<server name>\KLSHARE\Updates`).

   Адрес источника должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.
8. Нажмите на кнопку **OK**.

9. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

   Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

10. Сохраните внесенные изменения.

Как настроить обновление из папки общего доступа в Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление**.

   Откроется окно свойств задачи.

   Задача *Обновление* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.

3. Выберите вкладку **Параметры приложения** → **Локальный режим**.

4. В списке источников обновлений нажмите на кнопку **Добавить**.

5. В открывшемся окне введите UNC-путь к папке общего доступа (например, `\\<server name>\KLSHARE\Updates`).

   > Адрес источника должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.

6. Нажмите на кнопку **OK**.

7. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

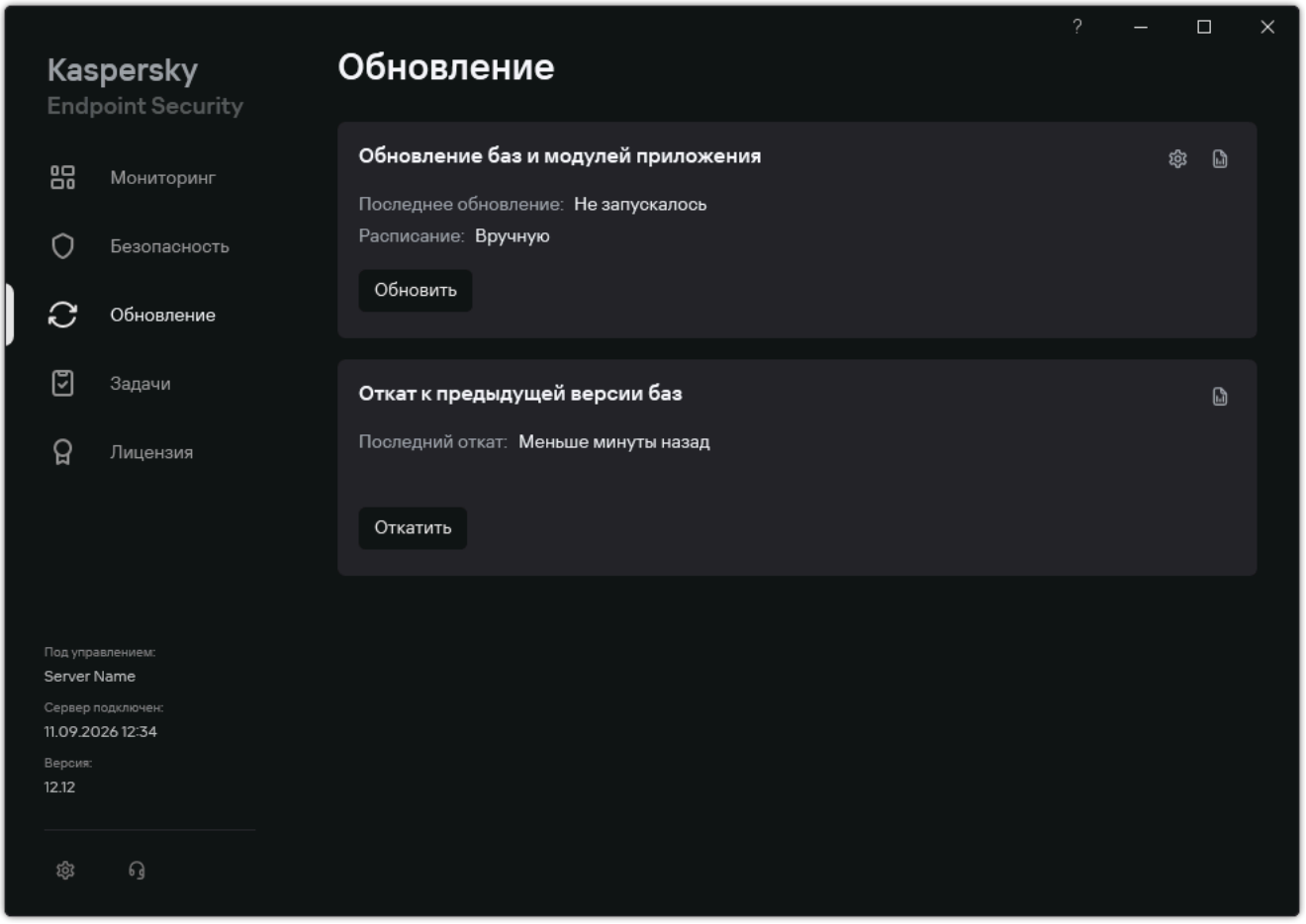
   Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

8. Сохраните внесенные изменения.

Как настроить обновление из папки общего доступа в интерфейсе приложения

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике.

1. В главном окне приложения перейдите в раздел **Обновление**.



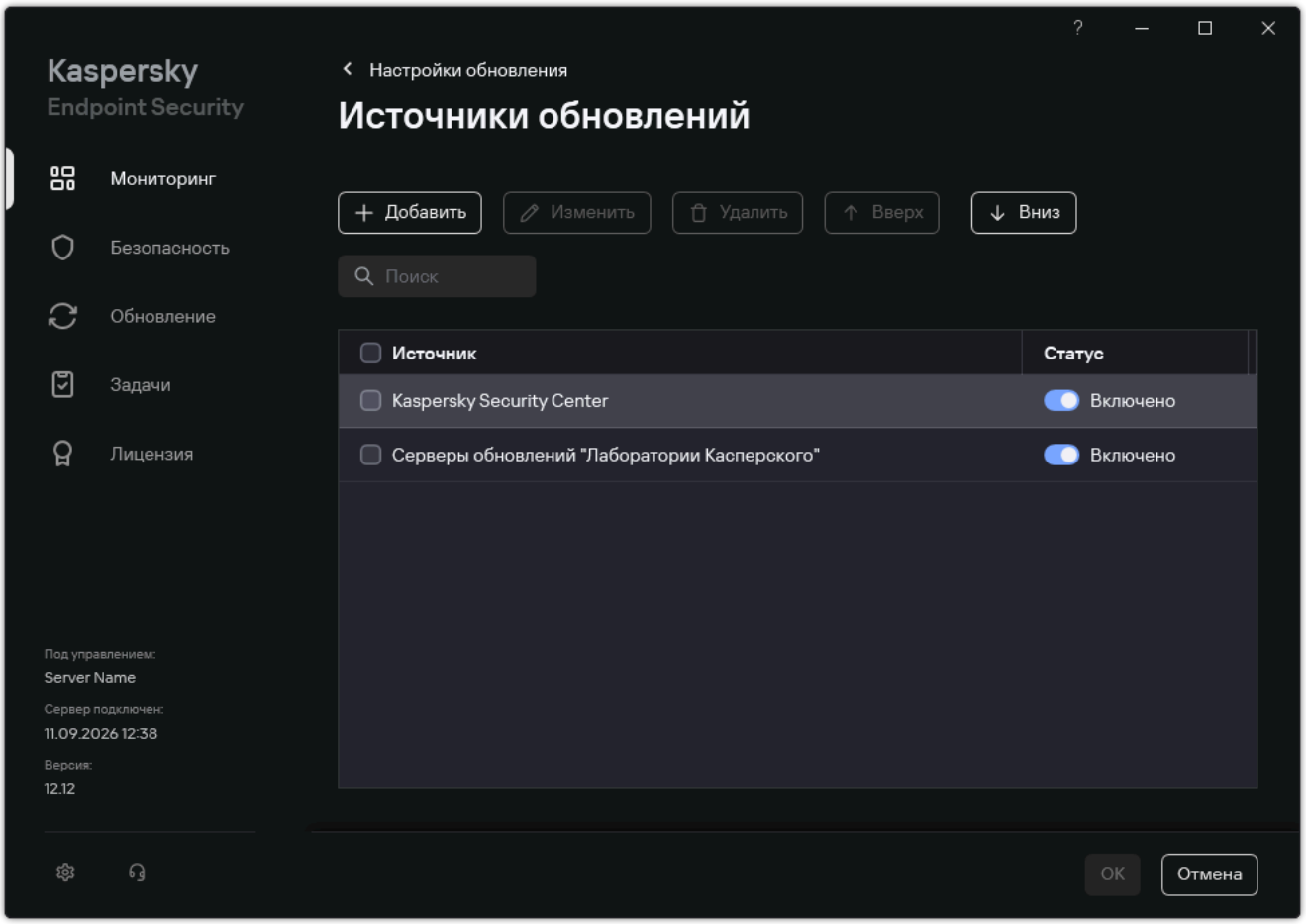
Локальные задачи обновления

2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку ⚙.

   Откроется окно свойств задачи.

3. В окне свойств задачи нажмите **Настроить источники обновлений**.

4. В списке источников обновлений нажмите на кнопку **Добавить**.



Источники обновлений

5. Введите UNC-путь к папке общего доступа (например, `\\<server name>\KLSHARE\Updates`).

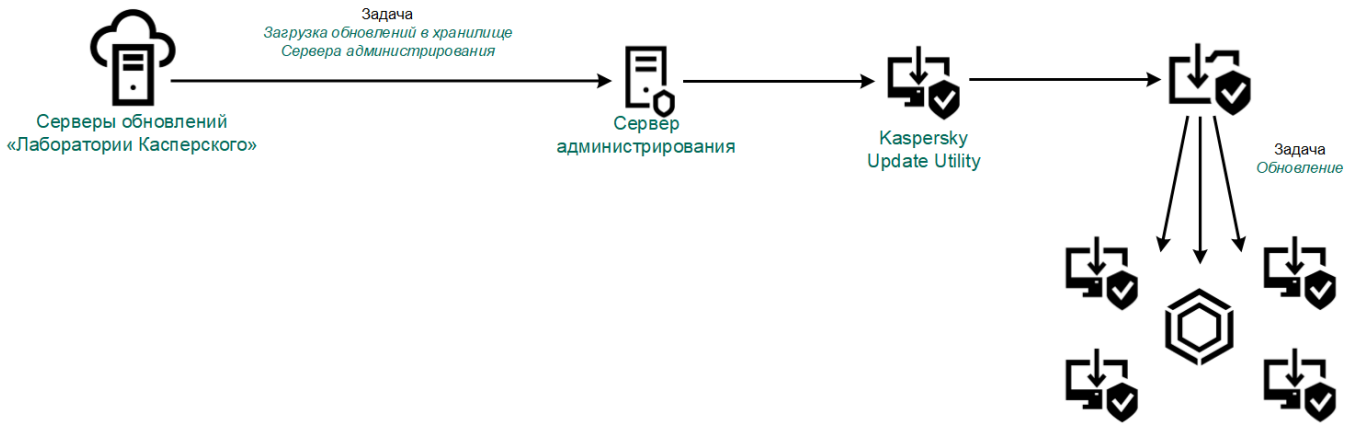
Адрес источника должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.

6. Нажмите на кнопку **Выбрать**.

7. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

   Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

8. Сохраните внесенные изменения.



Обновление с помощью Kaspersky Update Utility

Обновление в мобильном режиме

Мобильный режим – режим работы Kaspersky Endpoint Security, при котором компьютер покидает периметр сети организации (*автономный компьютер*). Подробнее о работе с автономными компьютерами и автономными пользователями см. в справке Kaspersky Security Center.

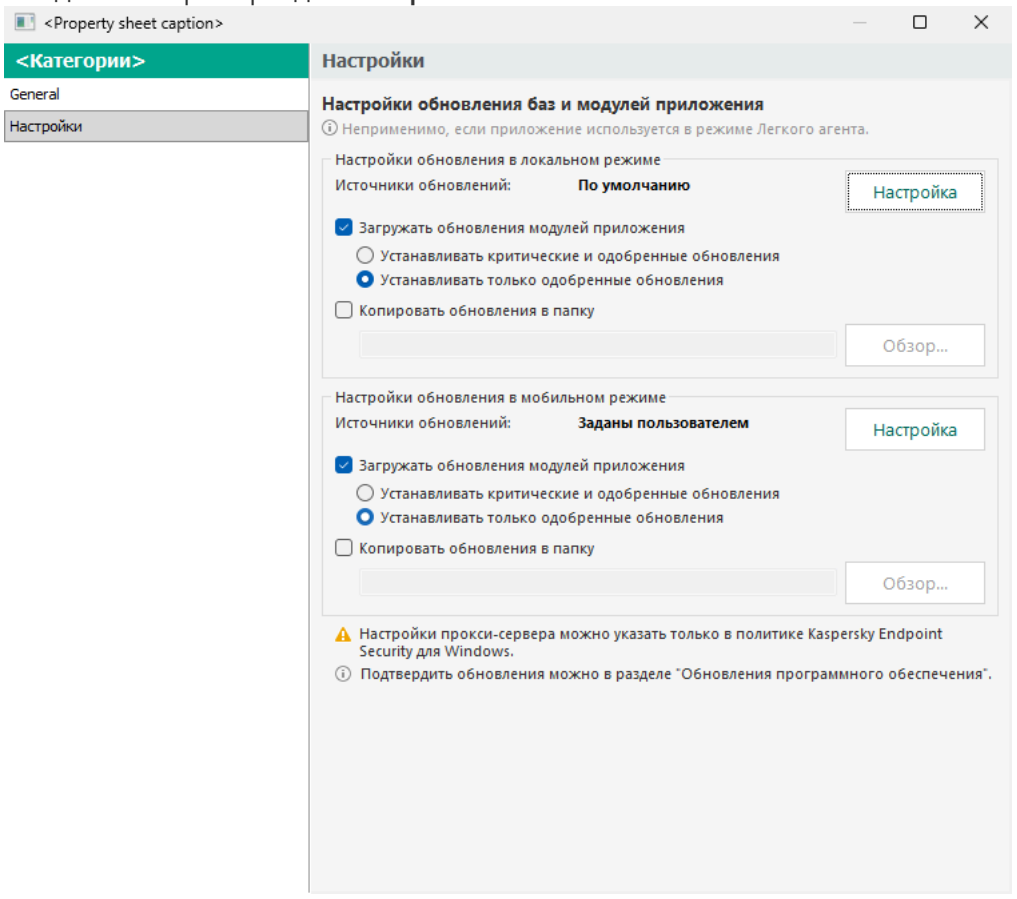
Автономный компьютер за пределами сети организации не может подключиться к Серверу администрирования для обновления баз и модулей приложения. По умолчанию для обновления баз и модулей приложения в мобильном режиме в качестве источника обновлений используются только серверы обновлений "Лаборатории Касперского". Использование прокси-сервера для подключения к интернету определяется специальной политикой для автономных пользователей. Политику для автономных пользователей требуется создать отдельно. После перехода Kaspersky Endpoint Security в мобильный режим задача обновления запускается раз в два часа.

Как настроить параметры обновления в мобильном режиме в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.
3. Нажмите на задачу Kaspersky Endpoint Security **Обновление баз и модулей приложения**.

   Откроется окно свойств задачи.

   Задача *Обновление баз и модулей приложения* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление баз и модулей приложения* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.
4. В окне свойств задачи выберите раздел **Настройки**.



Параметры задачи Обновление баз и модулей приложения

5. В блоке **Настройки обновления в мобильном режиме** нажмите на кнопку **Настройка**.

6. Настройте источники обновлений. В качестве источников обновлений могут быть использованы серверы обновлений "Лаборатории Касперского" или другие FTP- или HTTP-серверы, локальные или сетевые папки.

7. Сохраните внесенные изменения.

Как настроить параметры обновления в мобильном режиме в Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление**.

   Откроется окно свойств задачи.

   Задача *Обновление* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.

3. Выберите вкладку **Параметры приложения → Мобильный режим**.

4. Настройте источники обновлений. В качестве источников обновлений могут быть использованы серверы обновлений "Лаборатории Касперского" или другие FTP- или HTTP-серверы, локальные или сетевые папки.

5. Сохраните внесенные изменения.

В результате на компьютерах пользователей будут обновлены базы и модули приложения при переходе в мобильный режим.

Запуск и остановка задачи обновления

Независимо от выбранного режима запуска задачи обновления вы можете запустить или остановить задачу обновления Kaspersky Endpoint Security в любой момент.

Чтобы запустить или остановить задачу обновления, выполните следующие действия:

1. В главном окне приложения перейдите в раздел **Обновление**.

2. В плитке **Обновление баз и модулей приложения** нажмите на кнопку **Обновить**, если вы хотите запустить задачу обновления.

   Kaspersky Endpoint Security запустит обновление баз и модулей приложения. Приложение покажет процесс проверки, размер загруженных файлов и источник обновления. Вы можете остановить выполнение задачи в любое время кнопкой **Остановить обновление**.

Чтобы запустить или остановить задачу обновления при отображении упрощенного интерфейса приложения, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка приложения, который расположен в области уведомлений панели задач.

2. В контекстном меню в раскрывающемся списке **Задачи** выполните одно из следующих действий:

   - выберите незапущенную задачу обновления, чтобы запустить ее;

   - выберите запущенную задачу обновления, чтобы остановить ее;

   - выберите остановленную задачу обновления, чтобы возобновить ее или запустить ее заново.

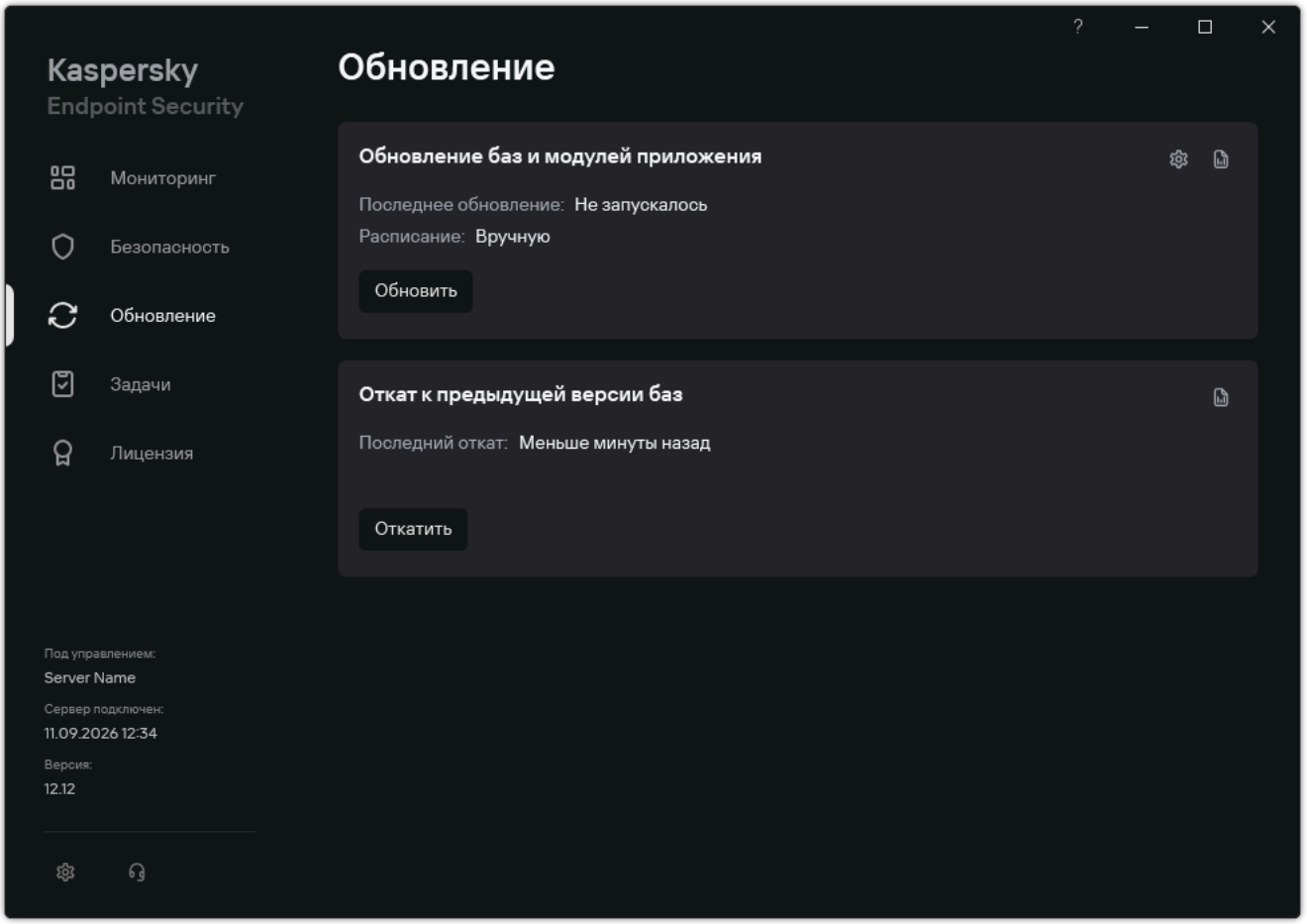
Запуск задачи обновления с правами другого пользователя

По умолчанию задача обновления приложения Kaspersky Endpoint Security запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление приложения Kaspersky Endpoint Security может производиться из источника обновления, к которому у пользователя нет прав доступа (например, из папки общего доступа, содержащей пакет обновлений) или для которого не настроено использование аутентификации на прокси-сервере. Вы можете указать пользователя, обладающего этими правами, в параметрах приложения и запускать задачу обновления приложения Kaspersky Endpoint Security от имени этого пользователя.

Чтобы запускать задачу обновления с правами другого пользователя, выполните следующие действия:

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике.

1. В главном окне приложения перейдите в раздел **Обновление**.



Локальные задачи обновления

2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку ⚙.

   Откроется окно свойств задачи.

3. Нажмите на кнопку **Запускать обновление баз с правами пользователя**.

4. В открывшемся окне выберите вариант **Другого пользователя**.

5. Введите учетные данные пользователя, права которого требуется использовать для доступа к источнику обновлений.

6. Сохраните внесенные изменения.

Выбор режима запуска для задачи обновления

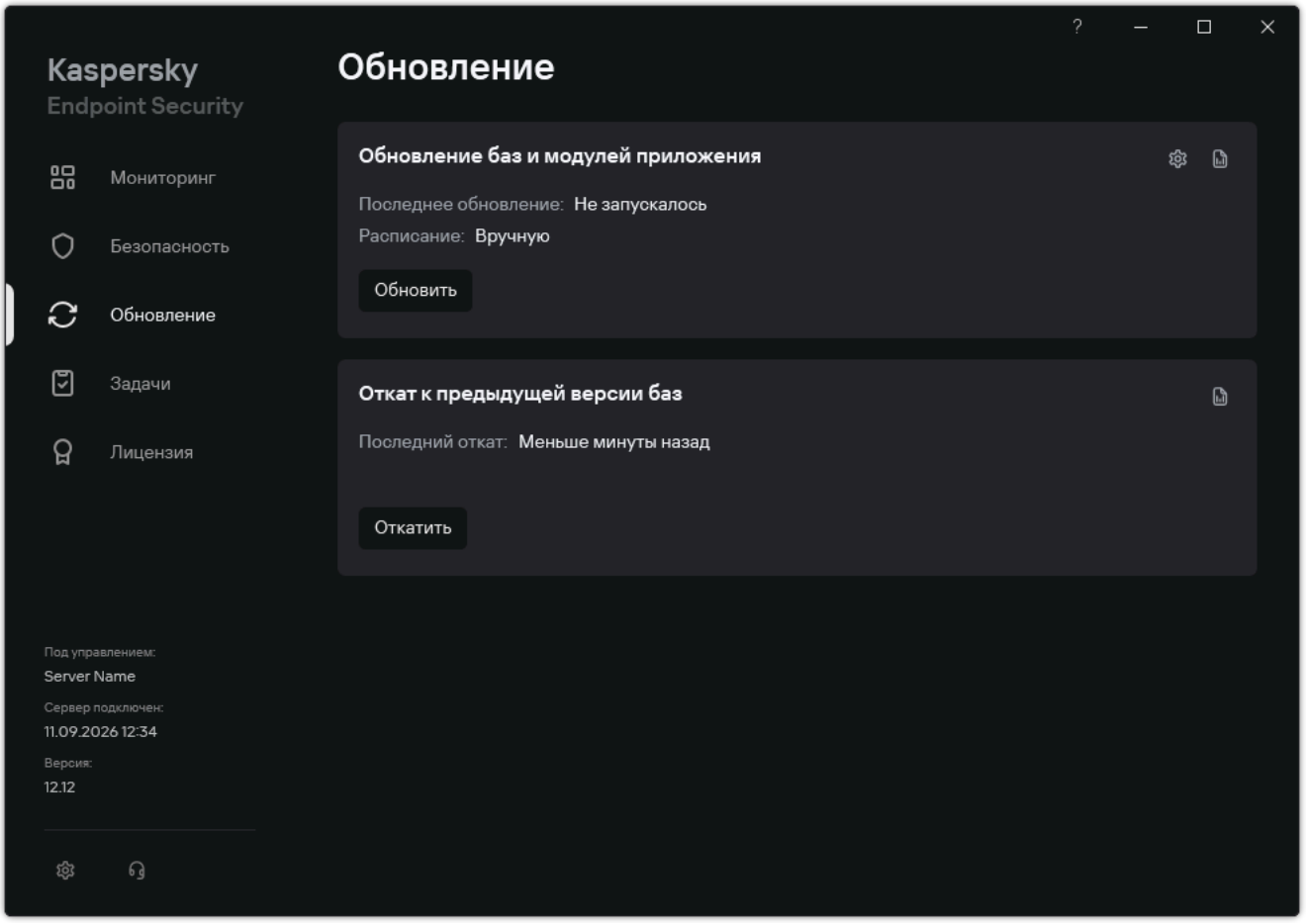
Если по каким-либо причинам запуск задачи обновления невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи обновления, как только это станет возможным.

Вы можете отложить запуск задачи обновления после старта приложения для случаев, если вы выбрали режим запуска задачи обновления **По расписанию** и время запуска Kaspersky Endpoint Security совпадает с расписанием запуска задачи обновления. Задача обновления запускается только по истечении указанного времени после старта Kaspersky Endpoint Security.

Чтобы выбрать режим запуска для задачи обновления, выполните следующие действия:

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике.

1. В главном окне приложения перейдите в раздел **Обновление**.



Локальные задачи обновления

2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку ⚙.

   Откроется окно свойств задачи.

3. Нажмите на кнопку **Режим запуска**.

4. В открывшемся окне выберите режим запуска задачи обновления:

   - Выберите вариант **Автоматически**, если вы хотите, чтобы Kaspersky Endpoint Security запускал задачу обновления в зависимости от наличия пакета обновлений в источнике обновления. Частота проверки Kaspersky Endpoint Security наличия пакета обновлений увеличивается во время вирусных эпидемий и сокращается при их отсутствии.

   - Выберите вариант **Вручную**, если вы хотите запускать задачу обновления вручную.

   - Выберите другие варианты, если вы хотите настроить расписание запуска задачи обновления. Настройте дополнительные параметры запуска задачи обновления:

     - В поле **Отложить запуск после старта приложения на N минут** укажите время, на которое следует отложить запуск задачи обновления после старта Kaspersky Endpoint Security.

     - Установите флажок **Запускать проверку по расписанию на следующий день, если компьютер был выключен**, если вы хотите, чтобы Kaspersky Endpoint Security запускал при первой возможности не запущенные вовремя задачи обновления. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени.

5. Сохраните внесенные изменения.

Добавление источника обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей приложения Kaspersky Endpoint Security.

Источником обновлений могут быть сервер Kaspersky Security Center, серверы обновлений "Лаборатории Касперского", сетевая или локальная папка.

Если серверы обновлений "Лаборатории Касперского" недоступны, Kaspersky Endpoint Security может использовать альтернативные домены для получения обновлений баз и модулей приложения. Подробнее см. в базе знаний Службы технической поддержки.

По умолчанию список источников обновлений содержит сервер Kaspersky Security Center и серверы обновлений "Лаборатории Касперского". Вы можете добавлять в список другие источники обновлений. В качестве источников обновлений можно указывать HTTP- или FTP-серверы, папки общего доступа.

Kaspersky Endpoint Security не поддерживает загрузку обновлений с HTTPS-серверов, если это не серверы обновлений "Лаборатории Касперского".

Если в качестве источников обновлений выбрано несколько ресурсов, в процессе обновления Kaspersky Endpoint Security обращается к ним строго по списку и выполняет задачу обновления, используя пакет обновлений первого доступного источника обновлений.

По умолчанию Kaspersky Endpoint Security использует сервер Kaspersky Security Center в качестве первого источника обновлений. Это позволяет сократить расход трафика при обновлении. Если к компьютеру не применена политика, в параметрах локальной задачи *Обновление баз и модулей приложения* выбраны серверы "Лаборатории Касперского" в качестве первого источника обновления, так как у приложения может отсутствовать доступ к серверу Kaspersky Security Center.

Если приложение работает в режиме Легкого агента, в качестве источника обновлений выбрана папка на SVM.

Как добавить источник обновлений в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

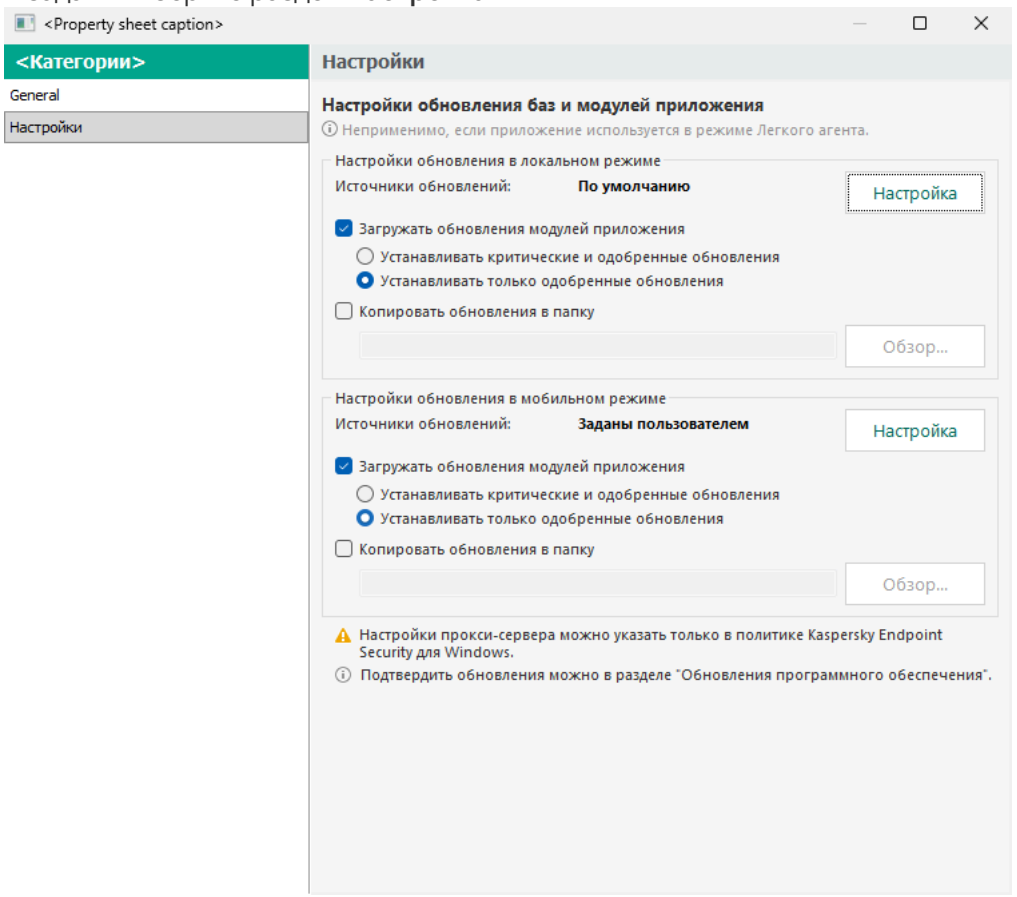
   В дереве консоли выберите папку **Задачи**.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление баз и модулей приложения**.

   Откроется окно свойств задачи.

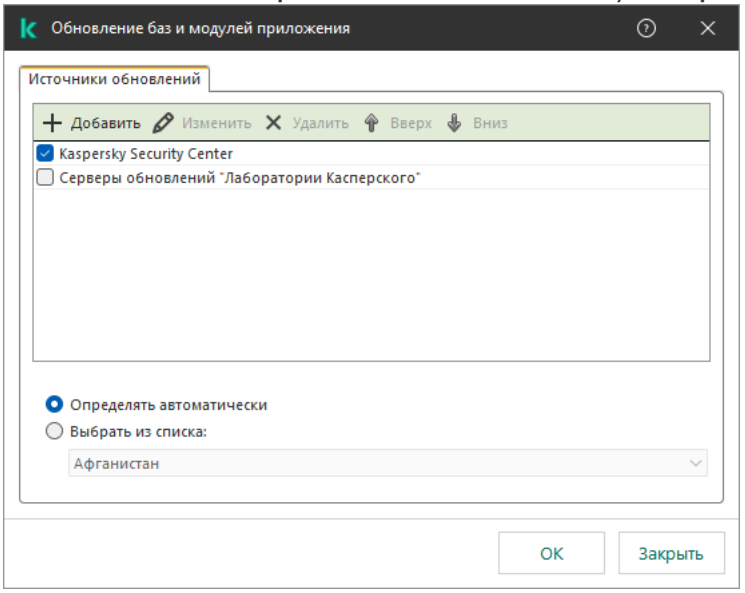
   Задача *Обновление баз и модулей приложения* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление баз и модулей приложения* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.

3. В окне свойств задачи выберите раздел **Настройка**.



Параметры задачи Обновление баз и модулей приложения

4. В блоке **Настройки обновления в локальном режиме** нажмите на кнопку **Настройка**.



Источники обновлений

5. В списке источников обновлений нажмите на кнопку **Добавить**.

6. В поле **Источники обновлений** укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, которая содержит пакет обновлений.

   Формат пути для источника обновлений следующий:

   - Для FTP- или HTTP-сервера введите веб-адрес или IP-адрес сайта.

     Например, `http://dnl-01.geo.kaspersky.com/` или `93.191.13.103`.

     Для FTP-сервера в адресе можно указывать параметры аутентификации в формате `ftp://<user name>:<password>@<node>:<port>`.

   - Для сетевой папки введите UNC-путь.

     Например, `\\Server\Share\Update distribution`.

   - Для локальной папки введите полный путь к папке.

     Например, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   Вы можете исключить источник обновлений, не удаляя его из списка источников. Для этого снимите флажок рядом с ним.

7. Нажмите на кнопку **OK**.

8. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

   Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

9. Если требуется, добавьте источник обновления для мобильного режима работы. *Мобильный режим* – режим работы Kaspersky Endpoint Security, при котором компьютер покидает периметр сети организации (*автономный компьютер*).

10. Сохраните внесенные изменения.

Как добавить источник обновлений в Web Console

1. В главном окне Web Console выберите **Задачи**.

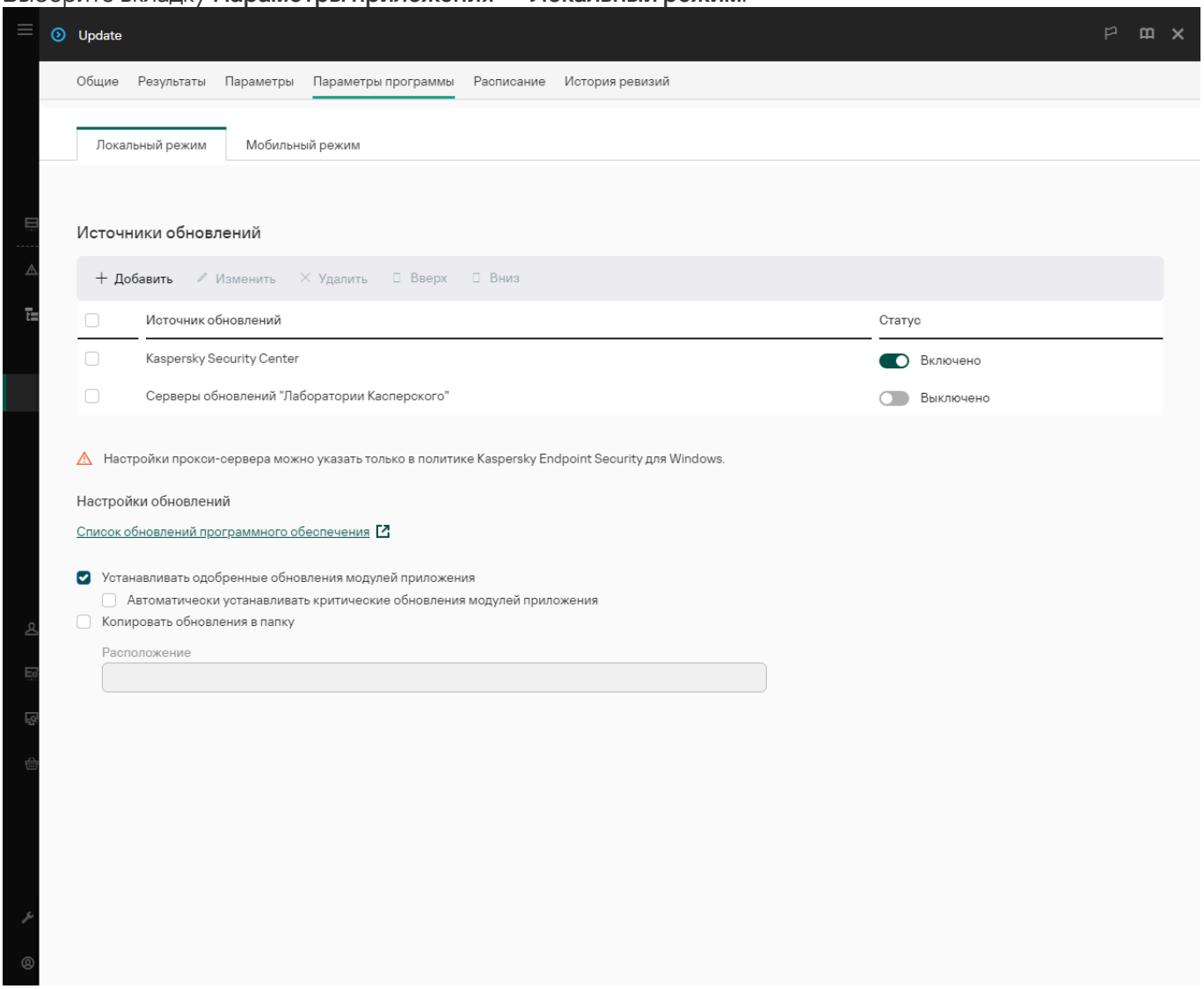
   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление**.

   Откроется окно свойств задачи.

   Задача *Обновление* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.

3. Выберите вкладку **Параметры приложения → Локальный режим**.



Источники обновлений

4. В списке источников обновлений нажмите на кнопку **Добавить**.

5. В открывшемся окне укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, которая содержит пакет обновлений.

   Формат пути для источника обновлений следующий:

   - Для FTP- или HTTP-сервера введите веб-адрес или IP-адрес сайта.

     Например, `http://dnl-01.geo.kaspersky.com/` или `93.191.13.103`.

Для FTP-сервера в адресе можно указывать параметры аутентификации в формате `ftp://<user name>:<password>@<node>:<port>`.

- Для сетевой папки введите UNC-путь.

  Например, `\\Server\Share\Update distribution`.

- Для локальной папки введите полный путь к папке.

  Например, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

Вы можете исключить источник обновлений, не удаляя его из списка источников. Для этого выключите переключатель рядом с ним.

6. Нажмите на кнопку **OK**.

7. Настройте приоритеты источников обновлений с помощью кнопок **Переместить вверх** и **Переместить вниз**.

   Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

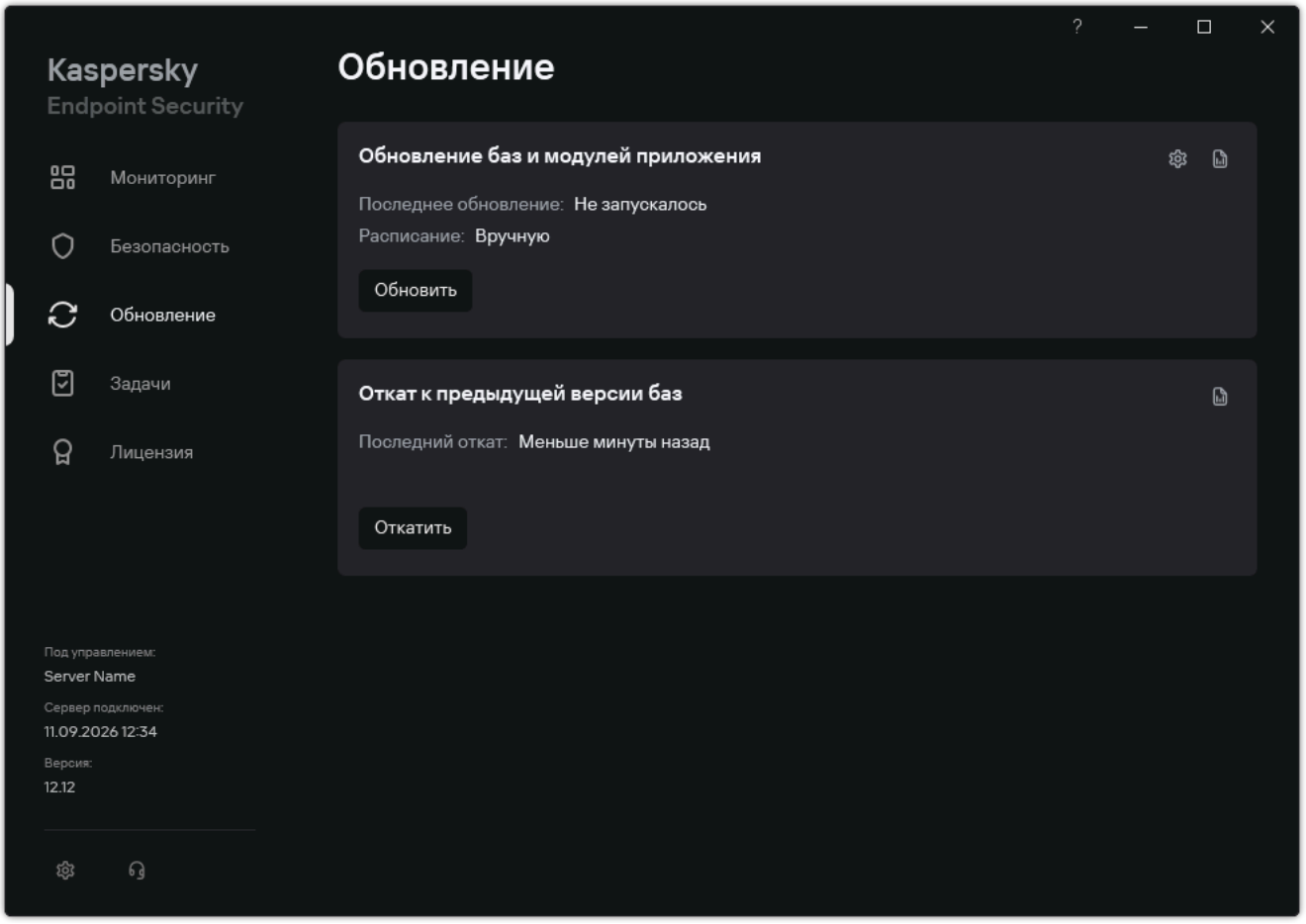
8. Если требуется, добавьте источник обновления для мобильного режима работы. *Мобильный режим* – режим работы Kaspersky Endpoint Security, при котором компьютер покидает периметр сети организации (*автономный компьютер*).

9. Сохраните внесенные изменения.

Как добавить источник обновлений в интерфейсе приложения

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике.

1. В главном окне приложения перейдите в раздел **Обновление**.



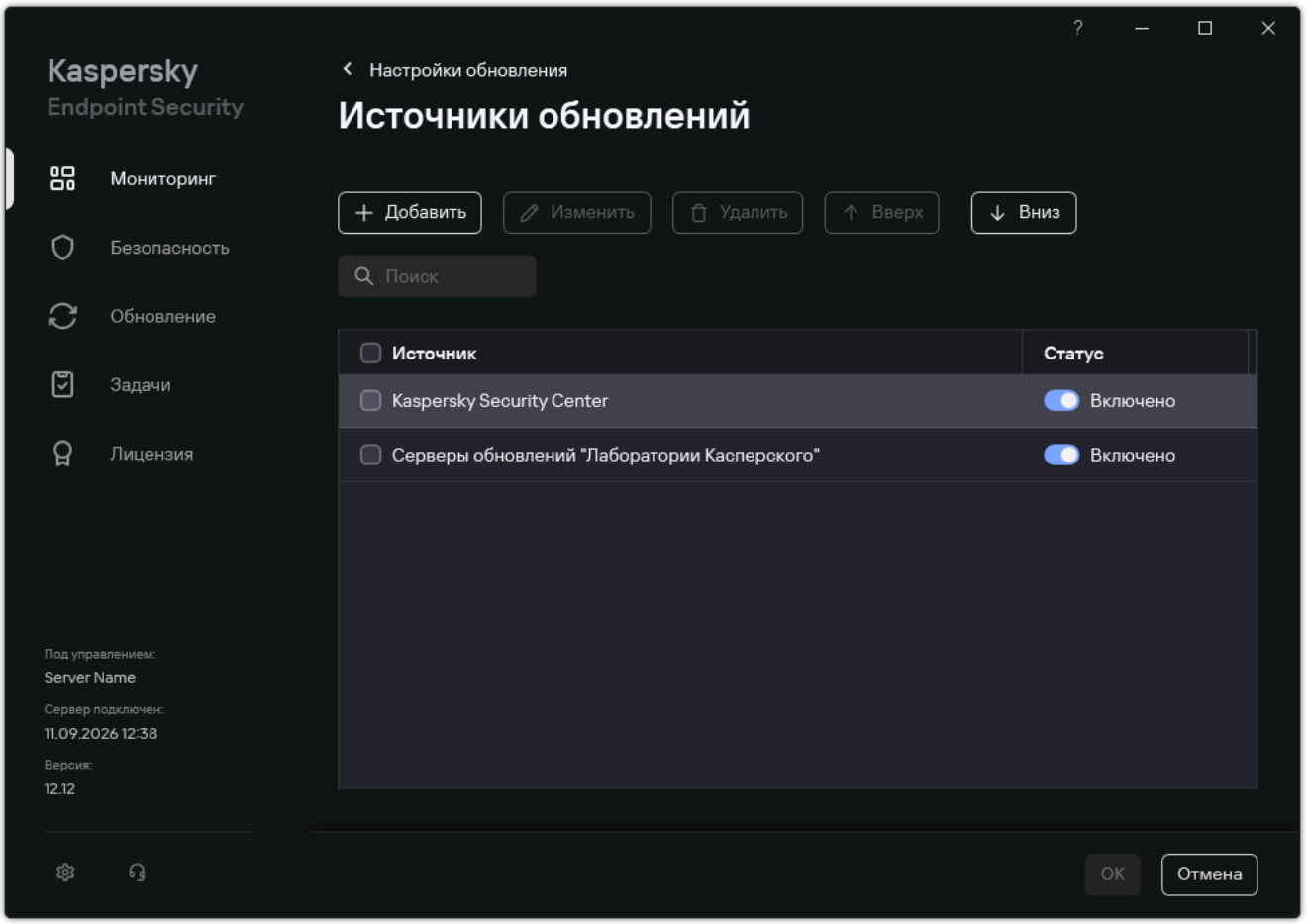
Локальные задачи обновления

2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку ⚙.

   Откроется окно свойств задачи.

3. Нажмите на кнопку **Настроить источники обновлений**.

4. В открывшемся окне нажмите на кнопку **Добавить**.



Источники обновлений

5. В открывшемся окне укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, которая содержит пакет обновлений.

   Формат пути для источника обновлений следующий:

   - Для FTP- или HTTP-сервера введите веб-адрес или IP-адрес сайта.

     Например, `http://dnl-01.geo.kaspersky.com/` или `93.191.13.103`.

     Для FTP-сервера в адресе можно указывать параметры аутентификации в формате `ftp://<user name>:<password>@<node>:<port>`.

   - Для сетевой папки введите UNC-путь.

     Например, `\\Server\Share\Update distribution`.

   - Для локальной папки введите полный путь к папке.

     Например, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Нажмите на кнопку **Выбрать**.

7. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

8. Сохраните внесенные изменения.

Обновление модулей приложения

Обновления модулей приложения исправляют ошибки, улучшают производительность, а также добавляют новые функции. При появлении нового обновления модулей приложения вам необходимо подтвердить установку обновления. Вы можете подтвердить установку обновления модулей приложения в интерфейсе приложения или в Kaspersky Security Center. При появлении обновления приложение покажет уведомление в главном окне Kaspersky Endpoint Security – . Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения, то приложение устанавливает обновление после согласия с положениями Лицензионного соглашения.

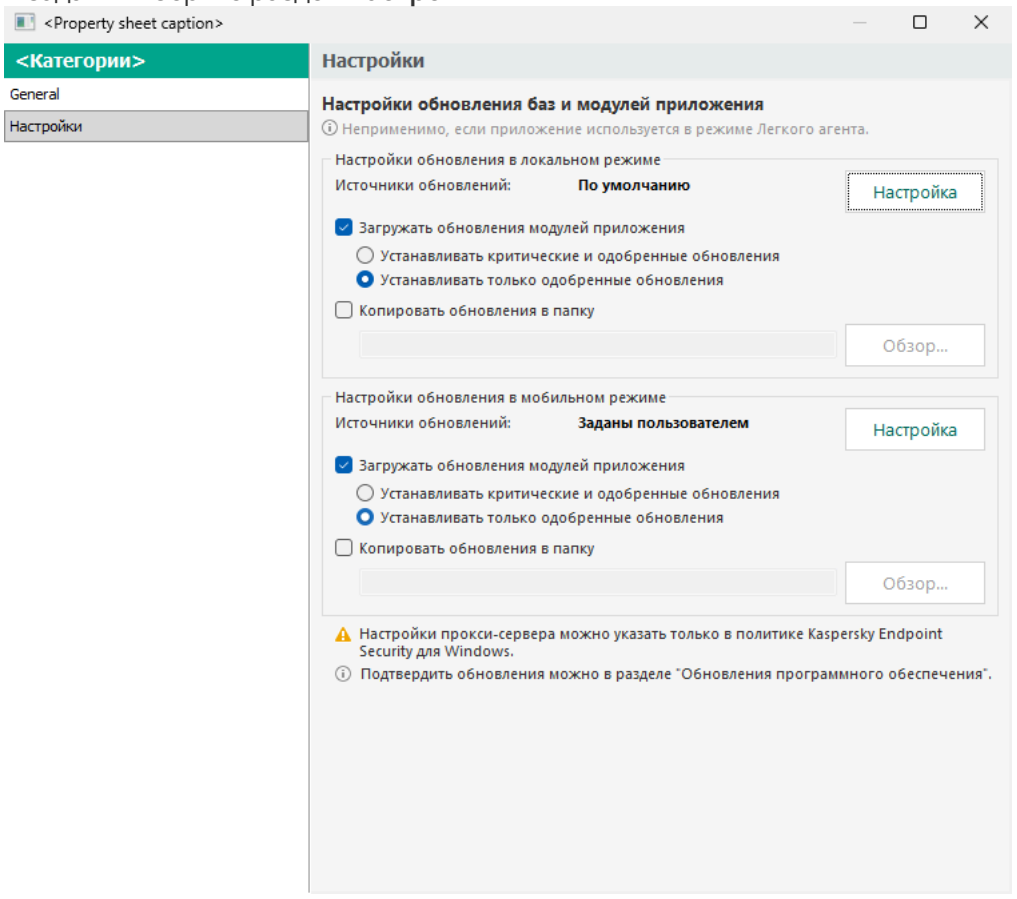
После установки обновления приложения может потребоваться перезагрузка компьютера.

Как настроить обновление модулей приложения в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.
3. Нажмите на задачу Kaspersky Endpoint Security **Обновление баз и модулей приложения**.

   Откроется окно свойств задачи.

   Задача *Обновление баз и модулей приложения* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление баз и модулей приложения* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.
4. В окне свойств задачи выберите раздел **Настройки**.



Параметры задачи Обновление баз и модулей приложения

5. В блоке **Настройки обновления в локальном режиме** установите флажок **Загружать обновления модулей приложения**.

   Если вы хотите запретить загрузку обновлений модулей приложения, снимите флажок **Загружать обновления модулей приложения** и запретите использование локальных задач пользователем.

6. Выберите обновления модулей приложения, которые вы хотите устанавливать:

   - **Устанавливать критические и одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает критические обновления автоматически, а остальные обновления модулей приложения – после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center.

   - **Устанавливать только одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center. Этот вариант выбран по умолчанию.

7. Если требуется, настройте обновление модулей приложения для мобильного режима работы. *Мобильный режим* – режим работы Kaspersky Endpoint Security, при котором компьютер покидает периметр сети организации (*автономный компьютер*).

8. Сохраните внесенные изменения.

Как настроить обновление модулей приложения в Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

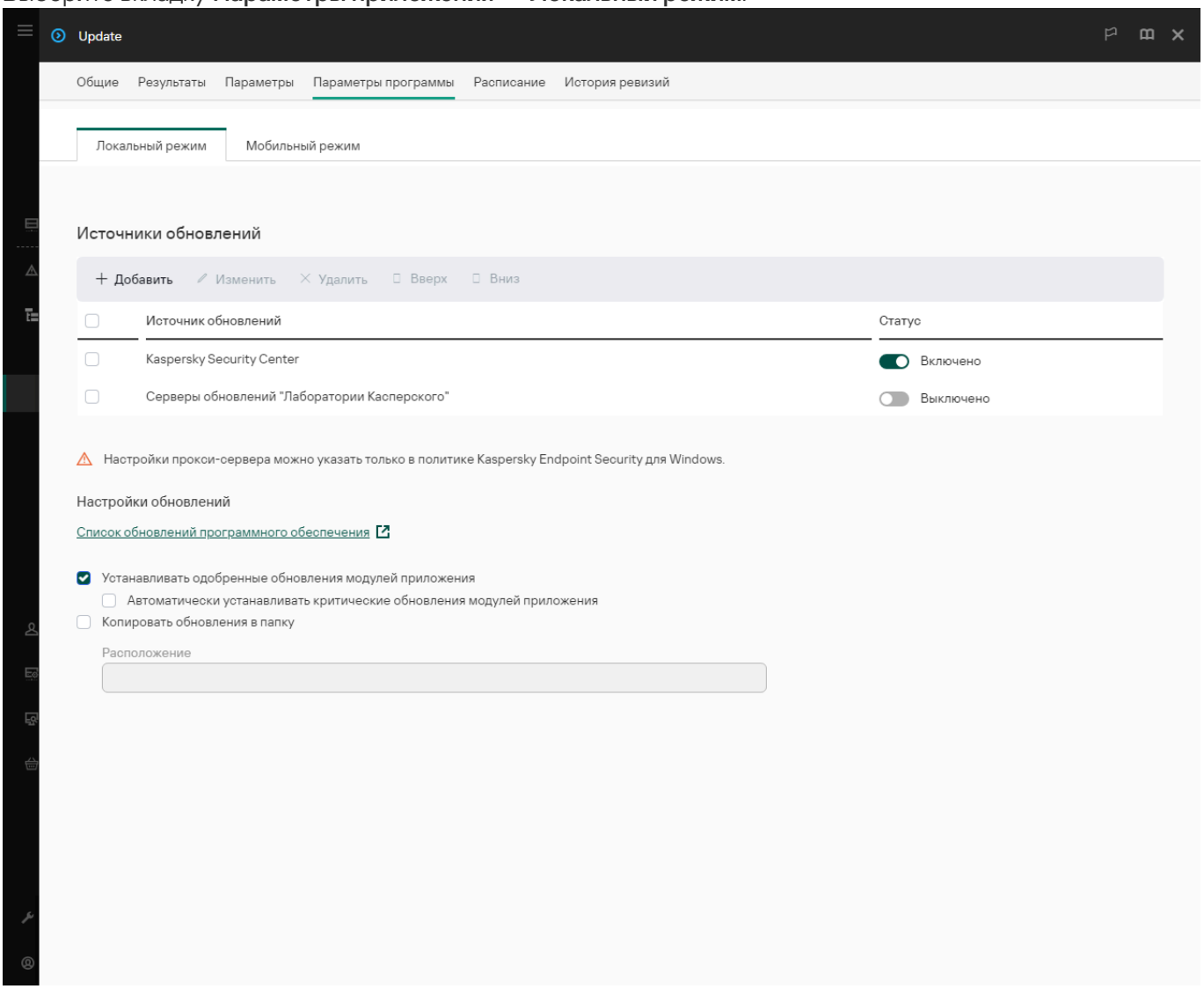
   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление баз и модулей приложения**.

   Откроется окно свойств задачи.

   Задача *Обновление баз и модулей приложения* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление баз и модулей приложения* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Windows.

3. Выберите вкладку **Параметры приложения** → **Локальный режим**.



Параметры задачи Обновление

4. В блоке **Настройки обновлений** выберите обновления модулей приложения, которые вы хотите устанавливать:

   - **Устанавливать одобренные обновления модулей приложения**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center. Этот вариант выбран по умолчанию.

   - **Автоматически устанавливать критические обновления модулей приложения**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает критические обновления автоматически, а остальные обновления модулей приложения – после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center.

   Если вы хотите запретить загрузку обновлений модулей приложения, снимите флажки **Устанавливать одобренные обновления модулей приложения** и **Автоматически устанавливать критические обновления модулей приложения** и запретите использование локальных задач пользователем.

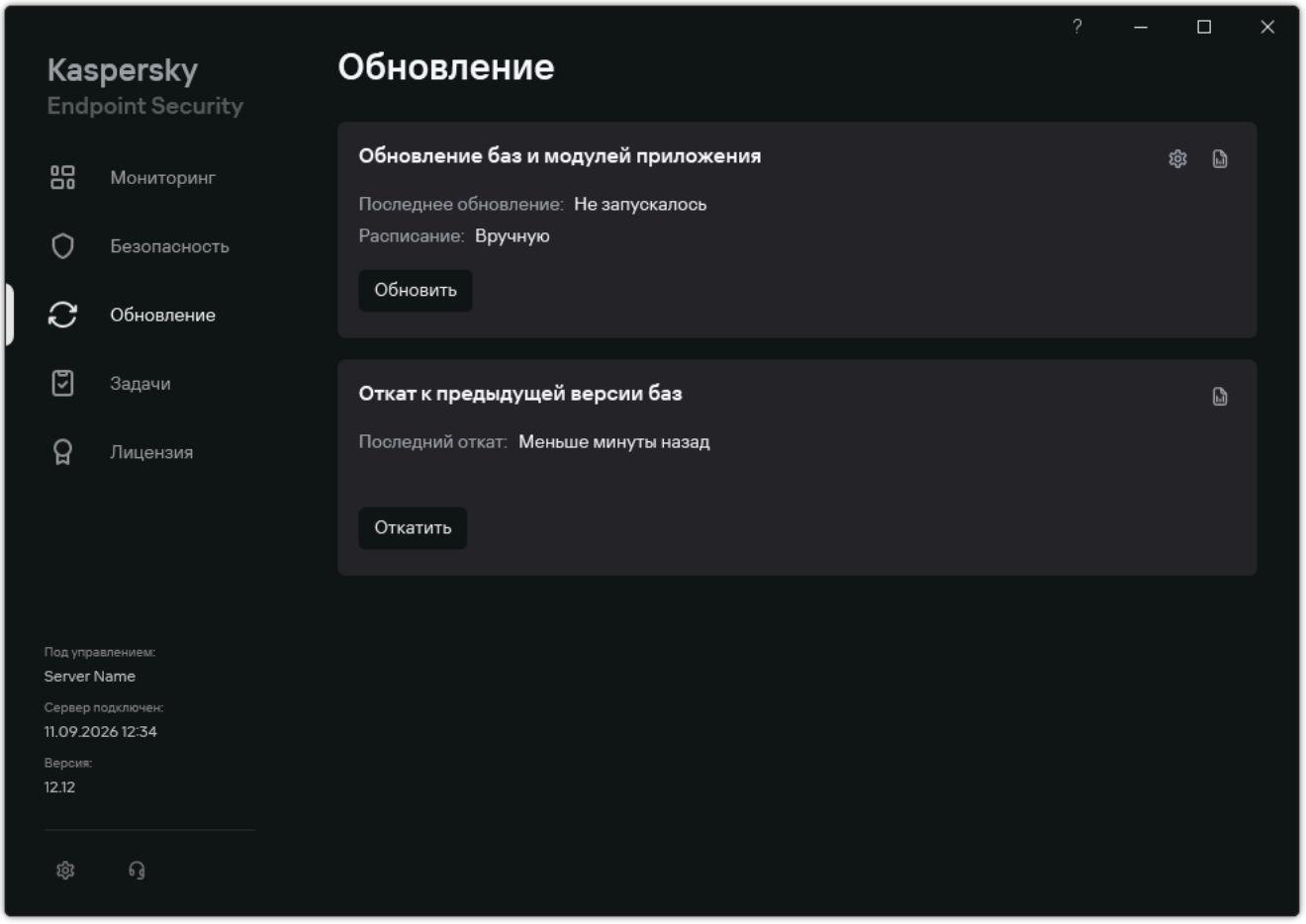
5. Если требуется, настройте обновление модулей приложения для мобильного режима работы. *Мобильный режим* – режим работы Kaspersky Endpoint Security, при котором компьютер покидает периметр сети организации (*автономный компьютер*).

6. Сохраните внесенные изменения.

Как настроить обновление модулей приложения в интерфейсе приложения

Настроить групповую задачу *Обновление баз и модулей приложения* в интерфейсе приложения невозможно. Пользователю доступна только локальная задача обновления – *Обновление баз и модулей приложения*. Если задача *Обновление баз и модулей приложения* не отображается, администратор запретил использование локальных задач в политике.

1. В главном окне приложения перейдите в раздел **Обновление**.



Локальные задачи обновления

2. В открывшемся списке задач выберите задачу *Обновление баз и модулей приложения* и нажмите на кнопку ⚙.

   Откроется окно свойств задачи.

3. В блоке **Загрузка и установка обновлений модулей приложения** установите флажок **Загружать обновления модулей приложения**.

4. Выберите обновления модулей приложения, которые вы хотите устанавливать:

   - **Устанавливать критические и одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает критические обновления автоматически, а остальные обновления модулей приложения – после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center.

   - **Устанавливать только одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center. Этот вариант выбран по умолчанию.

5. Сохраните внесенные изменения.

Использование прокси-сервера при обновлении

Для загрузки обновлений баз и модулей приложения из источника обновлений может потребоваться указать параметры прокси-сервера. Если источников обновлений несколько, параметры прокси-сервера применяются для всех источников. Если для некоторых источников обновлений прокси-сервер не нужен, вы можете выключить использование прокси-сервера в свойствах политики. Kaspersky Endpoint Security также будет использовать прокси-сервер для доступа к Kaspersky Security Network и серверам активации.

Чтобы настроить подключение к источникам обновлений через прокси-сервер, выполните следующие действия:

1. В главном окне Web Console нажмите ⚙.

   Откроется окно свойств Сервера администрирования.

2. Перейдите в раздел **Параметры доступа к сети интернет**.

3. Установите флажок **Использовать прокси-сервер**.

4. Настройте параметры подключения к прокси-серверу: адрес прокси-сервера, порт и параметры аутентификации (имя пользователя и пароль).

5. Сохраните внесенные изменения.

Чтобы выключить использование прокси-сервера для определенной группы администрирования, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки** → **Настройки сети**.

5. В блоке **Прокси-сервер** нажмите на кнопку **Настройки**.

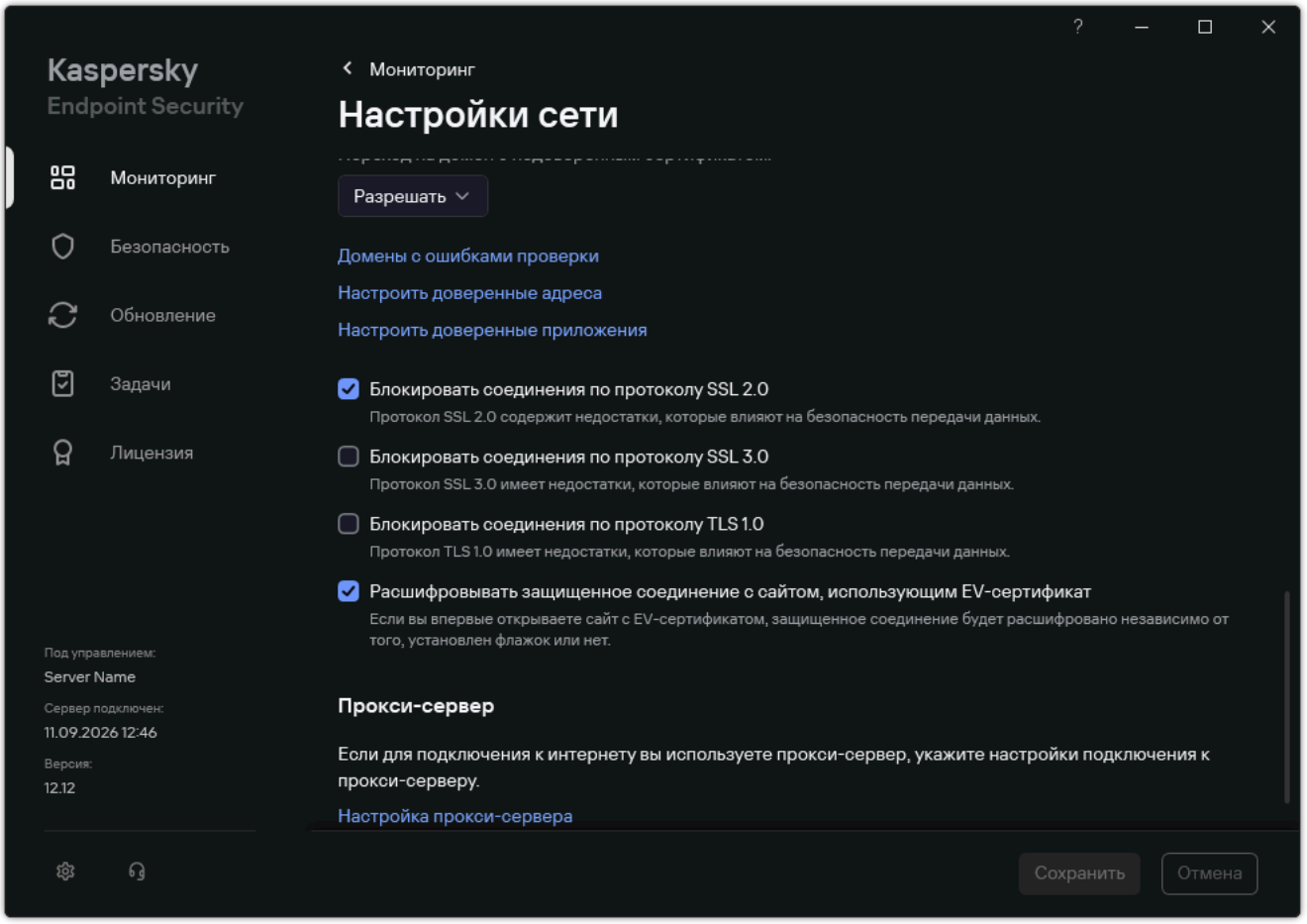
6. В открывшемся окне установите флажок **Не использовать прокси-сервер для локальных адресов**.

7. Сохраните внесенные изменения.

Чтобы настроить параметры прокси-сервера в интерфейсе приложения, выполните следующие действия:

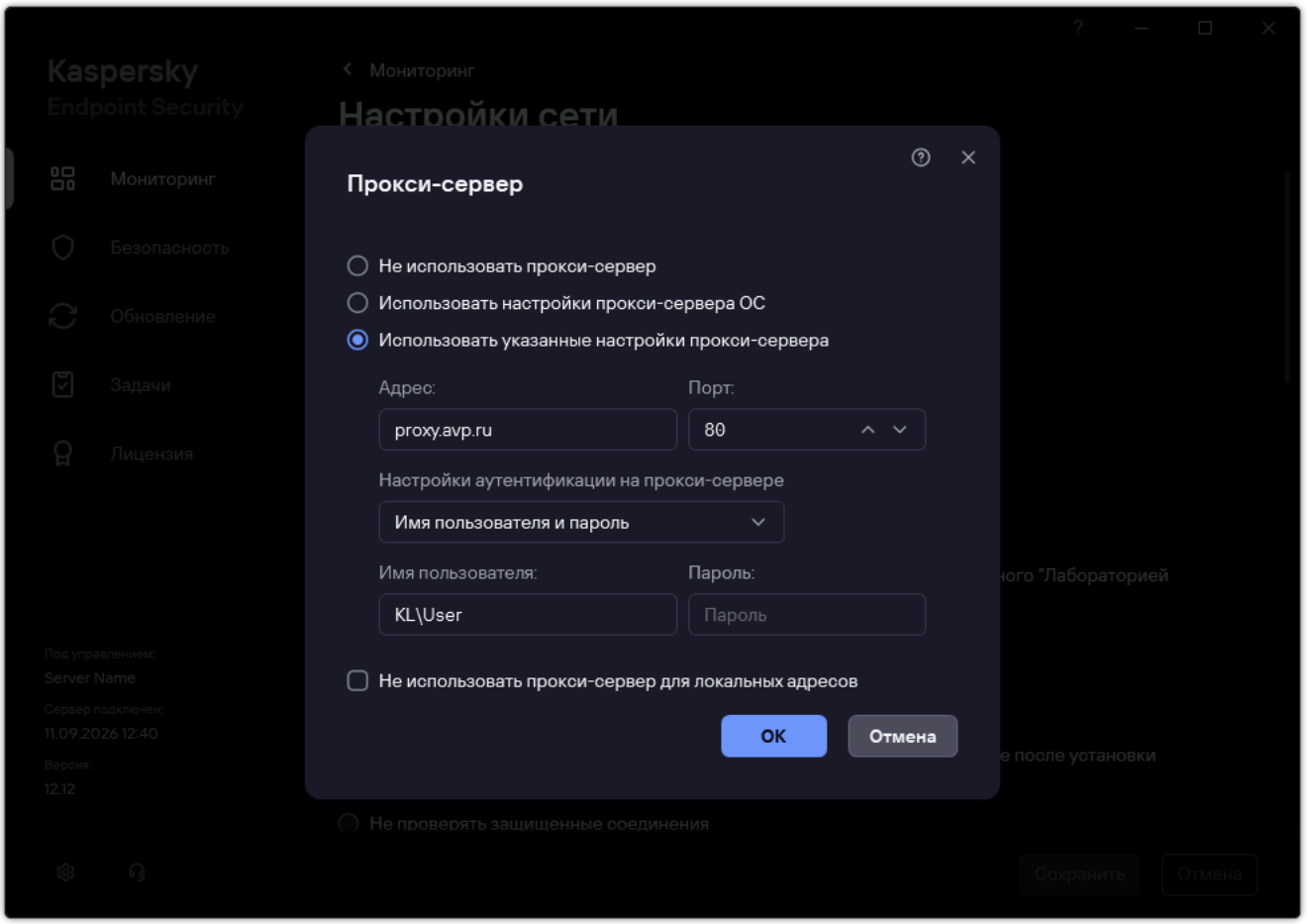
1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.



Параметры сети приложения

3. В блоке **Прокси-сервер** перейдите по ссылке **Настройка прокси-сервера**.



Параметры подключения к прокси-серверу

4. В открывшемся окне выберите один из следующих вариантов определения адреса прокси-сервера:

   - **Использовать настройки прокси-сервера ОС**.

     Этот вариант выбран по умолчанию. Kaspersky Endpoint Security использует параметры прокси-сервера, заданные в параметрах операционной системы.

   - **Использовать указанные настройки прокси-сервера**.

     Если вы выбрали этот вариант, настройте параметры подключения к прокси-серверу: адрес прокси-сервера и порт.

5. Выберите способ аутентификации приложения на прокси-сервере. По умолчанию приложение использует доменную NTLM-аутентификацию текущего пользователя.

6. Если вы хотите выключить использование прокси-сервера при обновлении баз и модулей приложения из папки общего доступа, установите флажок **Не использовать прокси-сервер для локальных адресов**.

7. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет использовать прокси-сервер для загрузки обновлений баз и модулей приложения. Также Kaspersky Endpoint Security использует прокси-сервер для доступа к серверам KSN и серверам активации "Лаборатории Касперского". Если требуется аутентификация на прокси-сервере, а учетные данные пользователя не указаны или указаны неверно, Kaspersky Endpoint Security запросит имя пользователя и пароль.

Откат последнего обновления

После второго обновления баз и модулей приложения становится доступна функция отката к предыдущим базам и модулям приложения.

Каждый раз, когда пользователь запускает обновление, Kaspersky Endpoint Security создает резервную копию используемых баз и модулей приложения и только потом приступает к их обновлению. Это позволяет вернуться к использованию предыдущих баз и модулей приложения при необходимости. Возможность отката последнего обновления полезна, например, в случае, если новая версия баз вызывает ложное срабатывание, из-за которого Kaspersky Endpoint Security блокирует безопасное приложение.

Kaspersky Endpoint Security в режиме Легкого агента не поддерживает задачу *Откат обновления*.

Как откатить последнее обновление в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

1. Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Откат обновления**.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 3. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную.

Шаг 4. Определение названия задачи

Введите название задачи.

Шаг 7. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как откатить последнее обновление в Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Откат обновления баз**.

   c. В поле **Название задачи** введите короткое описание, например, *Откат обновления*.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

5. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.

6. Завершите работу мастера.

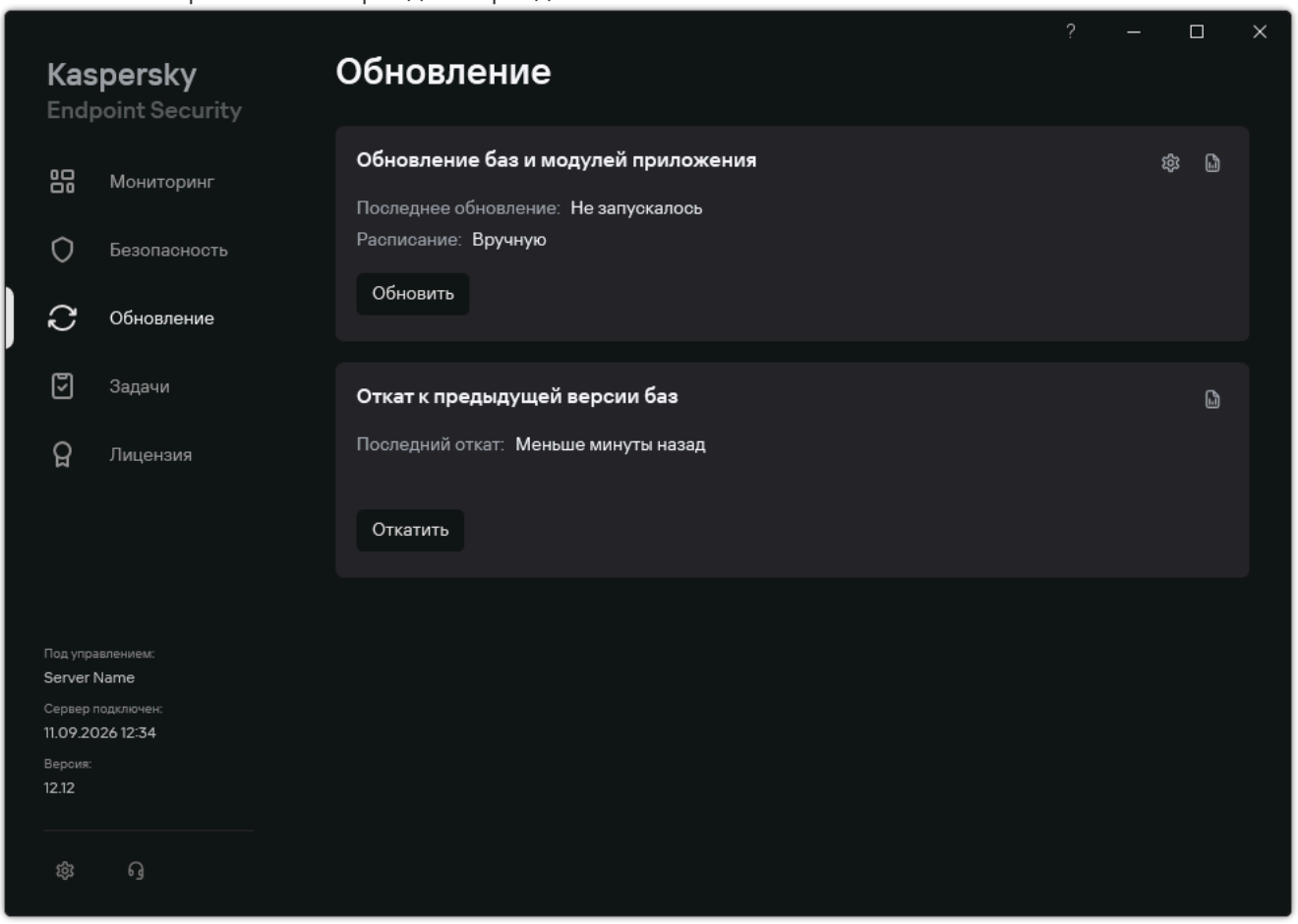
7. В списке задач отобразится новая задача.

8. Установите флажок напротив задачи.

9. Нажмите на кнопку **Запустить**.

Как откатить последнее обновление в интерфейсе приложения

1. В главном окне приложения перейдите в раздел **Обновление**.



Локальные задачи обновления

2. В плитке **Откат к предыдущей версии баз** нажмите на кнопку **Откатить**.

Kaspersky Endpoint Security запустит откат последнего обновления баз. Приложение покажет процесс отката, размер загруженных файлов и источник обновления. Вы можете остановить выполнение задачи в любое время кнопкой **Остановить обновление**.

Технология лечения активного заражения

Для работы с активными угрозами Kaspersky Endpoint Security использует технологию лечения активного заражения. Лечение активного заражения для рабочих станций и серверов отличается. Вы можете настроить лечение активного заражения в свойствах задачи *Поиск вредоносного ПО* и в параметрах приложения.

Если Kaspersky Endpoint Security не может остановить выполнение вредоносного приложения, вы можете использовать технологию лечения активного заражения. Для компьютеров под политикой технология лечения активного заражения по умолчанию выключена, так как технология использует значительные ресурсы компьютера. Для компьютеров не под политикой технология лечения активного заражения по умолчанию включена.

Работа технологии лечения активного заражения для рабочих станций и серверов отличается. Для работы технологии на серверах вам нужно включить немедленное лечение активного заражения в свойствах задачи *Поиск вредоносного ПО*. Для работы технологии на рабочих станциях это условие не является обязательным.

Как включить или выключить технологию лечения активного заражения в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Настройки приложения**.
4. В блоке **Общие** используйте флажок **Применять технологию лечения активного заражения**, чтобы включить или выключить технологию лечения активного заражения.
5. Сохраните внесенные изменения.

Как включить или выключить технологию лечения активного заражения в Web Console и Cloud Console

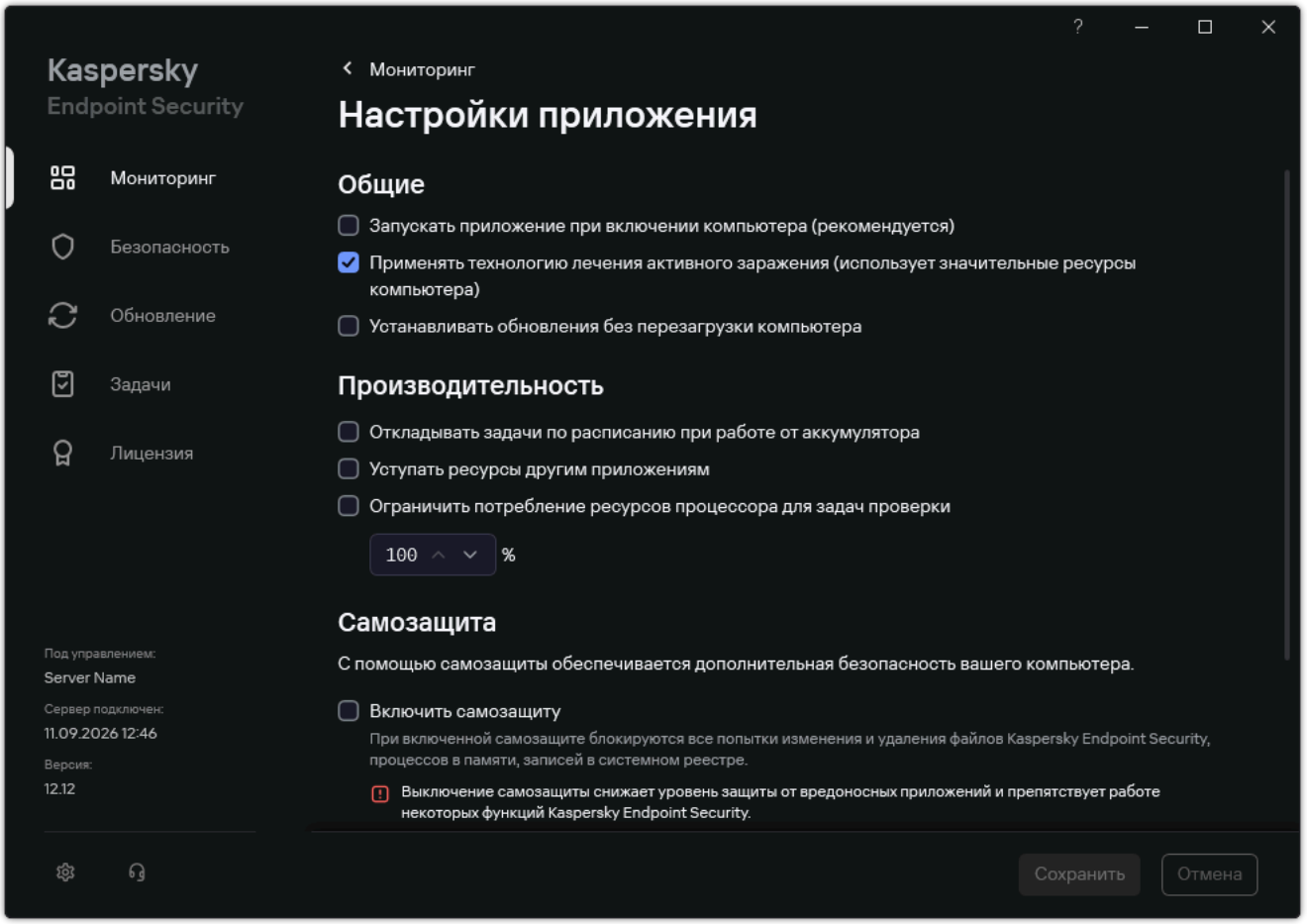
1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Общие настройки** → **Настройки обнаружения**.
5. В блоке **Технология лечения активного заражения** используйте переключатель **Технология лечения активного заражения ВКЛЮЧЕНА**, чтобы включить или выключить технологию лечения активного заражения.
6. Сохраните внесенные изменения.

Как включить или выключить технологию лечения активного заражения в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.



Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Общие** используйте флажок **Применять технологию лечения активного заражения (использует значительные ресурсы компьютера)**, чтобы включить или выключить технологию лечения активного заражения.

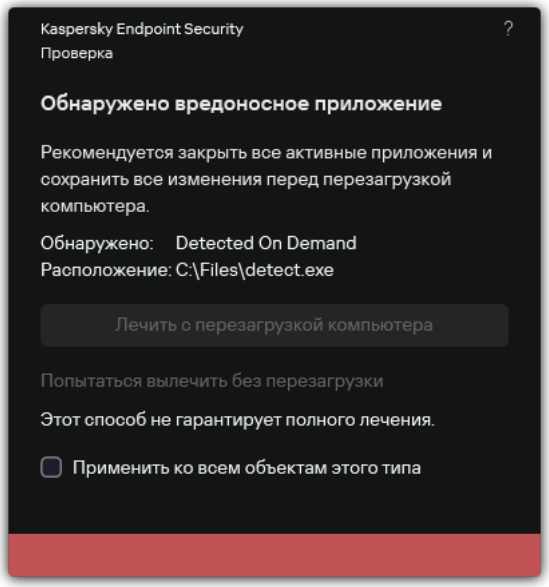
4. Сохраните внесенные изменения.

В результате при лечении активного заражения пользователю не будут доступны большинство функций операционной системы. После завершения лечения компьютер будет перезагружен.

Лечение активных угроз на рабочих станциях

Для работы с активными угрозами на рабочих станциях вам нужно включить технологию лечения активного заражения в параметрах приложения. Далее вам нужно настроить взаимодействие приложения с пользователем в свойствах задачи *Поиск вредоносного ПО*. В свойствах задачи есть флажок **Выполнять лечение активного заражения немедленно**. Если флажок установлен, Kaspersky Endpoint Security выполнит лечение без уведомления пользователя. После лечения угроз компьютер будет перезагружен. Если флажок снят, Kaspersky Endpoint Security показывает уведомление об обнаружении активных угроз (см. рис. ниже). Закрыть уведомление, не обработав файл, невозможно.

Лечение активного заражения в ходе выполнения задачи поиска вирусов на компьютере осуществляется только в том случае, если в свойствах примененной к этому компьютеру политики включена функция лечения активного заражения.



Уведомление об активной угрозе

Лечение активных угроз на серверах

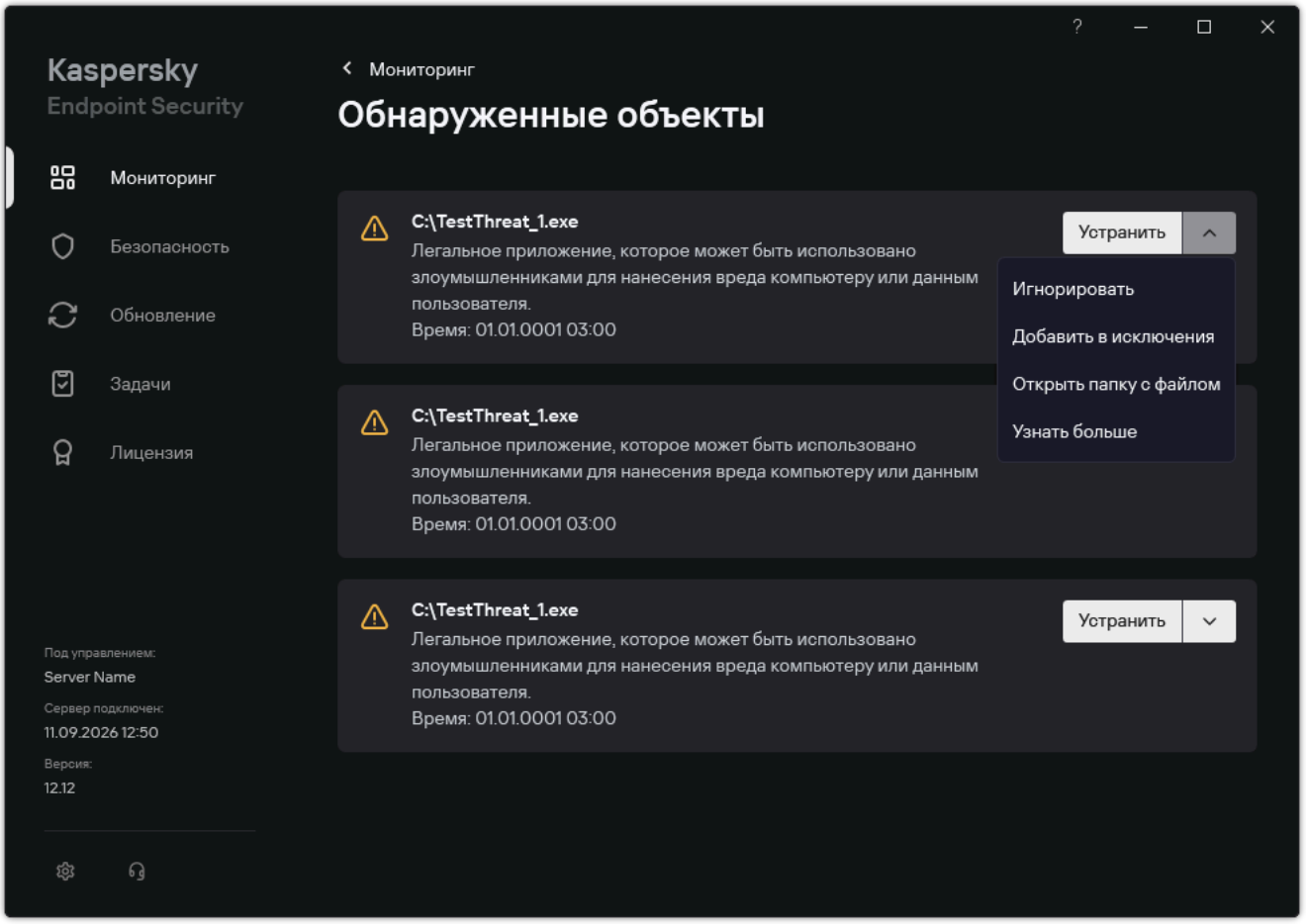
Для работы с активными угрозами на серверах вам нужно выполнить следующие действия:

- включите технологию лечения активного заражения в параметрах приложения;
- включите немедленное лечение активного заражения в свойствах задачи *Поиск вредоносного ПО*.

Если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов, Kaspersky Endpoint Security не показывает уведомление. Таким образом, пользователь не может выбрать действие для лечения активного заражения. Для устранения угрозы вам необходимо включить технологию лечения активного заражения в параметрах приложения и включить немедленное лечение активного заражения в свойствах задачи *Поиск вредоносного ПО*. Далее вам нужно запустить задачу *Поиск вредоносного ПО*.

Устранение необработанных угроз

Kaspersky Endpoint Security фиксирует информацию о файлах, которые она по каким-либо причинам не обработала. Эта информация записывается в виде событий в список активных угроз (см. рис. ниже).



Список активных угроз

Зараженный файл считается *обработанным*, если Kaspersky Endpoint Security в процессе проверки компьютера на вирусы и другие приложения, представляющие угрозу, вылечил или удалил угрозу.

Kaspersky Endpoint Security помещает файл в список активных угроз, если в процессе проверки компьютера на вирусы и другие приложения, представляющие угрозу, Kaspersky Endpoint Security по каким-либо причинам не совершил действие с этим файлом согласно заданным настройкам приложения.

Такая ситуация возможна в следующих случаях:

- Проверяемый файл недоступен (например, находится на сетевом диске или внешнем диске без прав на запись данных).
- В настройках задачи *Поиск вредоносного ПО* при обнаружении угрозы выбрано действие **Информировать**. Далее, когда на экране отобразилось уведомление о зараженном файле, пользователь выбрал вариант **Пропустить**.

При наличии необработанных угроз Kaspersky Endpoint Security изменит значок на . В главном окне приложения появится сообщение об угрозе (см. рис ниже). В консоли Kaspersky Security Center статус компьютера будет изменен на *Критический* – .

Как обработать угрозу в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку **Сервер администрирования** → **Дополнительно** → **Хранилища** → **Активные угрозы**.

   Откроется список активных угроз.

2. Выберите объект, который вы хотите обработать.

3. Выберите способ обработки угрозы:

   - **Лечить**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.

   - **Удалить**. Если выбран этот вариант действия, то приложение удаляет обнаруженный зараженный файл из хранилища активных угроз. При этом приложение оставляет обнаруженный файл в памяти компьютера. Для устранения угрозы на компьютере нужно выбрать **Лечить**.

Как обработать угрозу в Web Console

1. В главном окне Web Console выберите **Операции** → **Хранилища** → **Активные угрозы**.

   Откроется список активных угроз.

2. Выберите объект, который вы хотите обработать.

3. Выберите способ обработки угрозы:

   - **Лечить**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.

   - **Удалить**. Если выбран этот вариант действия, то приложение удаляет обнаруженный зараженный файл из хранилища активных угроз. При этом приложение оставляет обнаруженный файл в памяти компьютера. Для устранения угрозы на компьютере нужно выбрать **Лечить**.

Как обработать угрозу в интерфейсе приложения

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Безопасность под угрозой**.

   Откроется список активных угроз.

2. Выберите объект, который вы хотите обработать.

3. Выберите способ обработки угрозы:

   - **Устранить**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.

   - **Добавить в исключения**. Если выбран этот вариант действия, то Kaspersky Endpoint Security предложит добавить файл в список исключений из проверки. Приложение автоматически настроит параметры исключения. Если добавление исключения недоступно, администратор запретил добавление исключений в параметрах политики.

   - **Игнорировать**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удалит запись из списка активных угроз. Если в списке не осталось активных угроз, статус компьютера будет изменен на *OK*. При повторном обнаружении объекта Kaspersky Endpoint Security снова добавит запись в список активных угроз.

- **Открыть папку с файлом**. Если выбран этот вариант действия, то Kaspersky Endpoint Security откроет папку с объектом в файловом менеджере. Далее вы можете вручную удалить объект или переместить объект в папку, которая не входит в область защиты.

- **Узнать больше**. Если выбран этот вариант действия, то Kaspersky Endpoint Security откроет сайт с базой угроз и уязвимостей от "Лаборатории Касперского".

Для обработки активных угроз в консоли Kaspersky Security Center необходимо включить передачу данных о необработанных файлах на Сервер администрирования. По умолчанию передача данных включена.

Как включить передачу данных о необработанных угрозах в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Отчеты и хранилище**.
4. В блоке **Передача данных на Сервер администрирования** нажмите на кнопку **Настройка**.
5. Установите флажок **Необработанные файлы**.
6. Сохраните внесенные изменения.

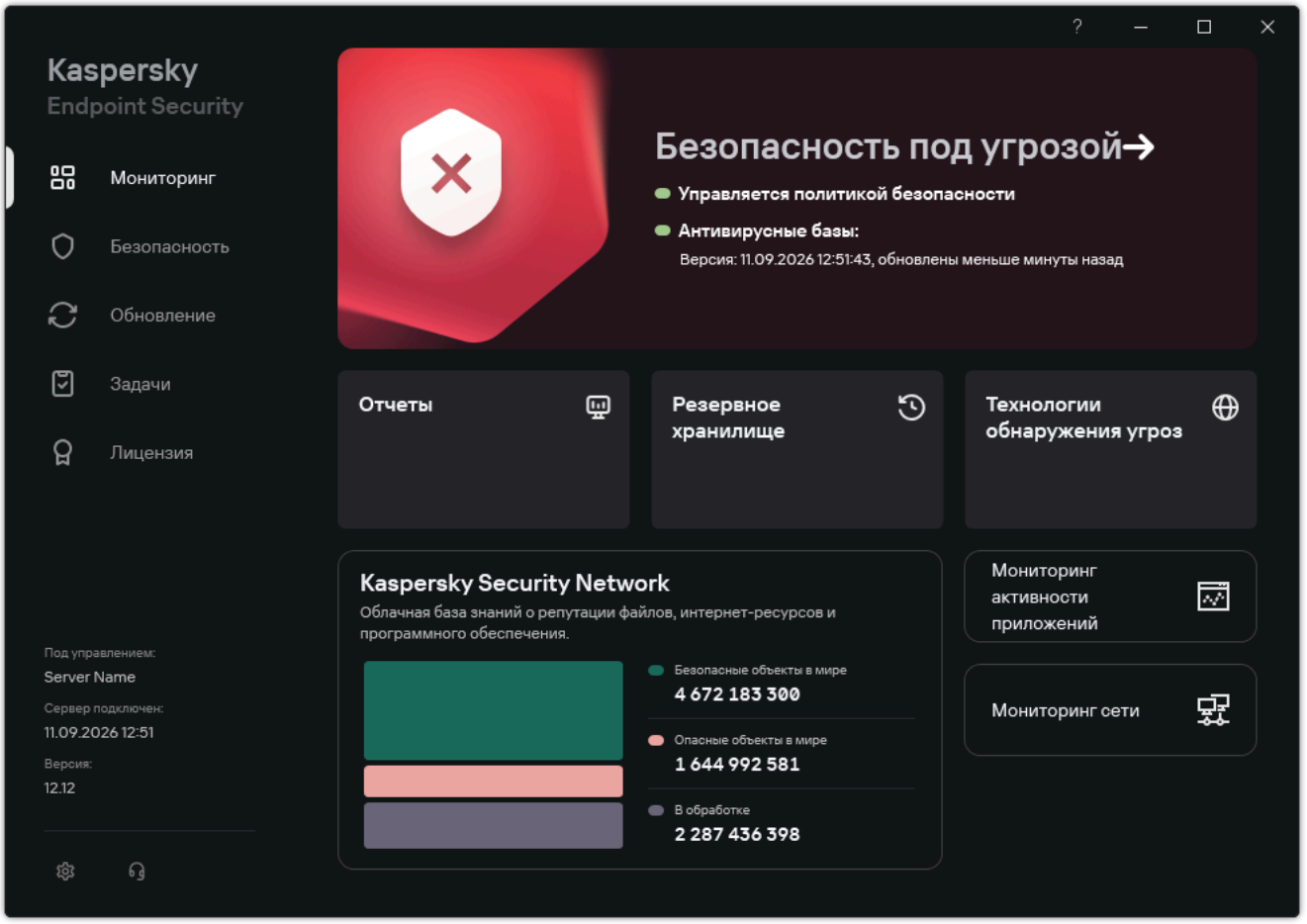
Как включить передачу данных о необработанных угрозах в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Интеграция с KSC**.

5. В блоке **Передача данных на Сервер администрирования** установите флажок **О необработанных файлах**.

6. Сохраните внесенные изменения.



Главное окно приложения при обнаружении угрозы

Защита компьютера

Статус постоянной защиты

Kaspersky Endpoint Security передает на Сервер администрирования Kaspersky Security Center параметр **Статус постоянной защиты**, значение которого зависит от текущего состояния компонентов защиты приложения на защищаемом компьютере (см. таблицу ниже).

Kaspersky Endpoint Security определяет статус постоянной защиты на основе состояния следующих компонентов приложения:

- Защита от файловых угроз;
- Защита от веб-угроз;
- Защита от почтовых угроз;
- AMSI-защита;
- Защита от атак BadUSB;
- Защита от сетевых угроз;
- Сетевой экран;
- Защита от эксплойтов;
- Анализ поведения;
- Откат вредоносных действий;
- Предотвращение вторжений.

Вы можете узнать статус постоянной защиты приложения в консоли Kaspersky Security Center.

Как узнать статус постоянной защиты в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Управляемые устройства**.

В списке устройств в графе **Статус постоянной защиты** отображается текущее значение статуса постоянной защиты. Если графа **Статус постоянной защиты** отсутствует, настройте параметры столбцов, нажав на ссылку **Добавить или удалить столбцы**.

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Управляемые устройства**.

В списке устройств в графе **Статус постоянной защиты** отображается текущее значение статуса постоянной защиты. Если графа **Статус постоянной защиты** отсутствует, настройте параметры столбцов, нажав на ссылку **Добавить или удалить столбцы**.

Как узнать статус постоянной защиты в Web Console

В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.

В списке устройств в графе **Статус постоянной защиты** отображается текущее значение статуса постоянной защиты. Если графа **Статус постоянной защиты** отсутствует, настройте параметры столбцов (⚙).

Возможные значения параметра Статус постоянной защиты

Значение	Описание
Нет данных	На Сервере администрирования отсутствует информация о статусе постоянной защиты для данного компьютера.
Не установлен	Ни один из компонентов не установлен.
Не поддерживается лицензией	Приложение не активировано или лицензия не допускает работу установленных компонентов.
Сбой	В работе одного или нескольких компонентов произошел сбой.
Остановлен	Один или несколько компонентов выключены.
Приостановлена	Работа одного или нескольких компонентов приостановлена.
Запускается	Выполняется включение одного или нескольких компонентов.
Выполняется	Компоненты приложения включены и работают.

Если в Kaspersky Security Center значение параметра **Статус постоянной защиты** отлично от *Выполняется*, проверьте, что установленные компоненты Kaspersky Endpoint Security из списка включены и приложение активировано.

Защита от файловых угроз

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. По умолчанию компонент Защита от файловых угроз постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы в режиме реального времени. Компонент проверяет файлы на всех дисках компьютера, а также на подключенных дисках. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Компонент проверяет файлы, к которым обращается пользователь или приложение. При обнаружении вредоносного файла Kaspersky Endpoint Security блокирует операцию с файлом. Далее приложение лечит или удаляет вредоносный файл, в зависимости от настройки компонента Защита от файловых угроз.

При обращении к файлу, содержимое которого расположено в облачном хранилище OneDrive, Kaspersky Endpoint Security загружает и проверяет содержимое этого файла.

Включение и выключение Защиты от файловых угроз

По умолчанию компонент Защита от файловых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для работы Защиты от файловых угроз приложение Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского" (см. таблицу ниже). Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

Компонент Защита от файловых угроз использует данные, полученные от других компонентов приложения. Включение этих компонентов не является обязательным. К компонентам, которые предоставляют дополнительные данные, относятся следующие компоненты:

- Kaspersky Security Network.
- Предотвращение вторжений.
- Анализ поведения.

Как включить или выключить компонент Защита от файловых угроз в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита → Защита от файловых угроз**.
4. Используйте флажок **Защита от файловых угроз**, чтобы включить или выключить компонент.
5. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:
     - **Высокий**. Уровень безопасности файлов, при котором компонент Защита от файловых угроз максимально контролирует все открываемые, сохраняемые и запускаемые файлы. Компонент Защита от файловых угроз проверяет все типы файлов на всех жестких, сменных и сетевых дисках компьютера, а также архивы, установочные пакеты и вложенные OLE-объекты.
     - **Рекомендуемый**. Уровень безопасности файлов, который рекомендован для использования специалистами "Лаборатории Касперского". Компонент Защита от файловых угроз проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты, компонент Защита от файловых угроз не проверяет архивы и установочные пакеты.
     - **Низкий**. Уровень безопасности файлов, параметры которого обеспечивают максимальную скорость проверки. Компонент Защита от файловых угроз проверяет только файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера, компонент Защита от файловых угроз не проверяет составные файлы.

- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка** и задайте параметры работы компонента (см. таблицу ниже).

  Вы можете восстановить значения предустановленных уровней безопасности по кнопке **По умолчанию**.

6. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами:

   - **Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.

   - **Лечить. Блокировать, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение блокирует этот файл.

   - **Блокировать**. Если выбран этот вариант действия, то приложение автоматически блокирует зараженный файл без попытки вылечить и удалить.

   Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить компонент Защита от файловых угроз в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз** → **Защита от файловых угроз**.

5. Используйте переключатель **Защита от файловых угроз ВКЛЮЧЕНА**, чтобы включить или выключить компонент.

6. Если вы хотите добавить новый объект в область защиты, выполните следующие действия:

   a. В блоке **Дополнительные настройки** выберите вкладку **Область защиты**.

   b. Нажмите на кнопку **Добавить**.

   c. В открывшемся окне выберите объекты, которые вы хотите добавить в область защиты.

Используйте маски:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Вы можете использовать маски в любом месте пути к файлу или папке. Например, если вы хотите включить в область проверки папку Загрузки для всех учетных записей пользователей компьютера, введите маску `C:\Users\*\Downloads\`.

Вы можете исключить объект из защиты, не удаляя его из списка объектов области защиты. Для этого выключите переключатель рядом с ним.

d. Сохраните внесенные изменения.

7. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами:

   - **Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.

   - **Лечить. Блокировать, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение блокирует этот файл.

   - **Блокировать**. Если выбран этот вариант действия, то приложение автоматически блокирует зараженный файл без попытки вылечить и удалить.

   Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.

8. Если требуется, настройте дополнительные параметры Защиты от файловых угроз.

9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить компонент Защита от файловых угроз в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.

3. Используйте переключатель **Защита от файловых угроз**, чтобы включить или выключить компонент.

4. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:

   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:

     - **Высокий**. Уровень безопасности файлов, при котором компонент Защита от файловых угроз максимально контролирует все открываемые, сохраняемые и запускаемые файлы. Компонент Защита от файловых угроз проверяет все типы файлов на всех жестких, сменных и сетевых дисках компьютера, а также архивы, установочные пакеты и вложенные OLE-объекты.

     - **Рекомендуемый**. Уровень безопасности файлов, который рекомендован для использования специалистами "Лаборатории Касперского". Компонент Защита от файловых угроз проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты, компонент Защита от файловых угроз не проверяет архивы и установочные пакеты.

     - **Низкий**. Уровень безопасности файлов, параметры которого обеспечивают максимальную скорость проверки. Компонент Защита от файловых угроз проверяет только файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера, компонент Защита от файловых угроз не проверяет составные файлы.

   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента (см. таблицу ниже).

     Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности**.

5. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами:

   - **Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.

   - **Лечить. Блокировать, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение блокирует этот файл.

   - **Блокировать**. Если выбран этот вариант действия, то приложение автоматически блокирует зараженный файл без попытки вылечить и удалить.

   Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.

6. Сохраните внесенные изменения.

Параметры Защиты от файловых угроз, рекомендованные специалистами "Лаборатории Касперского", (рекомендованный уровень безопасности)

Параметр	Значение	Описание
Типы файлов	**Файлы, проверяемые по формату**	Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.
Эвристический анализ	**Поверхностный**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Проверять только новые и измененные файлы	**Вкл**	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Использовать технологию iSwift	**Вкл**	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
Использовать технологию iChecker	**Вкл**	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Проверять файлы офисных форматов	**Вкл**	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Проверять файлы почтовых форматов	**Вкл**	Проверка файлов почтовых форматов. Приложение проверяет MSG- и EML-файлы. К файлам почтовых форматов также относятся OLE-объекты и MHT-файлы. Kaspersky Endpoint Security проверяет файлы почтовых форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Режим проверки	**Интеллектуальный**	Режим проверки, при котором Защита от файловых угроз проверяет объект на основании анализа операций, выполняемых над объектом. Например, при работе с документом Microsoft Office приложение Kaspersky Endpoint Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**	Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.

Автоматическая приостановка Защиты от файловых угроз

Вы можете настроить автоматическую приостановку Защиты от файловых угроз в указанное время или во время работы с определенными приложениями.

Приостановка работы Защиты от файловых угроз при конфликте с определенными приложениями является экстренной мерой. Если во время работы компонента возникают какие-либо конфликты, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского". Специалисты помогут вам наладить совместную работу компонента Защита от файловых угроз с другими приложениями на вашем компьютере.

Чтобы настроить автоматическую приостановку работы Защиты от файловых угроз, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Приостановка Защиты от файловых угроз** перейдите по ссылке **Приостановить Защиту от файловых угроз**.
5. В открывшемся окне настройте параметры приостановки работы Защиты от файловых угроз:
   a. Настройте расписание автоматической приостановки Защиты от файловых угроз.
   b. Сформируйте список приложений, во время работы которых Защиту от файловых угроз следует приостанавливать.
6. Сохраните внесенные изменения.

Изменение действия компонента Защита от файловых угроз над зараженными файлами

По умолчанию компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз удаляет эти файлы.

Чтобы изменить действие компонента Защита от файловых угроз над зараженными файлами, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:
   - **Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.
   - **Лечить. Блокировать, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение блокирует этот файл.
   - **Блокировать**. Если выбран этот вариант действия, то приложение автоматически блокирует зараженный файл без попытки вылечить и удалить.

Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.

4. Сохраните внесенные изменения.

Формирование области защиты компонента Защита от файловых угроз

Под областью защиты подразумеваются объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты компонента Защита от файловых угроз являются местоположение и тип проверяемых файлов. По умолчанию компонент Защита от файловых угроз проверяет только потенциально заражаемые файлы, запускаемые со всех жестких, съемных и сетевых дисков компьютера.

Выбирая тип проверяемых файлов, нужно учитывать следующее:

1. Вероятность внедрения вредоносного кода в файлы некоторых форматов и его последующей активации низка (например, формат TXT). В то же время существуют форматы файлов, которые содержат исполняемый код (например, форматы EXE, DLL). Также исполняемый код могут содержать форматы файлов, которые для этого не предназначены (например, формат DOC). Риск внедрения в такие файлы вредоносного кода и его активации высок.

2. Злоумышленник может отправить вирус или другое приложение, представляющее угрозу, на ваш компьютер в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки приложение пропускает такой файл. Если же выбрана проверка файлов по формату, то вне зависимости от расширения Kaspersky Endpoint Security анализирует заголовок файла. Если в результате выясняется, что файл имеет формат исполняемого файла (например, EXE), то приложение проверяет его.

Чтобы сформировать область защиты, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять компонентом Защита от файловых угроз:

   - **Все файлы**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений).

   - **Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.

   - **Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.

5. Перейдите по ссылке **Изменить область защиты**.

6. В открывшемся окне выберите объекты, которые вы хотите добавить в область защиты или исключить из нее.

   Вы не можете удалить или изменить объекты, включенные в область защиты по умолчанию.

7. Если вы хотите добавить новый объект в область защиты, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

      Откроется дерево папок.

   b. В поле **Путь** введите путь к папке или файлу.

      Используйте маски:

      - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

      - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

      - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

      Вы можете использовать маски в любом месте пути к файлу или папке. Например, если вы хотите включить в область проверки папку Загрузки для всех учетных записей пользователей компьютера, введите маску `C:\Users\*\Downloads\`.

      Объект **Этот компьютер** в списке файловых ресурсов компьютера включает в себя следующие объекты: **Все жесткие диски**, **Все сетевые диски** и **Все съемные диски**.

   Вы можете исключить объект из проверки, не удаляя его из списка объектов области проверки. Для этого снимите флажок рядом с ним.

8. Сохраните внесенные изменения.

Использование методов проверки

Во время своей работы Kaspersky Endpoint Security использует метод проверки Машинное обучение и сигнатурный анализ. В процессе сигнатурного анализа Kaspersky Endpoint Security сравнивает найденный объект с записями в базах приложения. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

Чтобы настроить использование эвристического анализа в работе компонента Защита от файловых угроз, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Методы проверки** установите флажок **Эвристический анализ**, если вы хотите, чтобы приложение использовало эвристический анализ для защиты от файловых угроз. Далее при помощи ползунка задайте уровень эвристического анализа: **Поверхностный**, **Средний** или **Глубокий**.
5. Сохраните внесенные изменения.

Использование технологий проверки в работе компонента Защита от файловых угроз

Чтобы настроить использование технологий проверки в работе компонента Защита от файловых угроз, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Технологии проверки** установите флажки около названий технологий, которые вы хотите использовать для защиты от файловых угроз:
   - **Использовать технологию iSwift**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
   - **Использовать технологию iChecker**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
5. Сохраните внесенные изменения.

Оптимизация проверки файлов

Вы можете оптимизировать проверку файлов компонентом Защита от файловых угроз: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

Вы также можете включить использование технологий iChecker и iSwift, которые позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

Чтобы оптимизировать проверку файлов, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Оптимизация** установите флажок **Проверять только новые и измененные файлы**.
5. Сохраните внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других приложений, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие приложения, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить типы проверяемых составных файлов, таким образом увеличив скорость проверки.

Способ обработки зараженного составного файла (лечение или удаление) зависит от типа файла.

Компонент Защита от файловых угроз лечит составные файлы форматов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и удаляет файлы всех остальных форматов (кроме почтовых баз).

Чтобы настроить проверку составных файлов, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты, файлы почтовых или офисных форматов.

5. Если режим проверки только новых и измененных файлов выключен, настройте параметры проверки каждого типа составных файлов: проверка всех файлов этого типа или только новых файлов.

   Если режим проверки только новых и измененных файлов включен, Kaspersky Endpoint Security проверяет только новые и измененные файлы всех типов составных файлов.

6. Настройте дополнительные параметры проверки составных файлов:

   - **Не распаковывать составные файлы большого размера**.

     Если флажок установлен, то Kaspersky Endpoint Security не проверяет составные файлы, размеры которых больше заданного значения.

     Если флажок снят, Kaspersky Endpoint Security проверяет составные файлы любого размера.

     > Kaspersky Endpoint Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

   - **Распаковывать составные файлы в фоновом режиме**.

     Если флажок установлен, Kaspersky Endpoint Security предоставляет доступ к составным файлам, размер которых превышает заданное значение, до проверки этих файлов. При этом Kaspersky Endpoint Security в фоновом режиме распаковывает и проверяет составные файлы.

     Kaspersky Endpoint Security предоставляет доступ к составным файлам, размер которых меньше данного значения, только после распаковки и проверки этих файлов.

     Если флажок снят, Kaspersky Endpoint Security предоставляет доступ к составным файлам только после распаковки и проверки файлов любого размера.

7. Сохраните внесенные изменения.

Изменение режима проверки файлов

Под *режимом проверки* подразумевается условие, при котором компонент Защита от файловых угроз начинает проверять файлы. По умолчанию Kaspersky Endpoint Security использует интеллектуальный режим проверки файлов. Работая в этом режиме проверки файлов, компонент Защита от файловых угроз принимает решение о проверке файлов на основании анализа операций, которые пользователь, приложение от имени пользователя (под учетными данными которого был осуществлен вход в операционную систему или другого пользователя) или операционная система выполняет над файлами. Например, работая с документом Microsoft Office Word, Kaspersky Endpoint Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

Чтобы изменить режим проверки файлов, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Режим проверки** выберите нужный режим:

   - **Интеллектуальный**. Режим проверки, при котором Защита от файловых угроз проверяет объект на основании анализа операций, выполняемых над объектом. Например, при работе с документом Microsoft Office приложение Kaspersky Endpoint Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

   - **При доступе и изменении**. Режим проверки, при котором Защита от файловых угроз проверяет объекты при попытке их открыть или изменить.

   - **При доступе**. Режим проверки, при котором Защита от файловых угроз проверяет объекты только при попытке их открыть.

   - **При выполнении**. Режим проверки, при котором Защита от файловых угроз проверяет объекты только при попытке их запустить.

5. Сохраните внесенные изменения.

Проверка контейнеров

Контейнер – это изолированная среда, где приложение может работать без прямого взаимодействия с операционной системой. Использование контейнеров включает в себя следующие риски:

- Уязвимости в процессе контейнеризации могут быть использованы злоумышленниками для компрометации приложений внутри контейнера.
- Небезопасная конфигурация контейнерной среды может быть использована злоумышленниками для получения несанкционированного доступа к данным компьютера или нарушения целостности системы.
- Взлом контейнера может позволить злоумышленнику получить доступ к данным компьютера.
- Сетевые уязвимости могут быть использованы злоумышленниками для перехвата сетевого трафика.

Kaspersky Endpoint Security проверяет файлы не только на дисках, то и внутри контейнеров. То есть Kaspersky Endpoint Security является внешним инструментом для обнаружения вредоносной активности внутри контейнеров. Это позволяет сохранить производительность контейнеров и избежать конфликтов с другими приложениями внутри контейнера. Установка приложения Kaspersky Endpoint Security внутрь контейнера не поддерживается.

Кроме обеспечения безопасности контейнеров, Kaspersky Endpoint Security позволяет управлять работой приложений внутри контейнеров с помощью Контроля приложений. Настройка Контроля приложения для контейнеров не отличается от настройки компонента для приложений, установленных на компьютере. Контроль целостности системы также поддерживает контейнеры.

Требования к контейнерам

- Контейнер создан на платформе Docker. Другие средства контейнеризации не поддерживаются.
- Контейнер запущен в режиме изоляции процессов. Режим изоляции Hyper-V не поддерживается.

- Контейнер расположен на сервере под управлением Windows Server 2016, 2019 или 2022 (Docker Host).
- Контейнер включает в себя образ Windows (Docker Image). ОС Windows 10 и 11 не поддерживаются. Образы Linux не поддерживаются.

Действие при обнаружении угрозы

При обнаружении угрозы внутри контейнера, приложение применяет действие, выбранное для компонента Защита от файловых угроз. Также проверка контейнеров имеет дополнительные параметры (см. инструкцию ниже). При обнаружении угрозы, приложение блокирует вредоносную активность и выполняет выбранное действие (например, пытается вылечить объект). Kaspersky Endpoint Security может остановить контейнер, если вылечить обнаруженный объект не удалось. По умолчанию функция остановки контейнеров выключена.

Как настроить проверку контейнеров в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита → Защита от файловых угроз**.
4. Нажмите на кнопку **Настройка**.
5. В открывшемся окне выберите вкладку **Дополнительно**.
6. В блоке **Проверка файловых операций, исполняемых в контейнерах Windows** настройте параметры проверки контейнеров:
   - **Останавливать контейнер, если лечение невозможно**. У приложения может не быть прав на чтение и запись обнаруженного объекта. В этом случае вылечить или удалить обнаруженный объект невозможно. Если флажок установлен, приложение блокирует обнаруженный объект и останавливает контейнер. Если флажок снят, приложение только блокирует обнаруженный объект.
   - **Не проверять файловые операции, исполняемые в контейнерах Windows**. Если флажок установлен, приложение проверяет контейнер только при запуске контейнера. Если флажок снят, приложение проверяет контейнер постоянно в режиме реального времени.
7. Сохраните внесенные изменения.

Как настроить проверку контейнеров в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз → Защита от файловых угроз**.
5. В блоке **Дополнительные настройки** выберите вкладку **Производительность**.

6. В блоке **Оптимизация проверки** настройте параметры проверки контейнеров:

   - **Остановить контейнер, если не удалось вылечить**. У приложения может не быть прав на чтение и запись обнаруженного объекта. В этом случае вылечить или удалить обнаруженный объект невозможно. Если флажок установлен, приложение блокирует обнаруженный объект и останавливает контейнер. Если флажок снят, приложение только блокирует обнаруженный объект.

   - **Не проверять файловые операции, исполняемые в контейнерах Windows**. Если флажок установлен, приложение проверяет контейнер только при запуске контейнера. Если флажок снят, приложение проверяет контейнер постоянно в режиме реального времени.

7. Сохраните внесенные изменения.

Как настроить проверку контейнеров в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от файловых угроз**.

3. В блоке **Проверка файловых операций, исполняемых в контейнерах Windows** настройте параметры проверки контейнеров:

   - **Останавливать контейнер, если лечение невозможно**. У приложения может не быть прав на чтение и запись обнаруженного объекта. В этом случае вылечить или удалить обнаруженный объект невозможно. Если флажок установлен, приложение блокирует обнаруженный объект и останавливает контейнер. Если флажок снят, приложение только блокирует обнаруженный объект.

   - **Не проверять файловые операции, исполняемые в контейнерах Windows**. Если флажок установлен, приложение проверяет контейнер только при запуске контейнера. Если флажок снят, приложение проверяет контейнер постоянно в режиме реального времени.

4. Сохраните внесенные изменения.

Предотвращение вторжений

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов.

Компонент Предотвращение вторжений (англ. Host Intrusion Prevention System, HIPS) предотвращает выполнение приложениями опасных для системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и персональным данным. Компонент обеспечивает защиту компьютера с помощью антивирусных баз и облачной службы Kaspersky Security Network.

Компонент контролирует работу приложений с помощью *прав приложений*. Права приложений включают в себя следующие параметры доступа:

- доступ к ресурсам операционной системы (например, параметры автозапуска, ключи реестра);
- доступ к персональным данным (например, к файлам, приложениям).

Сетевую активность приложений контролирует Сетевой экран с помощью *сетевых правил*.

Во время первого запуска приложения компонент Предотвращение вторжений выполняет следующие действия:

1. Проверяет безопасность приложения с помощью загруженных антивирусных баз.
2. Проверяет безопасность приложения в Kaspersky Security Network.

   Для более эффективной работы компонента Предотвращение вторжений вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает приложение в одну из групп доверия: *Доверенные*, *Слабые ограничения*, *Сильные ограничения*, *Недоверенные*.

   Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля активности приложений. Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от уровня опасности, которую это приложение может представлять для компьютера.

   Kaspersky Endpoint Security помещает приложение в группу доверия для компонентов Сетевой экран и Предотвращение вторжений. Изменить группу доверия только для Сетевого экрана или только для Предотвращения вторжений невозможно.

   Если вы отказались принимать участие в KSN или отсутствует сеть, Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации приложения от KSN группа доверия может быть изменена автоматически.

4. Блокирует действия приложения в зависимости от группы доверия. Например, приложениям из группы доверия *Сильные ограничения* запрещен доступ к модулям операционной системы.

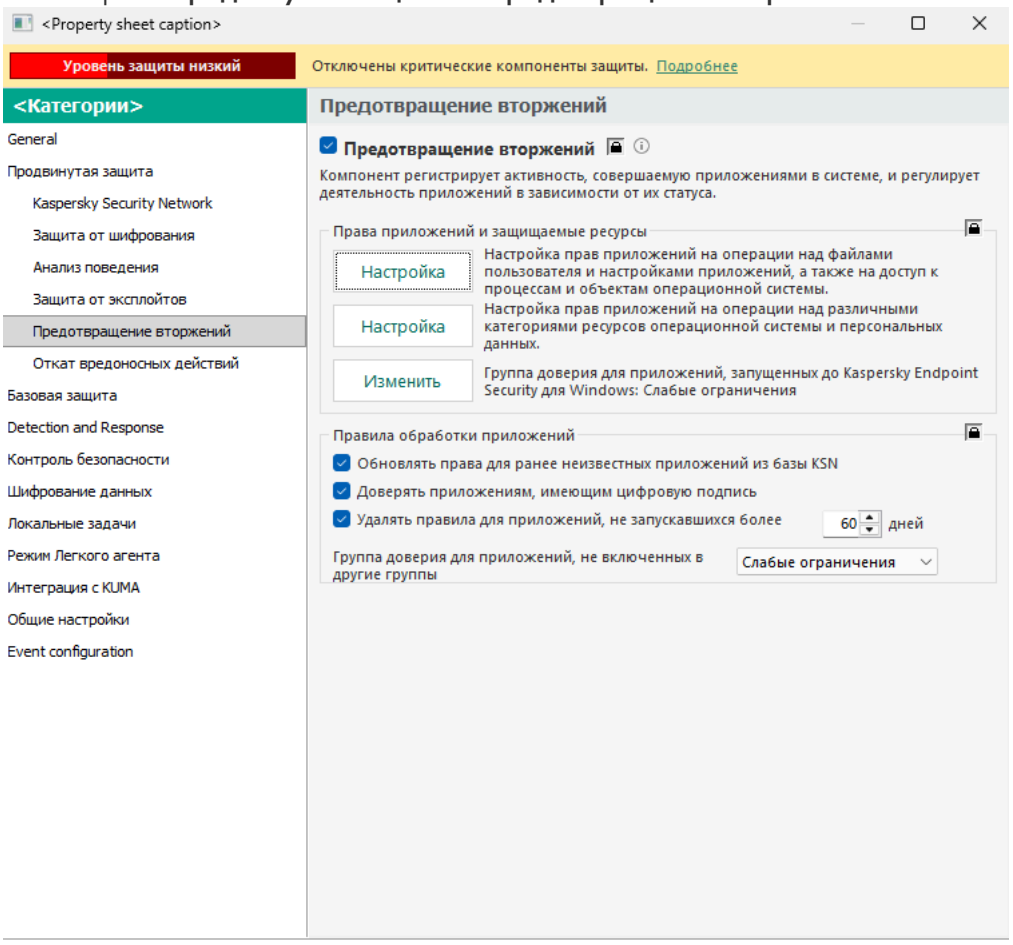
При следующем запуске приложения Kaspersky Endpoint Security проверяет целостность приложения. Если приложение не было изменено, компонент применяет к ней текущие права приложения. Если приложение было изменено, Kaspersky Endpoint Security исследует приложение как при первом запуске.

Включение и выключение Предотвращения вторжений

По умолчанию компонент Предотвращение вторжений включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме.

Как включить или выключить компонент Предотвращение вторжений в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.



Параметры Предотвращения вторжений

4. Используйте флажок **Предотвращение вторжений**, чтобы включить или выключить компонент.
5. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить компонент Предотвращение вторжений в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз → Предотвращение вторжений**.
5. Используйте переключатель **Предотвращение вторжений ВКЛЮЧЕНО**, чтобы включить или выключить компонент.
6. Сохраните внесенные изменения.

Как включить или выключить компонент Предотвращение вторжений в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. Используйте переключатель **Предотвращение вторжений**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если компонент Предотвращение вторжений включен, Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от уровня опасности, которую это приложение может представлять для компьютера. Далее Kaspersky Endpoint Security будет блокировать действия приложения в зависимости от группы доверия.

Работа с группами доверия приложений

Во время первого запуска каждого приложения компонент Предотвращение вторжений проверяет безопасность приложения и помещает приложение в одну из групп доверия.

На первом этапе проверки приложения Kaspersky Endpoint Security ищет запись о приложении во внутренней базе известных приложений и одновременно отправляет запрос в базу Kaspersky Security Network (при наличии подключения к интернету). По результатам проверки по внутренней базе и по базе Kaspersky Security Network приложение помещается в группу доверия. При каждом повторном запуске приложения Kaspersky Endpoint Security отправляет новый запрос в базу KSN и перемещает приложение в другую группу доверия, если репутация приложения в базе KSN изменилась.

Вы можете выбрать группу доверия, в которую Kaspersky Endpoint Security должен автоматически помещать все неизвестные приложения. Приложения, которые были запущены до Kaspersky Endpoint Security, автоматически помещаются в группу доверия, установленную в параметрах компонента Предотвращение вторжений.

Для приложений, запущенных до Kaspersky Endpoint Security, контролируется только сетевая активность. Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана.

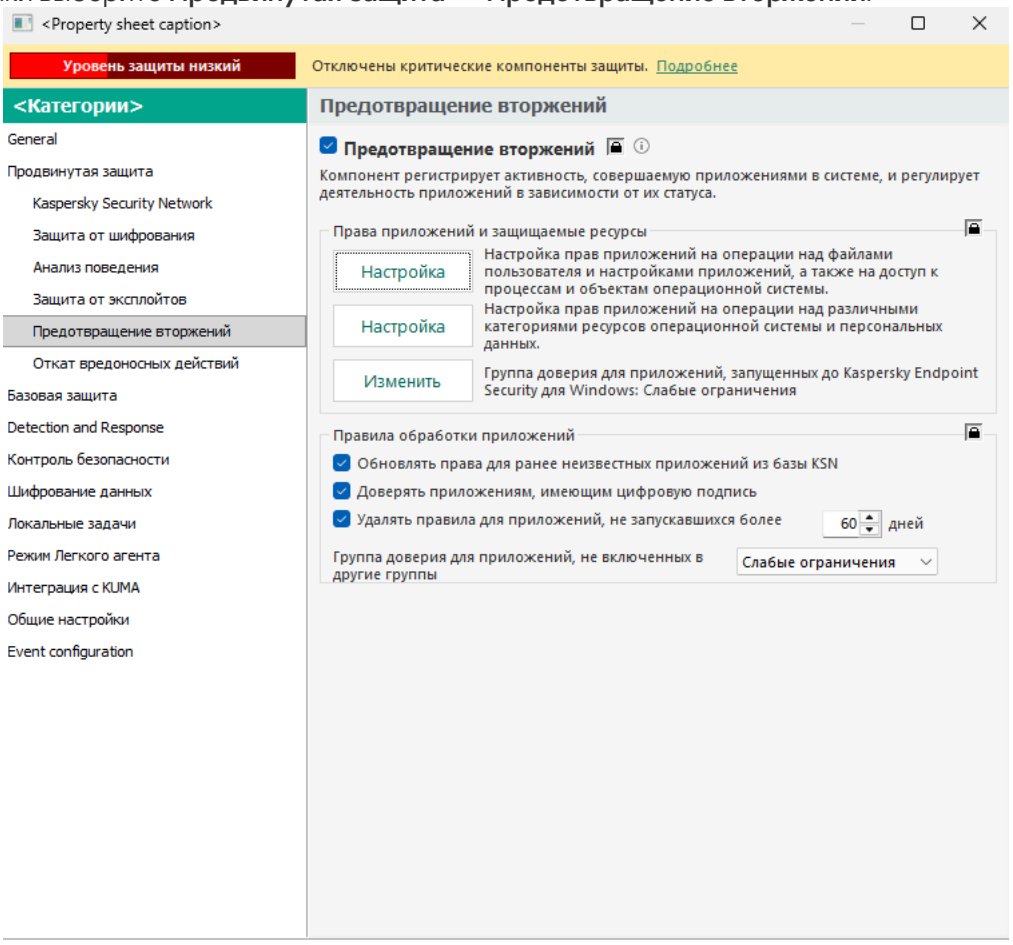
Изменение группы доверия для приложения

Во время первого запуска каждого приложения компонент Предотвращение вторжений проверяет безопасность приложения и помещает приложение в одну из групп доверия.

Специалисты "Лаборатории Касперского" не рекомендуют перемещать приложения из группы доверия, определенной автоматически, в другую группу доверия. Вместо этого при необходимости измените права отдельного приложения.

Как изменить группу доверия для приложения в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.



Параметры Предотвращения вторжений

4. В блоке **Права приложений и защищаемые ресурсы** нажмите на кнопку **Настройка**.

   Откроется окно настройки прав приложений и список защищаемых ресурсов.

5. Выберите вкладку **Права приложений**.
6. Нажмите на кнопку **Добавить**.
7. В открывшемся окне задайте параметры поиска приложения, для которой вы хотите изменить группу доверия.

   Вы можете ввести название приложения или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

8. Нажмите на кнопку **Обновить**.

   Kaspersky Endpoint Security выполнит поиск приложения в консолидированном списке приложений, установленных на управляемых компьютерах. Kaspersky Endpoint Security покажет список приложений, которые удовлетворяют параметрам поиска.

9. Выберите нужное приложение.

10. В раскрывающемся списке **Переместить приложение в группу доверия** выберите нужную группу доверия для приложения.

11. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как изменить группу доверия для приложения в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз** → **Предотвращение вторжений**.

5. В блоке **Права приложений и защищаемые ресурсы** нажмите на ссылку **Права приложений и защищаемые ресурсы**.

   Откроется окно настройки прав приложения и список защищаемых ресурсов.

6. Выберите вкладку **Права приложений**.

   Откроется список групп доверия в левой части окна и их свойства в правой части.

7. Нажмите на кнопку **Добавить**.

   Запустится мастер добавления приложения в группу доверия.

8. Выберите группу доверия, в которую вы хотите поместить приложение.

9. Выберите тип **Приложение**. Перейдите к следующему шагу.

   Если вы хотите изменить группу доверия для нескольких приложений, выберите тип **Группа** и задайте имя группы приложений.

10. В открывшемся списке приложений выберите приложения, для которых вы хотите изменить группу доверия.

    Используйте фильтр. Вы можете ввести название приложения или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

11. Завершите работу мастера.

    Приложение будет добавлено в группу доверия.

12. Сохраните внесенные изменения.

Как изменить группу доверия для приложения в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.

3. Нажмите на кнопку **Управление приложениями**.

   Откроется список установленных приложений.

4. Выберите нужное приложение.

5. В контекстном меню приложения выберите пункт **Ограничения → <группа доверия>**.

6. Сохраните внесенные изменения.

В результате приложение будет перемещено в другую группу доверия. Далее Kaspersky Endpoint Security будет блокировать действия приложения в зависимости от группы доверия. Приложению будет присвоен статус *(задано пользователем)*. При изменении репутации приложения в Kaspersky Security Network компонент Предотвращение вторжений оставит группу доверия для этого приложения без изменений.

Настройка прав группы доверия

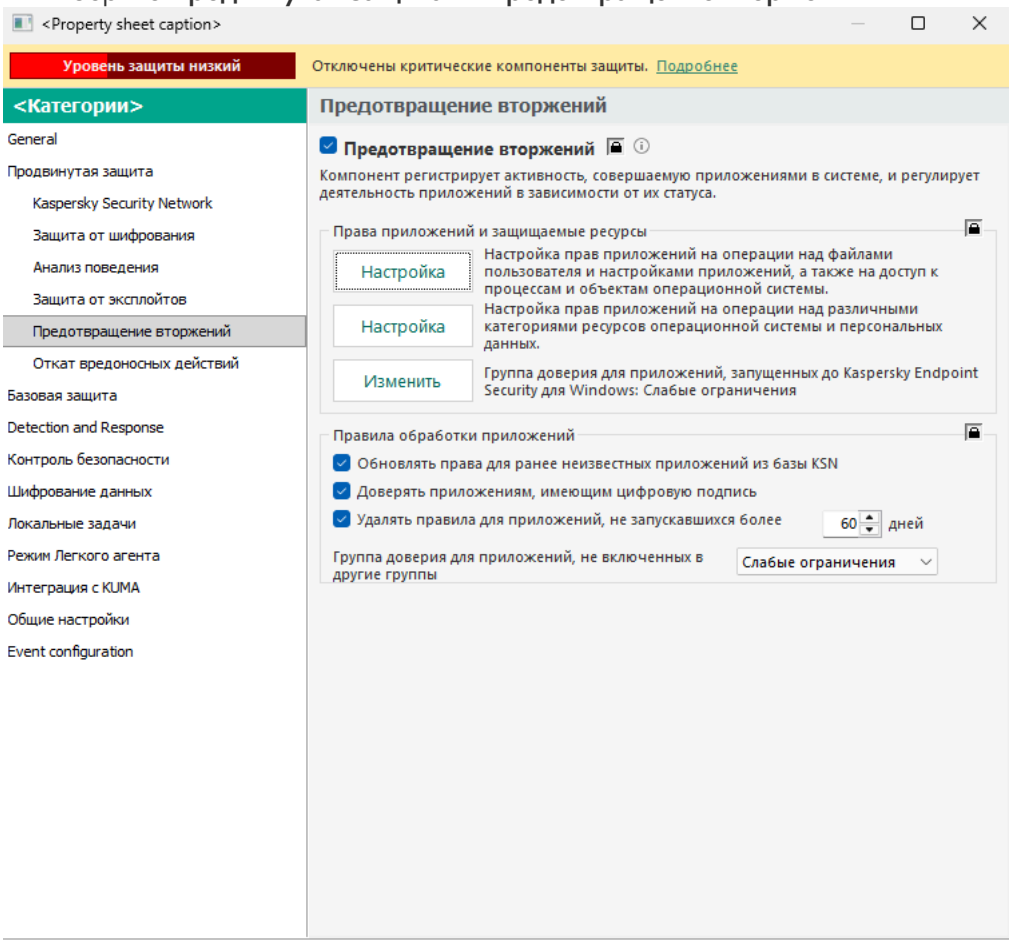
По умолчанию для разных групп доверия созданы оптимальные права приложений. Параметры прав групп приложений, входящих в группу доверия, наследуют значения параметров прав групп доверия.

Как изменить права группы доверия в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.



Параметры Предотвращения вторжений

4. В блоке **Права приложений и защищаемые ресурсы** нажмите на кнопку **Настройка**.

   Откроется окно настройки прав приложений и список защищаемых ресурсов.

5. Перейдите на вкладку **Права приложений**.

6. Выберите нужную группу доверия.
7. В контекстном меню группы доверия выберите пункт **Права группы**.

   Откроются свойства группы доверия.
8. Выполните одно из следующих действий:

   - Выберите вкладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами приложений.
   - Выберите вкладку **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

   Сетевую активность приложений контролирует Сетевой экран с помощью *сетевых правил*.
9. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт: **Наследовать**, **Разрешать** (✓) или **Запрещать** (⊘).
10. Если вы хотите контролировать использование ресурсов компьютера, выберите пункт **Записывать в отчет** (✓ / ⊘).

    Kaspersky Endpoint Security будет записывать информацию о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении приложением операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о приложениях, которые используют каждый ресурс.
11. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как изменить права группы доверия в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Предотвращение вторжений**.
5. В блоке **Права приложений и защищаемые ресурсы** нажмите на ссылку **Права приложений и защищаемые ресурсы**.

   Откроется окно настройки прав приложений и список защищаемых ресурсов.
6. Перейдите на вкладку **Права приложений**.

   Откроется список групп доверия в левой части окна и их свойства в правой части.
7. В левой части окна выберите нужную группу доверия.

8. В правой части окна в раскрывающемся списке выполните одно из следующих действий:

   - Выберите пункт **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами приложения.

   - Выберите пункт **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

   Сетевую активность приложений контролирует Сетевой экран с помощью *сетевых правил*.

9. Для нужного ресурса в графе соответствующего действия выберите нужный пункт: **Наследовать**, **Разрешить** (), **Блокировать** ().

10. Если вы хотите контролировать использование ресурсов компьютера, выберите пункт **Записывать в отчет** (/).

    Kaspersky Endpoint Security будет записывать информацию о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении приложением операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о приложениях, которые используют каждый ресурс.

11. Сохраните внесенные изменения.

Как изменить права группы доверия в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.

3. Нажмите на кнопку **Управление приложениями**.

   Откроется список установленных приложений.

4. Выберите нужную группу доверия.

5. В контекстном меню группы доверия выберите пункт **Подробности и правила**.

   Откроются свойства группы доверия.

6. Выполните одно из следующих действий:

   - Выберите вкладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами приложений.

   - Выберите вкладку **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

   Сетевую активность приложений контролирует Сетевой экран с помощью *сетевых правил*.

7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт: **Наследовать**, **Разрешить** (), **Запретить** ().

8. Если вы хотите контролировать использование ресурсов компьютера, выберите пункт **Записывать в отчет** ( ).

   Kaspersky Endpoint Security будет записывать информацию о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении приложением операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о приложениях, которые используют каждый ресурс.

9. Сохраните внесенные изменения.

В результате права группы доверия будут изменены. Далее Kaspersky Endpoint Security будет блокировать действия приложения в зависимости от группы доверия. Группе доверия будет присвоен статус (*Настройки пользователя*).

Выбор группы доверия для приложений, запускаемых до Kaspersky Endpoint Security

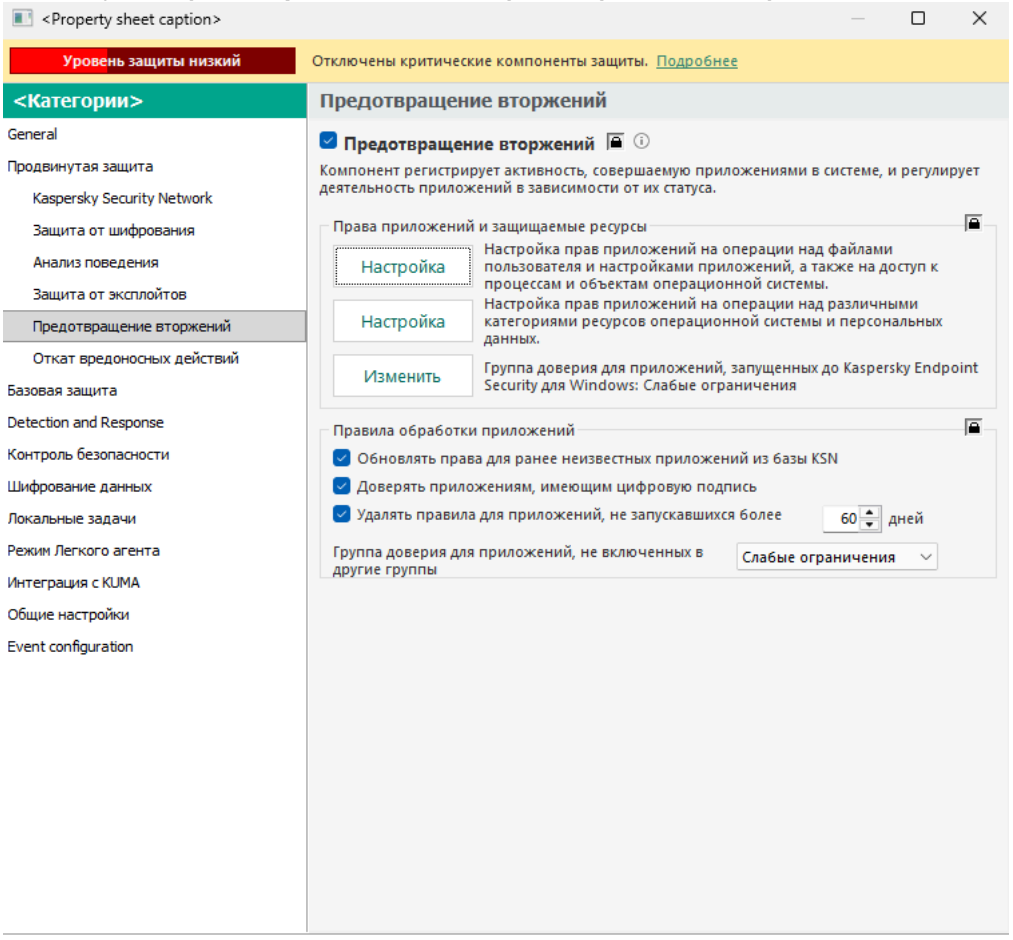
Для приложений, запущенных до Kaspersky Endpoint Security, контролируется только сетевая активность. Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана. Чтобы указать, какими сетевыми правилами должен регулироваться контроль сетевой активности таких приложений, необходимо выбрать группу доверия.

Как выбрать группу доверия для приложений, запускаемых до Kaspersky Endpoint Security, в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.



Параметры Предотвращения вторжений

4. В блоке **Права приложений и защищаемые ресурсы** нажмите на кнопку **Изменить**.

5. Для параметра **Группа доверия для приложений, запущенных до Kaspersky Endpoint Security** выберите нужную группу доверия.

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как выбрать группу доверия для приложений, запускаемых до Kaspersky Endpoint Security, в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз → Предотвращение вторжений**.

5. Для параметра **Группа доверия для приложений, запущенных до Kaspersky Endpoint Security** выберите нужную группу доверия.

6. Сохраните внесенные изменения.

Как выбрать группу доверия для приложений, запускаемых до Kaspersky Endpoint Security, в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. В блоке **Группа доверия для приложений, запущенных до Kaspersky Endpoint Security для Windows** выберите нужную группу доверия.
4. Сохраните внесенные изменения.

В результате приложение, запускаемое до Kaspersky Endpoint Security, будет помещено в другую группу доверия. Далее Kaspersky Endpoint Security будет блокировать действия приложения в зависимости от группы доверия.

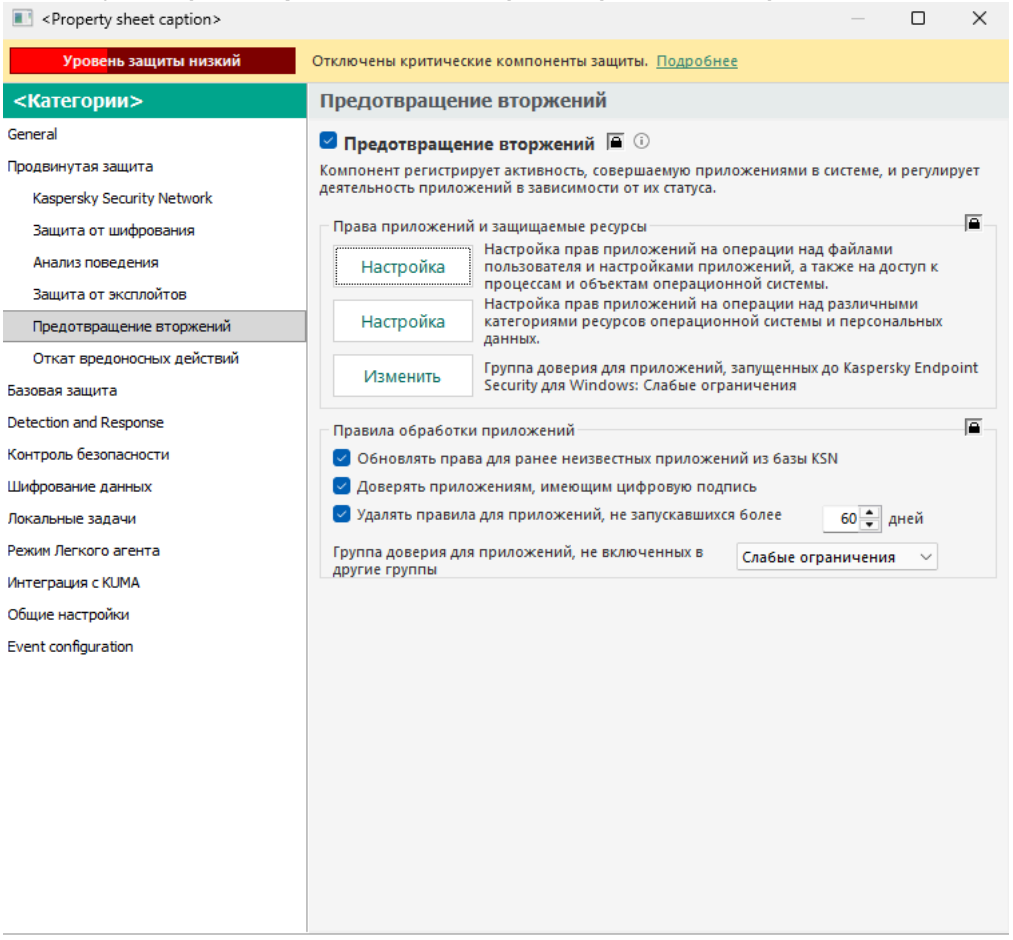
Выбор группы доверия для неизвестных приложений

Во время первого запуска приложения компонент Предотвращение вторжений определяет группу доверия для приложения. Если у вас отсутствует доступ в интернет или в Kaspersky Security Network нет информации об этом приложении, то Kaspersky Endpoint Security по умолчанию помещает приложение в группу *Слабые ограничения*. При обнаружении в KSN информации о ранее неизвестном приложении Kaspersky Endpoint Security обновит права приложения. После этого вы можете изменить права приложения вручную.

Как выбрать группу доверия для неизвестных приложений в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.



Параметры Предотвращения вторжений

4. В блоке **Правила обработки приложений** с помощью раскрывающегося списка **Группа доверия для приложений, не включенных в другие группы** выберите нужную группу доверия.

   Если участие в Kaspersky Security Network включено, Kaspersky Endpoint Security отправляет запрос о репутации приложения в KSN при каждом запуске приложения. На основе полученного ответа приложение может быть перемещено в группу доверия, отличную от заданной в параметрах компонента Предотвращение вторжений.

5. Используйте флажок **Обновлять права для ранее неизвестных приложений из базы KSN**, чтобы настроить автоматическое обновление прав неизвестных приложений.

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как выбрать группу доверия для неизвестных приложений в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз → Предотвращение вторжений**.

5. В блоке **Правила обработки приложений** с помощью раскрывающегося списка **Группа доверия для приложений, не включенных в другие группы** выберите нужную группу доверия.

   Если участие в Kaspersky Security Network включено, Kaspersky Endpoint Security отправляет запрос о репутации приложения в KSN при каждом запуске приложения. На основе полученного ответа приложение может быть перемещено в группу доверия, отличную от заданной в параметрах компонента Предотвращение вторжений.

6. Используйте флажок **Обновлять права для ранее неизвестных приложений из базы KSN**, чтобы настроить автоматическое обновление прав неизвестных приложений.

7. Сохраните внесенные изменения.

Как выбрать группу доверия для неизвестных приложений в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.

3. В блоке **Правила обработки приложений** выберите нужную группу доверия.

   Если участие в Kaspersky Security Network включено, Kaspersky Endpoint Security отправляет запрос о репутации приложения в KSN при каждом запуске приложения. На основе полученного ответа приложение может быть перемещено в группу доверия, отличную от заданной в параметрах компонента Предотвращение вторжений.

4. Используйте флажок **Обновлять правила для ранее неизвестных приложений из KSN**, чтобы настроить автоматическое обновление прав неизвестных приложений.

5. Сохраните внесенные изменения.

Выбор группы доверия для приложений с цифровой подписью

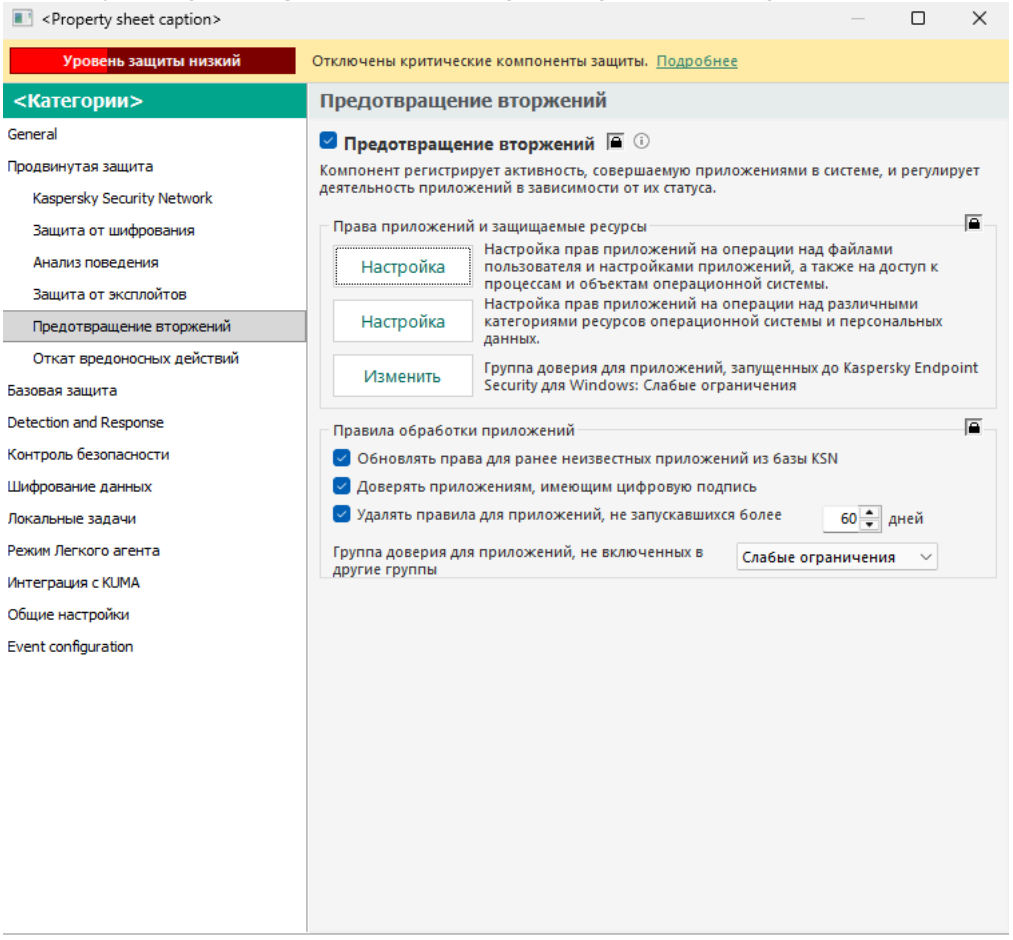
Kaspersky Endpoint Security всегда помещает приложения, подписанные сертификатами Microsoft или сертификатами "Лаборатории Касперского", в группу доверия *Доверенные*.

Как выбрать группу доверия для приложений с цифровой подписью в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.



Параметры Предотвращения вторжений

4. В блоке **Правила обработки приложений** используйте флажок **Доверять приложениям, имеющим цифровую подпись**, чтобы включить или выключить автоматическое перемещение приложений с цифровой подписью доверенных производителей в группу доверия *Доверенные*.

   Доверенные производители – производители, которые включены в список доверенных "Лабораторией Касперского". Также вы можете добавить сертификат производителя в доверенное системное хранилище сертификатов вручную.

   Если флажок снят, компонент Предотвращение вторжений не считает приложения с цифровой подписью доверенными и распределяет их по группам доверия на основании других параметров.

5. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как выбрать группу доверия для приложений с цифровой подписью в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз → Предотвращение вторжений**.

5. В блоке **Правила обработки приложений** используйте флажок **Доверять приложениям, имеющим цифровую подпись**, чтобы включить или выключить автоматическое перемещение приложений с цифровой подписью доверенных производителей в группу доверия *Доверенные*.

Доверенные производители – производители, которые включены в список доверенных "Лабораторией Касперского". Также вы можете добавить сертификат производителя в доверенное системное хранилище сертификатов вручную.

Если флажок снят, компонент Предотвращение вторжений не считает приложения с цифровой подписью доверенными и распределяет их по группам доверия на основании других параметров.

6. Сохраните внесенные изменения.

Как выбрать группу доверия для приложений с цифровой подписью в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.

3. В блоке **Правила обработки приложений** используйте флажок **Доверять приложениям, имеющим цифровую подпись**, чтобы включить или выключить автоматическое перемещение приложений с цифровой подписью доверенных производителей в группу доверия *Доверенные*.

   Доверенные производители – производители, которые включены в список доверенных "Лабораторией Касперского". Также вы можете добавить сертификат производителя в доверенное системное хранилище сертификатов вручную.

   Если флажок снят, компонент Предотвращение вторжений не считает приложения с цифровой подписью доверенными и распределяет их по группам доверия на основании других параметров.

4. Сохраните внесенные изменения.

Работа с правами приложений

По умолчанию для контроля работы приложения применяются права приложений, определенные для той группы доверия, в которую Kaspersky Endpoint Security поместил приложение при первом ее запуске. При необходимости вы можете изменить права приложений для всей группы доверия, для отдельного приложения или группы приложений внутри группы доверия.

Права приложений, заданные вручную, имеют более высокий приоритет, чем права приложений, определенные для группы доверия. То есть, если права приложения, заданные вручную, отличаются от прав приложений, определенных для группы доверия, компонент Предотвращение вторжения контролирует работу приложения в соответствии с правами приложений, заданными вручную.

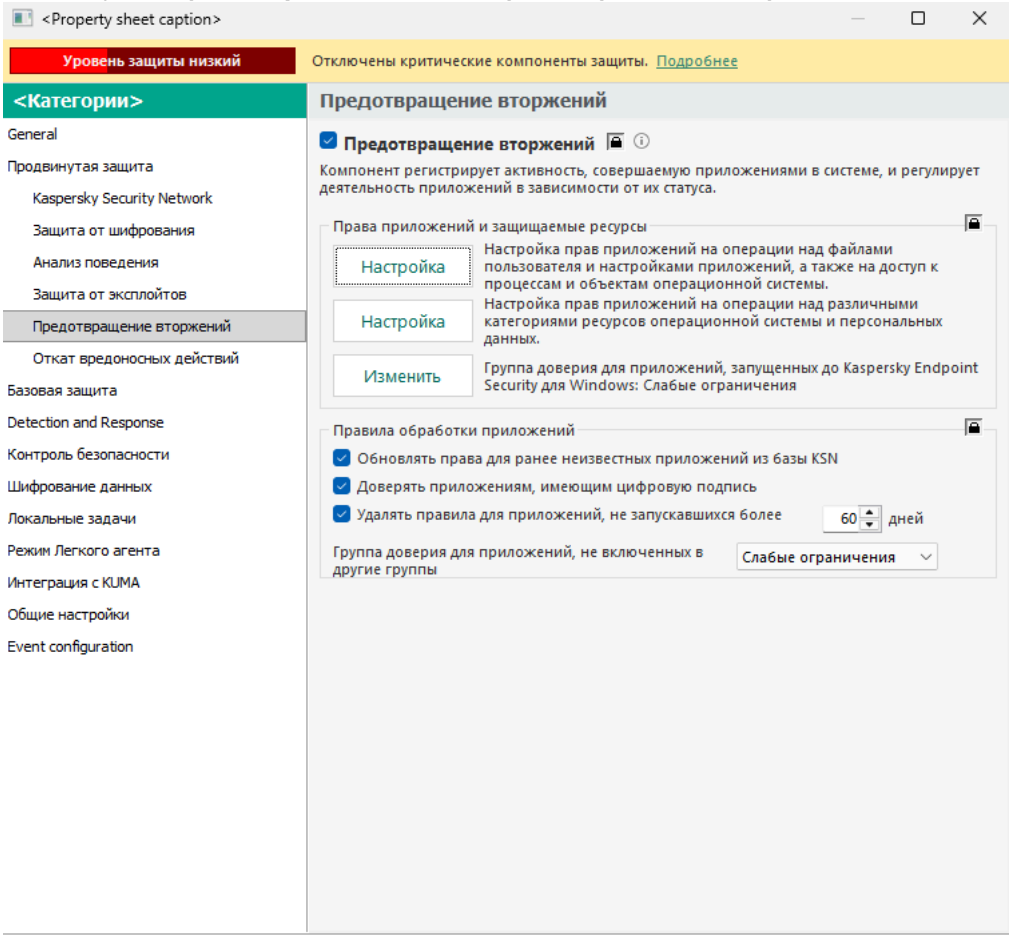
Правила, которые вы создаете для приложений, наследуются дочерними приложениями. Например, если вы запретили любую сетевую активность приложению cmd.exe, этот запрет будет распространятся на приложение notepad.exe, если она была запущена с помощью cmd.exe. При опосредованном запуске приложения (если приложение не является дочерним по отношению к приложению, из которого оно запускается), правила унаследованы не будут.

Как изменить права приложения в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.



Параметры Предотвращения вторжений

4. В блоке **Права приложений и защищаемые ресурсы** нажмите на кнопку **Настройка**.

   Откроется окно настройки прав приложений и список защищаемых ресурсов.

5. Перейдите на вкладку **Права приложений**.

6. Нажмите на кнопку **Добавить**.

7. В открывшемся окне задайте параметры поиска приложения, для которого вы хотите изменить права приложения.

   Вы можете ввести название приложения или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

8. Нажмите на кнопку **Обновить**.

   Kaspersky Endpoint Security выполнит поиск приложений в консолидированном списке приложений, установленных на управляемых компьютерах. Kaspersky Endpoint Security покажет список приложений, которые удовлетворяют параметрам поиска.

9. Выберите нужное приложение.

10. В раскрывающемся списке **Переместить приложение в группу доверия** выберите пункт **Исходные группы** и нажмите на кнопку **OK**.

    Приложение будет добавлено в исходную группу.

11. Выберите нужное приложение и в контекстном меню приложения выберите пункт **Права приложения**.

    Откроются свойства приложения.

12. Выполните одно из следующих действий:

    - Выберите вкладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами приложений.
    - Выберите вкладку **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

    Сетевую активность приложений контролирует Сетевой экран с помощью *сетевых правил*.

13. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт: **Наследовать**, **Разрешать** (✓) или **Запрещать** (⊘).

14. Если вы хотите контролировать использование ресурсов компьютера, выберите пункт **Записывать в отчет** (✓ / ⊘).

    Kaspersky Endpoint Security будет записывать информацию о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении приложением операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о приложениях, которые используют каждый ресурс.

15. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как изменить права приложения в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Предотвращение вторжений**.
5. В блоке **Права приложений и защищаемые ресурсы** нажмите на ссылку **Права приложений и защищаемые ресурсы**.

   Откроется окно настройки прав приложений и список защищаемых ресурсов.
6. Перейдите на вкладку **Права приложений**.

   Откроется список групп доверия в левой части окна и их свойства в правой части.
7. Нажмите на кнопку **Добавить**.

   Запустится мастер добавления приложения в группу доверия.
8. Выберите группу доверия, в которую вы хотите поместить приложение.
9. Выберите тип **Приложение**. Перейдите к следующему шагу.

   Если вы хотите изменить группу доверия для нескольких приложений, выберите тип **Группа** и задайте имя группы приложений.

10. В открывшемся списке приложений выберите приложения, для которых вы хотите изменить права приложения.

    Используйте фильтр. Вы можете ввести название приложения или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

11. Завершите работу мастера.

    Приложение будет добавлено в группу доверия.

12. В левой части окна выберите нужное приложение.

13. В правой части окна в раскрывающемся списке выполните одно из следующих действий:

    - Выберите пункт **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами приложения.

    - Выберите пункт **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

    Сетевую активность приложений контролирует Сетевой экран с помощью *сетевых правил*.

14. Для нужного ресурса в графе соответствующего действия выберите нужный пункт: **Наследовать**, **Разрешить** (), **Блокировать** ().

15. Если вы хотите контролировать использование ресурсов компьютера, выберите пункт **Записывать в отчет** (/).

    Kaspersky Endpoint Security будет записывать информацию о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении приложением операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о приложениях, которые используют каждый ресурс.

16. Сохраните внесенные изменения.

Как изменить права приложения в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.

3. Нажмите на кнопку **Управление приложениями**.

   Откроется список установленных приложений.

4. Выберите нужное приложение.

5. В контекстном меню приложения выберите пункт **Подробности и правила**.

   Откроются свойства приложения.

6. Выполните одно из следующих действий:

   - Выберите вкладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами приложений.

   - Выберите вкладку **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт: **Наследовать**, **Разрешить** (), **Запретить** ().

8. Если вы хотите контролировать использование ресурсов компьютера, выберите пункт **Записывать в отчет** ().

   Kaspersky Endpoint Security будет записывать информацию о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении приложением операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о приложениях, которые используют каждый ресурс.

9. Выберите вкладку **Исключения** и настройте дополнительные параметры приложения (см. таблицу ниже).

10. Сохраните внесенные изменения.

Дополнительные параметры приложения

Параметр	Описание
Не проверять открываемые файлы	Kaspersky Endpoint Security исключает из проверки все файлы, открываемые с помощью приложения. Например, если вы используете приложения резервного копирования файлов, функция позволит снизить потребление ресурсов компьютера Kaspersky Endpoint Security.
Не контролировать активность приложения	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложения в операционной системе. Вы можете настроить контроль активности приложения для разных компонентов Kaspersky Endpoint Security: • **Не контролировать для компонентов защиты и контроля**. Контроль за активностью приложения выполняют следующие компоненты: Анализ поведения, Защита от эксплойтов, Предотвращение вторжений, Откат вредоносных действий и Сетевой экран. • **Не контролировать для Managed Detection and Response и Endpoint Detection and Response**. Контроль за активностью приложения выполняют встроенный агент MDR и встроенный агент EDR (KATA). • **Не перехватывать консольный ввод для Endpoint Detection and Response**. Kaspersky Endpoint Security не отправляет данные телеметрии об управлении приложением через консоль. Данные телеметрии использует Kaspersky Anti Targeted Attack Platform (EDR).
Не наследовать ограничения родительского процесса (приложения)	Kaspersky Endpoint Security не применяет ограничения к процессу, которые настроены для родительского процесса. Родительский процесс запускает приложение, для которой настроены права приложения (Предотвращение вторжений) и сетевые правила приложения (Сетевой экран).
Не контролировать активность дочерних приложений	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложений, которые запускает приложение. Вы можете применить исключение рекурсивно. То есть приложение не контролирует активность всей цепочки дочерних приложений.
Разрешить взаимодействие с интерфейсом Kaspersky Endpoint Security для Windows	Самозащита Kaspersky Endpoint Security блокирует все попытки управления службами приложения с удаленного компьютера. Если флажок установлен, то приложению удаленного доступа к компьютеру разрешено управлять параметрами Kaspersky Endpoint Security через интерфейс Kaspersky Endpoint Security.
Не проверять зашифрованный трафик / Не проверять весь трафик	Kaspersky Endpoint Security исключает из проверки сетевой трафик, инициируемый приложением. Вы можете исключить из проверки весь трафик или только зашифрованный трафик. Также вы можете исключить из проверки отдельные IP-адреса или номера портов. Kaspersky Endpoint Security версии 14.0 и ниже не поддерживает исключение сетевого трафика, если для доверенного приложения указан хеш, а не путь.

Защита ресурсов ОС и персональных данных

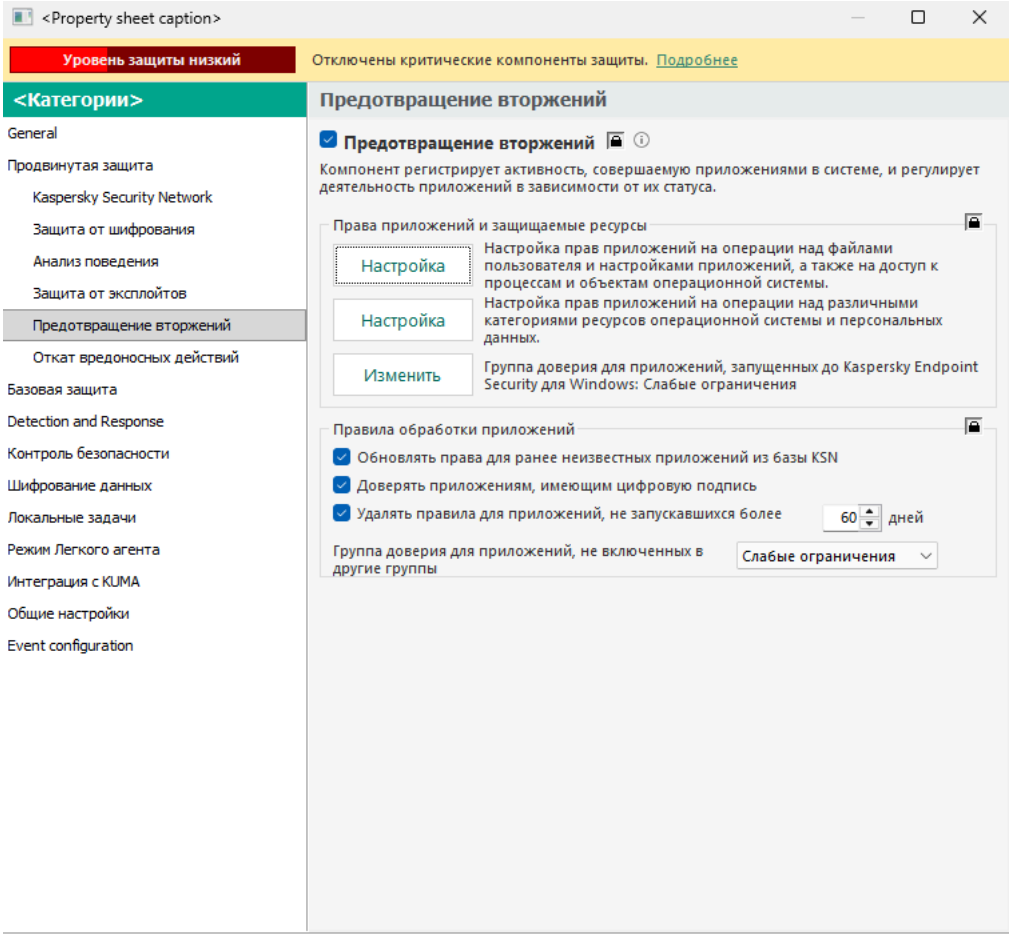
Компонент Предотвращение вторжений управляет правами приложений на операции над различными категориями ресурсов операционной системы и персональных данных. Специалисты "Лаборатории Касперского" выделили предустановленные категории защищаемых ресурсов. Например, в категории *Операционная система* есть подкатегория *Настройки автозапуска*, где перечислены все ключи реестра, относящиеся к автозапуску приложений. Вы не можете изменять или удалять предустановленные категории защищаемых ресурсов и относящиеся к ним защищаемые ресурсы.

Как добавить защищаемый ресурс в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.



Параметры Предотвращения вторжений

4. В блоке **Права приложений и защищаемые ресурсы** нажмите на кнопку **Настройка**.

   Откроется окно настройки прав приложений и список защищаемых ресурсов.

5. Перейдите на вкладку **Защищаемые ресурсы**.

   Откроется список защищаемых ресурсов в левой части окна и права доступа к этим ресурсам, в зависимости от группы доверия.

6. Выберите категорию защищаемых ресурсов, в которую вы хотите добавить новый защищаемый ресурс.

   Если вы хотите добавить вложенную категорию, нажмите на кнопку **Добавить** → **Категорию**.

7. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите тип ресурса, который вы хотите добавить: **Файл или папку** или **Ключ реестра**.

8. В открывшемся окне выберите файл, папку или ключ реестра.

   Вы можете посмотреть права доступа приложений к добавленным ресурсам. Для этого выберите добавленный ресурс в левой части окна и Kaspersky Endpoint Security покажет права доступа для каждой из групп доверия. Также вы можете выключить контроль действия приложений на операции с ресурсами с помощью флажка рядом с новым ресурсом.

9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как добавить защищаемый ресурс в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз** → **Предотвращение вторжений**.

5. В блоке **Права приложений и защищаемые ресурсы** нажмите на ссылку **Права приложений и защищаемые ресурсы**.

   Откроется окно настройки прав приложений и список защищаемых ресурсов.

6. Перейдите на вкладку **Защищаемые ресурсы**.

   Откроется список защищаемых ресурсов в левой части окна и права доступа к этим ресурсам, в зависимости от группы доверия.

7. Нажмите на кнопку **Добавить**.

   Запустится мастер добавления ресурса.

8. В блоке **Имя группы** выберите категорию защищаемых ресурсов, в которую вы хотите добавить новый защищаемый ресурс.

   Если вы хотите добавить вложенную категорию, выберите вариант **Категория защищаемых ресурсов**.

9. Выберите тип ресурса, который вы хотите добавить: **Файл или папка** или **Ключ реестра**.

10. Выберите файл, папку или ключ реестра.

11. Завершите работу мастера.

    Вы можете посмотреть права доступа приложений к добавленным ресурсам. Для этого выберите добавленный ресурс в левой части окна и Kaspersky Endpoint Security покажет права доступа для каждой из групп доверия. Также вы можете выключить контроль действия приложений на операции с ресурсами с помощью флажка в графе **Статус**.

12. Сохраните внесенные изменения.

Как добавить защищаемый ресурс в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление ресурсами**.

   Откроется список защищаемых ресурсов.
4. Выберите категорию защищаемых ресурсов, в которую вы хотите добавить новый защищаемый ресурс.

   Если вы хотите добавить вложенную категорию, нажмите на кнопку **Добавить** → **Категорию**.
5. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите тип ресурса, который вы хотите добавить: **Файл или папку** или **Ключ реестра**.
6. В открывшемся окне выберите файл, папку или ключ реестра.

   Вы можете посмотреть права доступа приложений к добавленным ресурсам. Для этого выберите добавленный ресурс в левой части окна и Kaspersky Endpoint Security покажет список приложений и права доступа для каждого из приложений. Также вы можете выключить контроль действия приложений на операции с ресурсами кнопкой **Включить контроль** в графе **Статус**.
7. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет контролировать доступ к добавленным ресурсам операционной системы и персональных данных. Kaspersky Endpoint Security контролирует доступ приложения к ресурсам на основании присвоенной группы доверия. Вы также можете изменить группу доверия для приложения.

Удаление информации о неиспользуемых приложениях

Kaspersky Endpoint Security контролирует работу приложений с помощью прав приложений. Права приложения определены группой доверия. Kaspersky Endpoint Security помещает приложение в группу доверия при первом запуске. Вы можете изменить группу доверия для приложения вручную. Также вы можете настроить права для отдельного приложения вручную. Таким образом, Kaspersky Endpoint Security хранит следующую информацию о приложении: группа доверия и права приложения.

Kaspersky Endpoint Security автоматически удаляет информацию о неиспользуемых приложениях для экономии ресурсов компьютера. Kaspersky Endpoint Security удаляет информацию о приложениях по следующим правилам:

- Если группа доверия и права приложения определены автоматически, Kaspersky Endpoint Security удаляет информацию об этом приложении через 30 дней. Изменить время хранения информации о приложении или выключить автоматическое удаление невозможно.
- Если вы вручную поместили приложение в группу доверия или настроили права доступа, Kaspersky Endpoint Security удаляет информацию об этом приложении через 60 дней (значение по умолчанию). Вы можете изменить время хранения информации о приложении или выключить автоматическое удаление (см. инструкцию ниже).

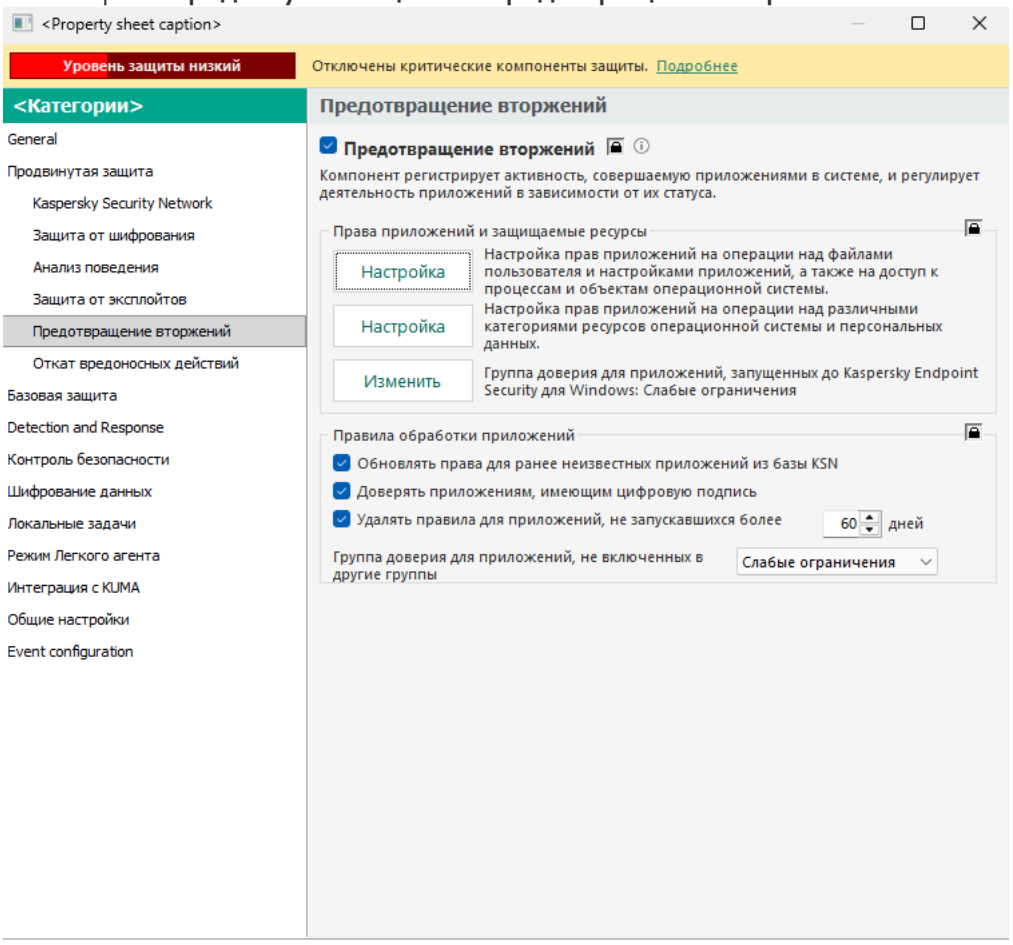
При запуске приложения, информация о которой была удалена, Kaspersky Endpoint Security исследует приложение как при первом запуске.

Как настроить автоматическое удаление информации о неиспользуемых приложениях в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.



Параметры Предотвращения вторжений

4. В блоке **Правила обработки приложений** выполните одно из следующих действий:

   - Если вы хотите настроить автоматическое удаление, установите флажок **Удалять правила для приложений, не запускавшихся более N дней** и укажите нужное количество дней.

     Kaspersky Endpoint Security будет удалять информацию о тех приложениях, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, через заданное количество дней. Также Kaspersky Endpoint Security будет удалять информацию о приложениях, для которых группа доверия и права приложения определены автоматически, через 30 дней.

   - Если вы хотите выключить автоматическое удаление, снимите флажок **Удалять правила для приложений, не запускавшихся более N дней**.

     Kaspersky Endpoint Security будет хранить информацию о тех приложениях, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, без ограничений по времени. Kaspersky Endpoint Security будет удалять информацию только о приложениях, для которых группа доверия и права приложения определены автоматически, через 30 дней.

5. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить автоматическое удаление информации о неиспользуемых приложениях в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Предотвращение вторжений**.
5. В блоке **Правила обработки приложений** выполните одно из следующих действий:

   - Если вы хотите настроить автоматическое удаление, установите флажок **Удалять правила для приложений, не запускавшихся более (дней, от 1 до 90)** и укажите нужное количество дней.

     Kaspersky Endpoint Security будет удалять информацию о тех приложениях, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, через заданное количество дней. Также Kaspersky Endpoint Security будет удалять информацию о приложениях, для которых группа доверия и права приложения определены автоматически, через 30 дней.

   - Если вы хотите выключить автоматическое удаление, снимите флажок **Удалять правила для приложений, не запускавшихся более (дней, от 1 до 90)**.

     Kaspersky Endpoint Security будет хранить информацию о тех приложениях, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, без ограничений по времени. Kaspersky Endpoint Security будет удалять информацию только о приложениях, для которых группа доверия и права приложения определены автоматически, через 30 дней.
6. Сохраните внесенные изменения.

Как настроить автоматическое удаление информации о неиспользуемых приложениях в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Предотвращение вторжений**.
3. В блоке **Правила обработки приложений** выполните одно из следующих действий:

   - Если вы хотите настроить автоматическое удаление, установите флажок **Удалять правила для приложений, не запускавшихся более N дней (от 1 до 90)** и укажите нужное количество дней.

     Kaspersky Endpoint Security будет удалять информацию о тех приложениях, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, через заданное количество дней. Также Kaspersky Endpoint Security будет удалять информацию о приложениях, для которых группа доверия и права приложения определены автоматически, через 30 дней.

   - Если вы хотите выключить автоматическое удаление, снимите флажок **Удалять правила для приложений, не запускавшихся более N дней (от 1 до 90)**.

     Kaspersky Endpoint Security будет хранить информацию о тех приложениях, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, без ограничений по времени. Kaspersky Endpoint Security будет удалять информацию только о приложениях, для которых группа доверия и права приложения определены автоматически, через 30 дней.
4. Сохраните внесенные изменения.

Мониторинг работы Предотвращения вторжений

Вы можете получать отчеты о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении приложением операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о приложениях, которые используют каждый ресурс.

Для мониторинга работы Предотвращения вторжений вам нужно включить запись в отчет. Например, вы можете включить отправку отчетов для отдельных приложений в параметрах компонента Предотвращение вторжений.

При настройке мониторинга работы Предотвращения вторжения учитывайте нагрузку на сеть при отправке событий в Kaspersky Security Center. Также вы можете включить сохранение отчетов только в локальном журнале Kaspersky Endpoint Security.

Защита доступа к аудио и видео

Функциональность защиты аудиосигнала и защиты доступа приложений к веб-камерам не поддерживается на компьютерах с Arm-архитектурой.

Злоумышленники могут с помощью специальных приложений пытаться получить доступ к устройствам записи аудио и видео (например, микрофоны или веб-камеры). Kaspersky Endpoint Security контролирует получение приложениями аудиосигнала и видеосигнала и защищает данные от несанкционированного перехвата.

По умолчанию Kaspersky Endpoint Security разрешает получение аудиосигнала и видеосигнала только для приложений из группы *Доверенные*. Приложениям из групп *Слабые ограничения*, *Сильные ограничения* и *Недоверенные* доступ к аудиосигналу и видеосигналу запрещен. Вы можете вручную разрешать приложениям получать аудиосигнал и видеосигнал.

Особенности защиты аудиосигнала

Функциональность защиты аудиосигнала имеет следующие особенности:

- Для работы функциональности необходимо, чтобы был включен компонент Предотвращение вторжений.
- Если приложение начало получать аудиосигнал до запуска компонента Предотвращение вторжений, то Kaspersky Endpoint Security разрешает приложению получение аудиосигнала и не показывает никаких уведомлений.
- Если вы поместили приложение в группу *Недоверенные* или *Сильные ограничения* после того, как приложение начало получать аудиосигнал, то Kaspersky Endpoint Security разрешает приложению получение аудиосигнала и не показывает никаких уведомлений.

- При изменении параметров доступа приложения к устройствам записи звука (например, приложению было запрещено получение аудиосигнала) требуется перезапуск этого приложения, чтобы она перестала получать аудиосигнал.

- Контроль получения аудиосигнала с устройств записи звука не зависит от параметров доступа приложений к веб-камере.

- Kaspersky Endpoint Security защищает доступ только к встроенным и внешним микрофонам. Другие устройства передачи звука не поддерживаются.

- Kaspersky Endpoint Security не гарантирует защиту аудиосигнала, передаваемого с таких устройств, как DSLR-камеры, портативные видеокамеры, экшн-камеры.

- При первом запуске приложения Kaspersky Endpoint Security с момента ее установки воспроизведение или запись аудио и видео могут быть прерваны в приложениях записи или воспроизведения аудио и видео. Это необходимо для того, чтобы включилась функциональность контроля доступа приложений к устройствам записи звука. Системная служба управления средствами работы со звуком будет перезапущена при первом запуске приложения Kaspersky Endpoint Security.

Особенности доступа приложений к веб-камерам

Функциональность защиты доступа к веб-камере имеет следующие особенности и ограничения:

- Приложение контролирует видео и статические изображения, полученные в результате обработки данных веб-камеры.

- Приложение контролирует аудиосигнал, если он является частью видеопотока, получаемого с веб-камеры.

- Приложение контролирует только веб-камеры, подключаемые по интерфейсу USB или IEEE1394 и отображаемые в Диспетчере устройств Windows как Устройства обработки изображений (англ. Imaging Device).

- Kaspersky Endpoint Security поддерживает следующие веб-камеры:

  - Logitech HD Webcam C270;

  - Logitech HD Webcam C310;

  - Logitech Webcam C210;

  - Logitech Webcam Pro 9000;

  - Logitech HD Webcam C525;

  - Microsoft LifeCam VX-1000;

  - Microsoft LifeCam VX-2000;

  - Microsoft LifeCam VX-3000;

- Microsoft LifeCam VX-800;
- Microsoft LifeCam Cinema.

"Лаборатория Касперского" не гарантирует поддержку веб-камер, не указанных в этом списке.

Защита от атак BadUSB

Некоторые вирусы изменяют встроенное программное обеспечение USB-устройств так, чтобы операционная система определяла USB-устройство как клавиатуру. В результате вирус может выполнять команды под вашей учетной записью, например, загрузить вредоносное приложение.

Компонент Защита от атак BadUSB позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру.

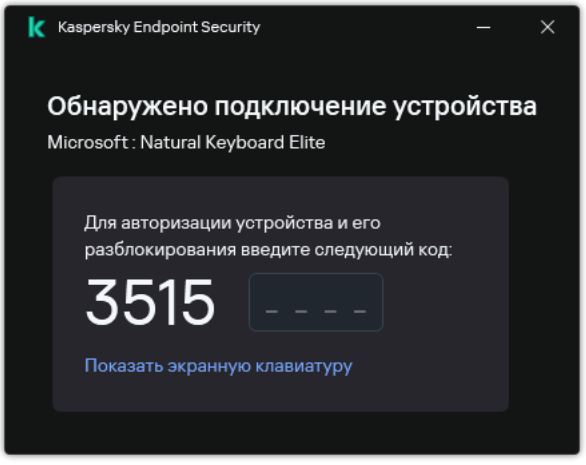
Когда к компьютеру подключается USB-устройство, определенное операционной системой как клавиатура, приложение предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) цифровой код, сформированный приложением (см. рис. ниже). Эта процедура называется авторизацией клавиатуры.

Если код введен правильно, приложение сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется.

При подключении авторизованной клавиатуры через другой USB-порт компьютера приложение снова запрашивает ее авторизацию.

Если цифровой код введен неправильно, приложение формирует новый. Вы можете настроить число попыток для ввода цифрового кода. Если цифровой код введен неправильно несколько раз или закрыто окно авторизации клавиатуры (см. рис. ниже), приложение блокирует ввод с этой клавиатуры. По истечении времени блокировки USB-устройства или перезагрузке операционной системы приложение снова предлагает пройти авторизацию клавиатуры.

Приложение разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.



Авторизация клавиатуры

Включение и выключение Защиты от атак BadUSB

USB-устройства, определенные операционной системой как клавиатуры и подключенные к компьютеру до установки компонента Защита от атак BadUSB, считаются авторизованными после его установки.

Как включить или выключить компонент Защита от атак BadUSB в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита → Защита от атак BadUSB**.
4. Используйте флажок **Защита от атак BadUSB**, чтобы включить или выключить компонент.
5. В блоке **Авторизация USB-устройств при подключении** настройте параметры безопасности ввода кода авторизации:

   - **Максимальное количество попыток авторизации USB-устройства**. Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Endpoint Security покажет время блокировки USB-устройства. По истечении указанного времени вам будут снова доступны 5 попыток ввода кода авторизации.

   - **Тайм-аут при достижении максимального количества попыток (минут)**. Время блокировки USB-устройства после заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить компонент Защита от атак BadUSB в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз → Защита от атак BadUSB**.
5. Используйте переключатель **Защита от атак BadUSB ВКЛЮЧЕНА**, чтобы включить или выключить компонент.

6. В блоке **Авторизация USB-устройств** настройте параметры безопасности ввода кода авторизации:

   - **Максимальное количество попыток авторизации USB-устройства**. Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Endpoint Security покажет время блокировки USB-устройства. По истечении указанного времени вам будут снова доступны 5 попыток ввода кода авторизации.

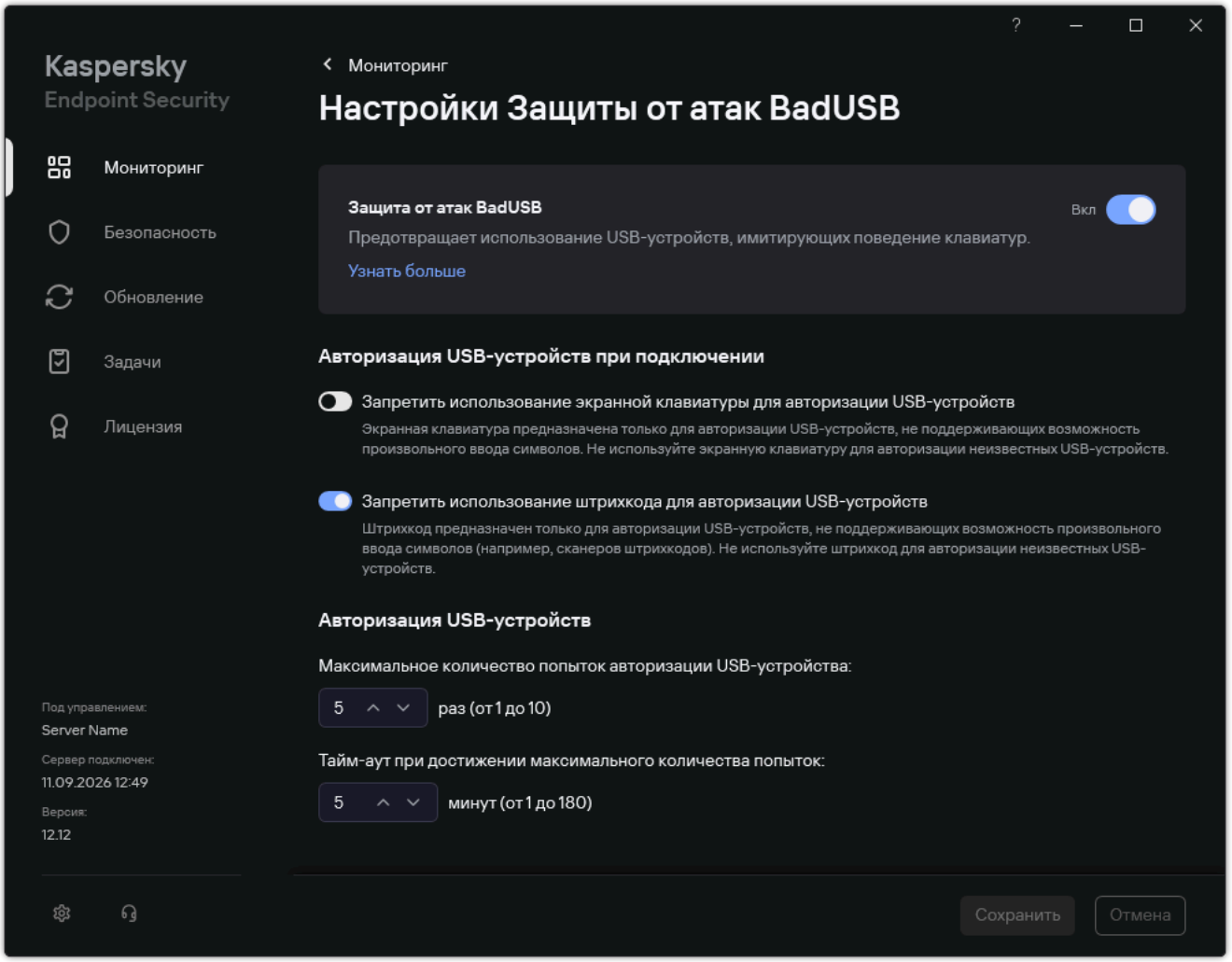
   - **Тайм-аут при достижении максимального количества попыток (мин)**. Время блокировки USB-устройства после заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).

7. Сохраните внесенные изменения.

Как включить или выключить компонент Защита от атак BadUSB в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от атак BadUSB**.



Параметры Защиты от атак BadUSB

3. Используйте переключатель **Защита от атак BadUSB**, чтобы включить или выключить компонент.

4. В блоке **Авторизация USB-устройств при подключении** настройте параметры безопасности ввода кода авторизации:

   - **Максимальное количество попыток авторизации USB-устройства**. Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Endpoint Security покажет время блокировки USB-устройства. По истечении указанного времени вам будут снова доступны 5 попыток ввода кода авторизации.

   - **Тайм-аут при достижении максимального количества попыток**. Время блокировки USB-устройства после заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).

5. Сохраните внесенные изменения.

В результате, если Защита от атак BadUSB включена, Kaspersky Endpoint Security требует авторизацию подключенного USB-устройства, определенного операционной системой как клавиатура. Пользователь не может использовать неавторизованную клавиатуру до тех пор, пока она не будет авторизована.

Использование экранной клавиатуры при авторизации USB-устройств

Возможность использовать экранную клавиатуру предназначена только для авторизации USB-устройств, не поддерживающих произвольный ввод символов (например, сканеров штрихкодов). Не рекомендуется использовать экранную клавиатуру для авторизации неизвестных вам USB-устройств.

Как разрешить или запретить использование экранной клавиатуры при авторизации в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Базовая защита → Защита от атак BadUSB**.

4. Используйте флажок **Запретить использование экранной клавиатуры для авторизации USB-устройств**, чтобы запретить или разрешить использование экранной клавиатуры для авторизации.

5. Сохраните внесенные изменения.

Как разрешить или запретить использование экранной клавиатуры при авторизации в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз → Защита от атак BadUSB**.

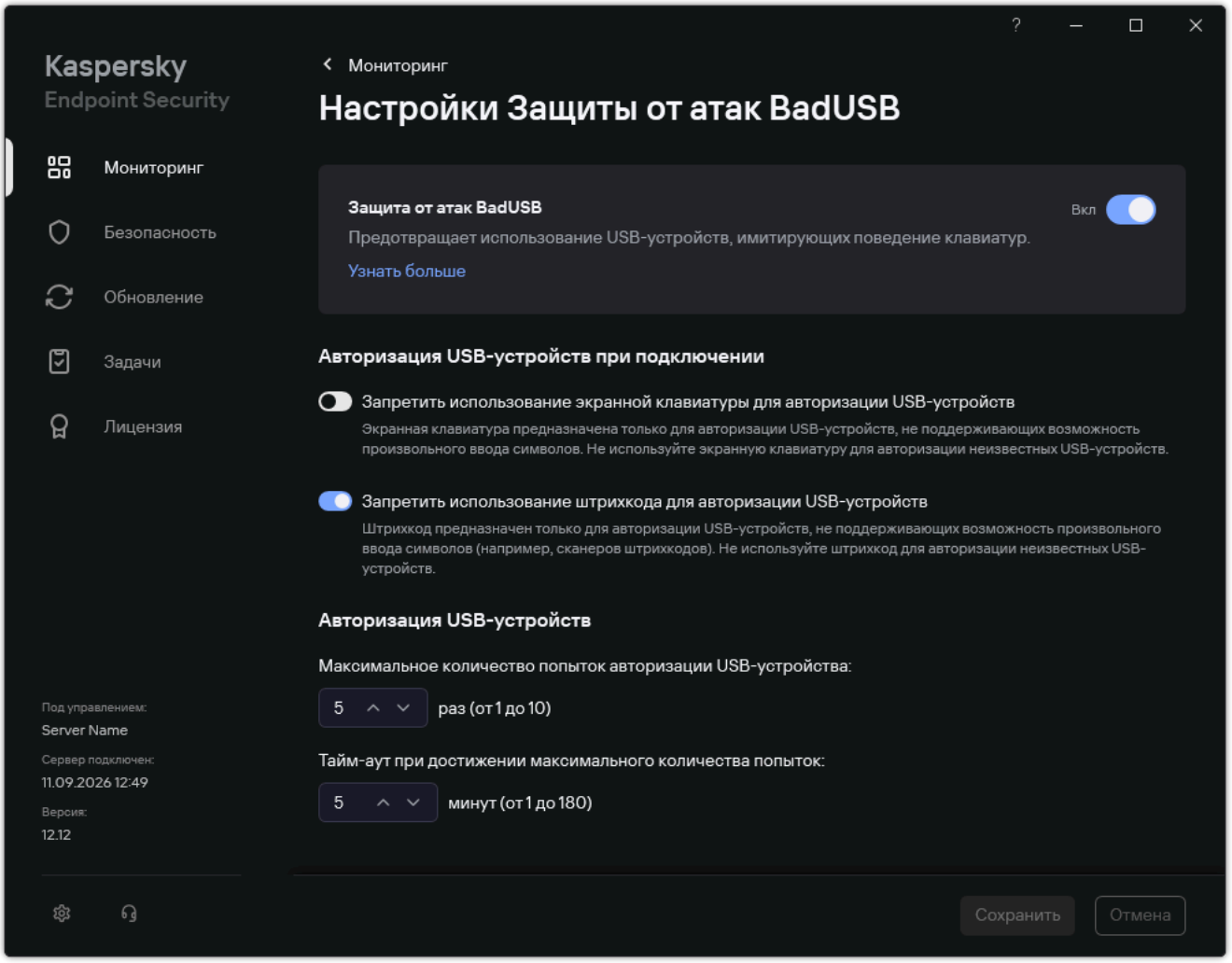
5. Используйте переключатель **Запрет на использование экранной клавиатуры для авторизации USB-устройств**, чтобы запретить или разрешить использование экранной клавиатуры для авторизации.

6. Сохраните внесенные изменения.

Как разрешить или запретить использование экранной клавиатуры при авторизации в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

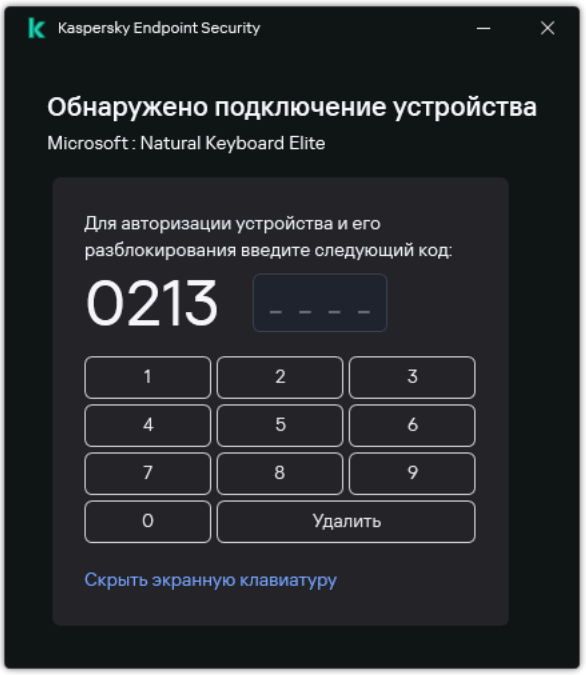
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от атак BadUSB**.



Параметры Защиты от атак BadUSB

3. Используйте переключатель **Запретить использование экранной клавиатуры для авторизации USB-устройств**, чтобы запретить или разрешить использование экранной клавиатуры для авторизации.

4. Сохраните внесенные изменения.



Авторизация USB-устройств

Авторизация сканеров штрихкода

При подключении сканера штрихкодов к компьютеру компонент Защита от атак BadUSB определяет это устройство как устройство ввода и предлагает выполнить процедуру авторизации. Для авторизации сканера штрихкодов вам нужно считать штрихкод с экрана. Приложение формирует штрихкод в формате Code39, который поддерживает большинство сканеров штрихкодов и сканеров QR-кодов.

Kaspersky Endpoint Security также поддерживает другой способ авторизации сканеров штрихкодов. Если вы используете устройства с сенсорным экраном, для авторизации сканера штрихкодов вы можете ввести код с помощью экранной клавиатуры. Для этого вам нужно разрешить использование экранной клавиатуры. Этот способ удобен, например, для стационарных сканеров штрихкодов в составе кассовых аппаратов. Другие способы авторизации сканеров штрихкодов запрещены.

По умолчанию приложение не использует штрихкод для авторизации USB-устройств.

Как включить авторизацию USB-устройств по штрихкоду в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите папку **Политики**.

3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

4. В окне политики выберите **Базовая защита** → **Защита от атак BadUSB**.

5. Используйте флажок **Запретить использование штрихкода для авторизации USB-устройств**, чтобы запретить или разрешить использование штрихкодов для авторизации.

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить авторизацию USB-устройств по штрихкоду в Web Console и Cloud Console

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз → Защита от атак BadUSB**.

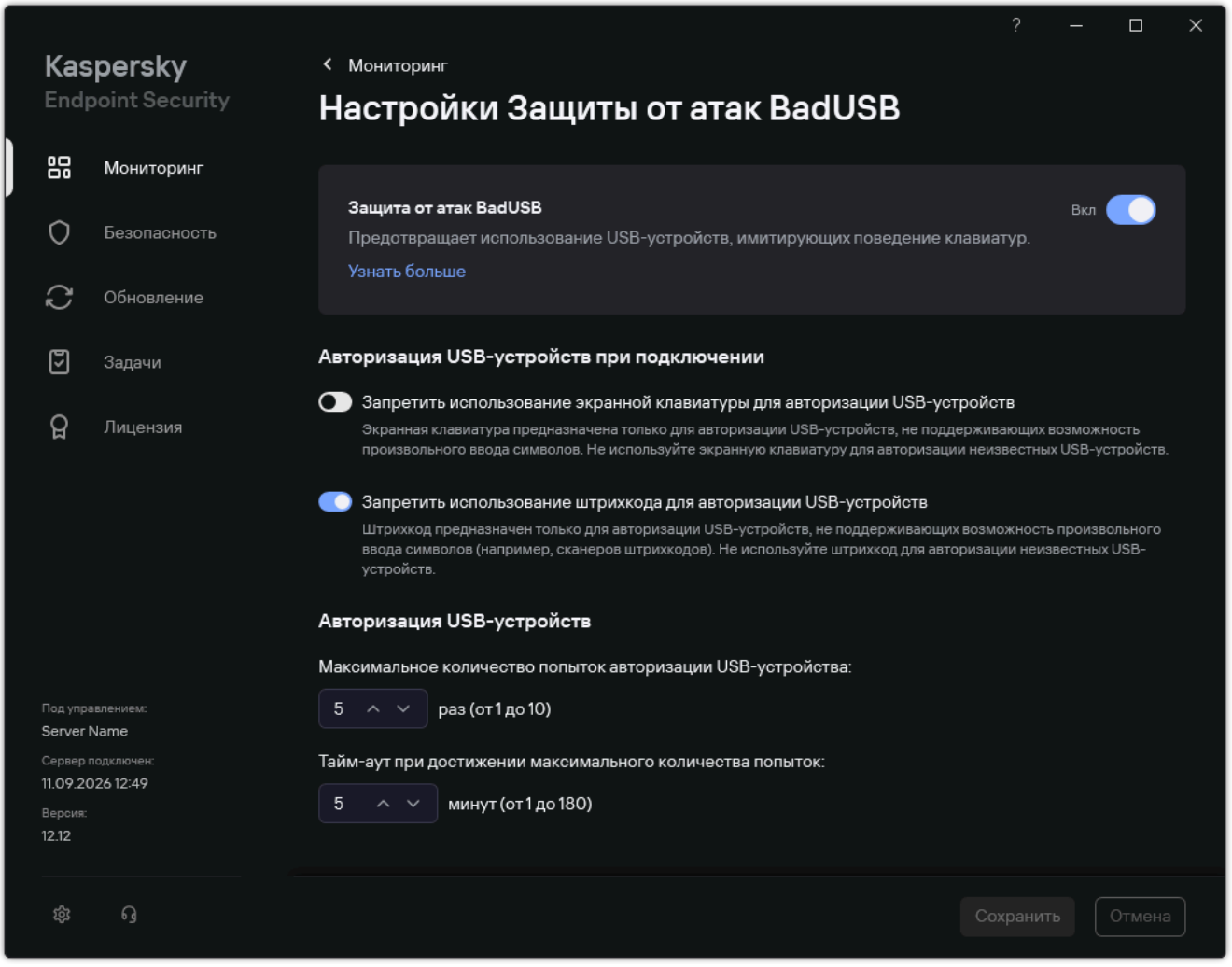
5. Используйте переключатель **Запрет на использование штрихкода для авторизации USB-устройств**, чтобы запретить или разрешить использование штрихкодов для авторизации.

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить авторизацию USB-устройств по штрихкоду в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .

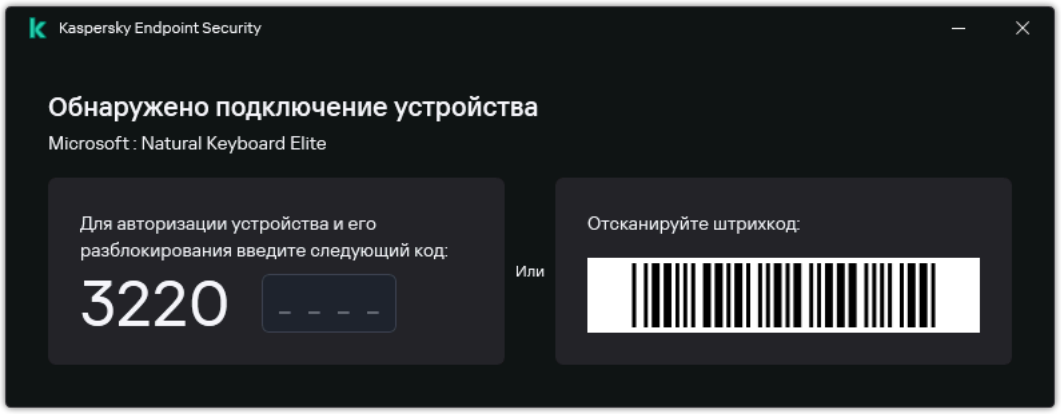
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от атак BadUSB**.



Параметры Защиты от атак BadUSB

3. Используйте переключатель **Запретить использование штрихкода для авторизации USB-устройств**, чтобы запретить или разрешить использование штрихкодов для авторизации.

4. Сохраните внесенные изменения.

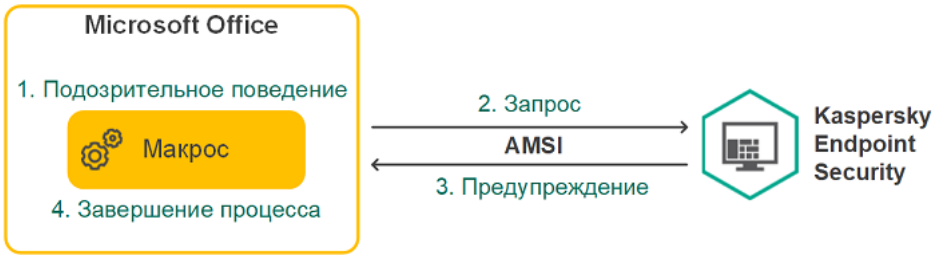


Авторизация сканеров штрихкода

AMSI-защита

Компонент AMSI-защита предназначен для поддержки интерфейса Antimalware Scan Interface от Microsoft. *Интерфейс Antimalware Scan Interface (AMSI)* позволяет сторонним приложениям с поддержкой AMSI отправлять объекты (например, скрипты PowerShell) в Kaspersky Endpoint Security для дополнительной проверки и получать результаты проверки этих объектов. Сторонними приложениями могут быть, например, приложения Microsoft Office (см. рис. ниже). Подробнее об интерфейсе AMSI см. в документации Microsoft.

AMSI-защита может только обнаруживать угрозу и уведомлять стороннее приложение об обнаруженной угрозе. Стороннее приложение после получения уведомления об угрозе не дает выполнить вредоносные действия (например, завершает работу).



Пример работы AMSI

Компонент AMSI-защита может отклонить запрос от стороннего приложения, например, если это приложение превысило максимальное количество запросов за промежуток времени. Kaspersky Endpoint Security отправляет информацию об отклонении запроса от стороннего приложения на Сервер администрирования. Компонент AMSI-защита не отклоняет запросы от тех сторонних приложений, для которых включена функция постоянного взаимодействия с компонентом AMSI-защита.

AMSI-защита доступна для следующих операционных систем рабочих станций и серверов:

- Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise / Enterprise multi-session;
- Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise / Enterprise multi-session;

- Windows Server 2016 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая режим Server Core);
- Windows Server 2025 Standard / Datacenter.

Включение и выключение AMSI-защиты

По умолчанию AMSI-защита включена и работает в рекомендованном специалистами "Лаборатории Касперского" режиме (см. таблицу ниже).

Как включить или выключить AMSI-защиту в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита → AMSI-защита**.
4. Используйте флажок **AMSI-защита**, чтобы включить или выключить компонент.
5. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

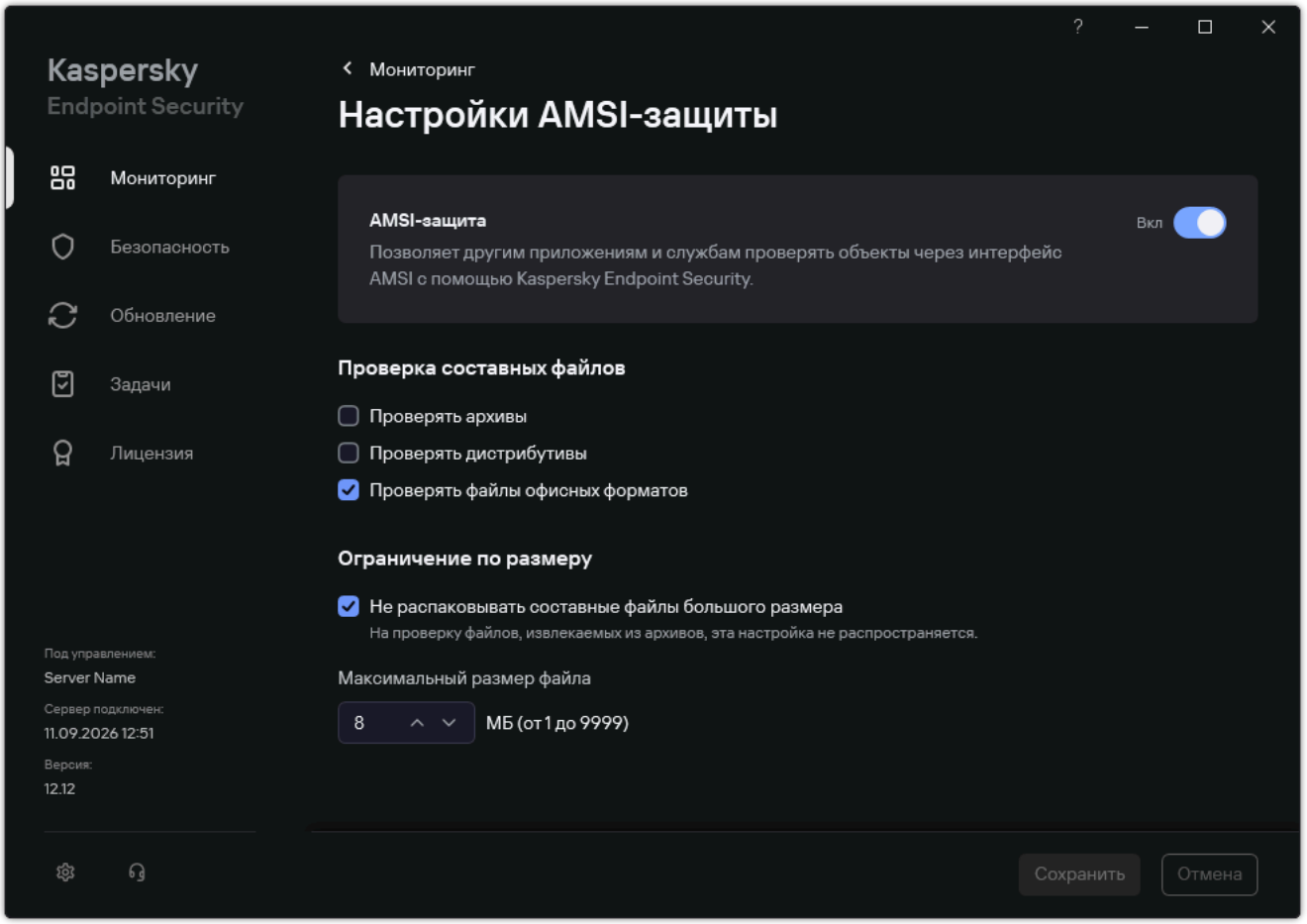
Как включить или выключить AMSI-защиту в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз → AMSI-защита**.
5. Используйте переключатель **AMSI-защита ВКЛЮЧЕНА**, чтобы включить или выключить компонент.
6. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как включить или выключить AMSI-защиту в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **AMSI-защита**.



Параметры AMSI-защиты

3. Используйте переключатель **AMSI-защита**, чтобы включить или выключить компонент.

4. Сохраните внесенные изменения.

Параметры AMSI-защиты, рекомендованные специалистами "Лаборатории Касперского"

Параметр	Значение	Описание
Проверять архивы	**Выкл**	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	**Выкл**	Проверка дистрибутивов сторонних приложений.
Проверять файлы офисных форматов	**Вкл**	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Не распаковывать составные файлы большого размера	**Максимальный размер файла 8 МБ**	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.

Оптимизация проверки файлов AMSI-защитой

Вы можете оптимизировать проверку файлов: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security. Вы можете выбрать составные файлы, которые необходимо проверять: архивы, дистрибутивы или файлы офисных форматов. Вы можете также ограничить размер проверяемых составных файлов. Компонент AMSI-защита не будет распаковывать составные файлы больше указанного размера.

Распространенной практикой сокрытия вирусов и других приложений, представляющих угрозу, является внедрение их в составные файлы, например, архивы. Чтобы обнаружить скрытые таким образом вирусы и другие приложения, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить набор типов проверяемых составных файлов, таким образом увеличив скорость проверки.

Как оптимизировать проверку файлов AMSI-защитой в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита → AMSI-защита**.
4. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, дистрибутивы или файлы офисных форматов.
5. В блоке **Ограничение по размеру** выполните одно из следующих действий:
   - Чтобы запретить компоненту AMSI-защита распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и укажите нужное значение. Компонент AMSI-защита не будет распаковывать составные файлы больше указанного размера.
   - Чтобы разрешить компоненту AMSI-защита распаковывать составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

   Компонент AMSI-защита проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.
6. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как оптимизировать проверку файлов AMSI-защитой в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз → AMSI-защита**.

5. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, дистрибутивы или файлы офисных форматов.

6. В блоке **Оптимизация проверки** выполните одно из следующих действий:

   - Чтобы запретить компоненту AMSI-защита распаковывать составные файлы большого размера, установите флажок **Ограничение на размер объекта включено** и укажите нужное значение. Компонент AMSI-защита не будет распаковывать составные файлы больше указанного размера.

   - Чтобы разрешить компоненту AMSI-защита распаковывать составные файлы большого размера, снимите флажок **Ограничение на размер объекта включено**.

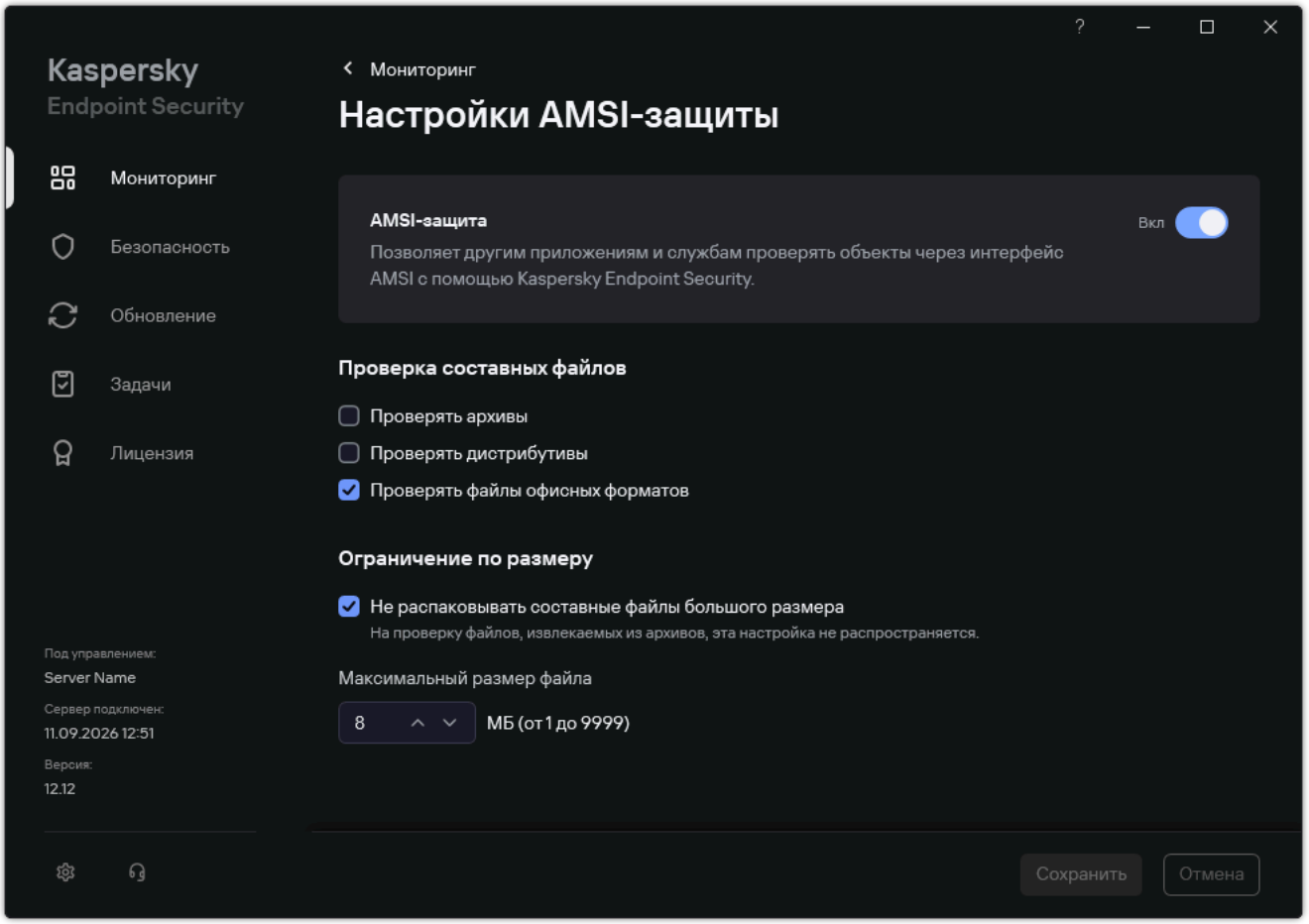
   Компонент AMSI-защита проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Ограничение на размер объекта включено**.

7. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как оптимизировать проверку файлов AMSI-защитой в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **AMSI-защита**.



Параметры AMSI-защиты

3. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, дистрибутивы или файлы офисных форматов.

4. В блоке **Ограничение по размеру** выполните одно из следующих действий:

   - Чтобы запретить компоненту AMSI-защита распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и укажите нужное значение. Компонент AMSI-защита не будет распаковывать составные файлы больше указанного размера.

   - Чтобы разрешить компоненту AMSI-защита распаковывать составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

   Компонент AMSI-защита проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

5. Сохраните внесенные изменения.

Защита от веб-угроз

Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует соединение с вредоносными и фишинговыми веб-сайтами. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Kaspersky Endpoint Security проверяет HTTP-, HTTPS- и FTP-трафик. Kaspersky Endpoint Security проверяет URL- и IP-адреса.

Для работы Защиты от веб-угроз необходимо выполнить первоначальную настройку приложения:

- Для контроля HTTPS-трафика включите проверку защищенных соединений (по умолчанию проверка включена).

- Выберите порты, которые Kaspersky Endpoint Security будет контролировать (по умолчанию приложение контролирует все порты).

- Выберите приложения, трафик которых будет контролировать Kaspersky Endpoint Security. Основные браузеры уже добавлены в список, рекомендованный "Лабораторией Касперского". Если вашего браузера нет в списке, добавьте приложение вручную.

- Рекомендуется внедрить в трафик скрипт для взаимодействия с веб-страницами (по умолчанию внедрение скрипта выключено). Скрипт позволяет регистрировать события работы Защиты от веб-угроз для журнала событий приложения, журнала событий ОС, отчетов.

При попытке пользователя открыть вредоносный или фишинговый веб-сайт, Kaspersky Endpoint Security заблокирует доступ и покажет предупреждение.

Включение и выключение Защиты от веб-угроз

По умолчанию компонент Защита от веб-угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для работы Защиты от веб-угроз приложение применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности веб-трафика **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского" (см. таблицу ниже). Вы можете выбрать один из предустановленных уровней безопасности веб-трафика, получаемых или передаваемых по протоколам HTTP и FTP, или настроить уровень безопасности веб-трафика самостоятельно. После того как вы изменили параметры уровня безопасности веб-трафика, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности веб-трафика.

Вы можете выбрать или настроить уровень безопасности только в Консоли администрирования (MMC) или в локальном интерфейсе приложения. Выбрать или настроить уровень безопасности в Web Console или Cloud Console невозможно.

Как включить или выключить компонент Защита от веб-угроз в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита** → **Защита от веб-угроз**.
4. Используйте флажок **Защита от веб-угроз**, чтобы включить или выключить компонент.
5. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:

   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:

     - **Высокий**. Уровень безопасности веб-трафика, при котором компонент Защита от веб-угроз максимально проверяет веб-трафик, поступающий на компьютер по HTTP- и FTP-протоколам. Защита от веб-угроз детально проверяет все объекты веб-трафика, используя полный набор баз приложения, а также выполняет максимально глубокий эвристический анализ.
     - **Рекомендуемый**. Уровень безопасности веб-трафика, обеспечивающий оптимальный баланс между производительностью приложения и безопасностью веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на среднем уровне. Этот уровень безопасности веб-трафика рекомендован для использования специалистами "Лаборатории Касперского". Значения параметров для рекомендуемого уровня безопасности см. в таблице ниже.
     - **Низкий**. Уровень безопасности веб-трафика, параметры которого обеспечивают максимальную скорость проверки веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на поверхностном уровне.

   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка** и задайте параметры работы компонента (см. таблицу ниже).

     Вы можете восстановить значения предустановленных уровней безопасности по кнопке **По умолчанию**.

6. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами веб-трафика:

   - **Блокировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере.

   - **Информировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта Kaspersky Endpoint Security разрешает загрузку этого объекта на компьютер и добавляет информацию о зараженном объекте в список активных угроз.

7. Сохраните внесенные изменения.

Как включить или выключить компонент Защита от веб-угроз в Web Console

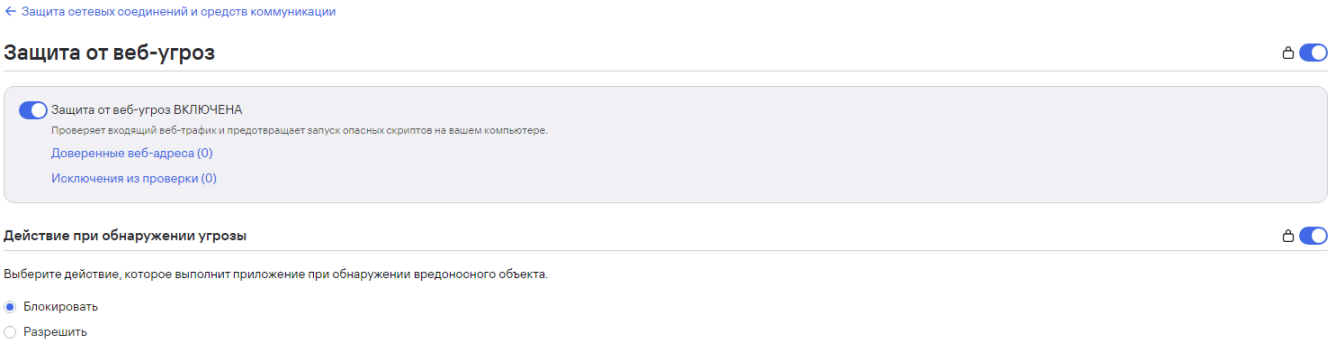
1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Защита от веб-угроз**.



Параметры Защиты от веб-угроз

5. Используйте переключатель **Защита от веб-угроз ВКЛЮЧЕНА**, чтобы включить или выключить компонент.

6. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами веб-трафика:

   - **Блокировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере.

   - **Разрешить, информировать или запросить действие (в зависимости от ОС)**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта Kaspersky Endpoint Security разрешает загрузку этого объекта на компьютер и добавляет информацию о зараженном объекте в список активных угроз.

7. Если требуется, сформируйте список доверенных веб-адресов.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить компонент Защита от веб-угроз в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от веб-угроз**.

3. Используйте переключатель **Защита от веб-угроз**, чтобы включить или выключить компонент.

4. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:

   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:

     - **Высокий**. Уровень безопасности веб-трафика, при котором компонент Защита от веб-угроз максимально проверяет веб-трафик, поступающий на компьютер по HTTP- и FTP-протоколам. Защита от веб-угроз детально проверяет все объекты веб-трафика, используя полный набор баз приложения, а также выполняет максимально глубокий эвристический анализ.

     - **Рекомендуемый**. Уровень безопасности веб-трафика, обеспечивающий оптимальный баланс между производительностью приложения и безопасностью веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на среднем уровне. Этот уровень безопасности веб-трафика рекомендован для использования специалистами "Лаборатории Касперского". Значения параметров для рекомендуемого уровня безопасности см. в таблице ниже.

     - **Низкий**. Уровень безопасности веб-трафика, параметры которого обеспечивают максимальную скорость проверки веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на поверхностном уровне.

   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента (см. таблицу ниже).

     Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности**.

5. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами веб-трафика:

   - **Блокировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере.

   - **Информировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта Kaspersky Endpoint Security разрешает загрузку этого объекта на компьютер и добавляет информацию о зараженном объекте в список активных угроз.

6. Сохраните внесенные изменения.

Параметры Защиты от веб-угроз, рекомендованные специалистами "Лаборатории Касперского", (рекомендованный уровень безопасности)

Параметр	Значение	Описание
Проверять веб-адрес по базе вредоносных веб-адресов	**Вкл**	Проверка ссылок на принадлежность к базе вредоносных веб-адресов позволяет отследить веб-сайты, которые находятся в списке запрещенных веб-адресов. База вредоносных веб-адресов формируется специалистами "Лаборатории Касперского", входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security.
Проверять веб-адрес по базе фишинговых веб-адресов	**Вкл**	В состав базы фишинговых веб-адресов включены веб-адреса известных на настоящее время веб-сайтов, которые используются для фишинг-атак. Базу фишинговых веб-адресов специалисты "Лаборатории Касперского" пополняют веб-адресами, предоставленными международной организацией по борьбе с фишингом The Anti-Phishing Working Group. База фишинговых веб-адресов входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security.

Параметр	Значение	Описание
Использовать эвристический анализ (Защита от веб-угроз)	**Средний**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки веб-трафика на наличие вирусов и других приложений, представляющих угрозу, эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Использовать эвристический анализ (Анти-Фишинг)	**Вкл**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.
Действие при обнаружении угрозы	**Блокировать**	Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере.

Настройка методов обнаружения вредоносных веб-адресов

Защита от веб-угроз обнаруживает вредоносные веб-адреса с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Вы можете выбрать методы обнаружения вредоносных веб-адресов только в Консоли администрирования (MMC) или в локальном интерфейсе приложения. Выбрать методы обнаружения вредоносных веб-адресов в Web Console или Cloud Console невозможно. По умолчанию проверка по базе вредоносных веб-адресов с использованием эвристического анализа (средний уровень) включена.

Проверка по базе вредоносных адресов

Проверка ссылок на принадлежность к базе вредоносных веб-адресов позволяет отследить веб-сайты, которые находятся в списке запрещенных веб-адресов. База вредоносных веб-адресов формируется специалистами "Лаборатории Касперского", входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security.

Kaspersky Endpoint Security проверяет все ссылки по базам вредоносных веб-адресов. Параметры проверки защищенных соединений приложения не влияют на проверку ссылок. То есть, если проверка защищенных соединений выключена, Kaspersky Endpoint Security проверяет ссылки по базам вредоносных веб-адресов, даже если сетевой трафик передается по защищенному соединению.

Как включить или выключить проверку по базе вредоносных адресов в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита** → **Защита от веб-угроз**.

4. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне в блоке **Методы проверки** используйте флажок **Проверять веб-адрес по базе вредоносных веб-адресов**, чтобы включить или выключить проверку по базе вредоносных адресов.

6. Сохраните внесенные изменения.

Как включить или выключить проверку по базе вредоносных адресов в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от веб-угроз**.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Методы проверки** используйте флажок **Проверять веб-адрес по базе вредоносных веб-адресов**, чтобы включить или выключить проверку по базе вредоносных адресов.

5. Сохраните внесенные изменения.

Эвристический анализ

В процессе эвристического анализа Kaspersky Endpoint Security анализирует активность, которую приложения производят в операционной системе. Эвристический анализ позволяет обнаруживать угрозы, записей о которых еще нет в базах Kaspersky Endpoint Security.

Во время проверки веб-трафика на наличие вирусов и других приложений, представляющих угрозу, эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

Как включить или выключить использование эвристического анализа в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Базовая защита → Защита от веб-угроз**.

4. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне в блоке **Методы проверки** установите флажок **Использовать эвристический анализ**, если вы хотите, чтобы приложение использовало эвристический анализ при проверке веб-трафика на наличие вирусов и других приложений, представляющих угрозу.

6. При помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.

   Во время проверки веб-трафика на наличие вирусов и других приложений, представляющих угрозу эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

7. Сохраните внесенные изменения.

Как включить или выключить использование эвристического анализа в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от веб-угроз**.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Методы проверки** установите флажок **Использовать эвристический анализ**, если вы хотите, чтобы приложение использовало эвристический анализ при проверке веб-трафика на наличие вирусов и других приложений, представляющих угрозу.

   Во время проверки веб-трафика на наличие вирусов и других приложений, представляющих угрозу, эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

5. Сохраните внесенные изменения.

Анти-Фишинг

Защита от веб-угроз проверяет ссылки на принадлежность к фишинговым веб-адресам. Это позволяет избежать *фишинговых атак*. Частным примером фишинговых атак может служить сообщение электронной почты якобы от банка, клиентом которого вы являетесь, со ссылкой на официальный веб-сайт банка в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его веб-адрес в браузере, однако находитесь на фиктивном веб-сайте. Все ваши дальнейшие действия на веб-сайте отслеживаются и могут быть использованы для кражи ваших денежных средств.

Поскольку ссылка на фишинговый веб-сайт может содержаться не только в сообщении электронной почты, но и, например, в сообщении мессенджера, компонент Защита от веб-угроз отслеживает попытки перейти на фишинговый веб-сайт на уровне проверки веб-трафика и блокирует доступ к таким веб-сайтам. Списки фишинговых веб-адресов включены в комплект поставки Kaspersky Endpoint Security.

Вы можете настроить функцию Анти-Фишинг только в Консоли администрирования (MMC) или в локальном интерфейсе приложения. Настроить функцию Анти-Фишинг в Web Console или Cloud Console невозможно. По умолчанию функция Анти-Фишинг с использованием эвристического анализа включена.

Как включить или выключить функцию Анти-Фишинг в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Базовая защита → Защита от веб-угроз**.

4. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне в блоке **Настройки Анти-Фишинга** используйте флажок **Проверять веб-адрес по базе фишинговых веб-адресов**, чтобы включить или выключить функцию Анти-Фишинг.

   В состав базы фишинговых веб-адресов включены веб-адреса известных на настоящее время веб-сайтов, которые используются для фишинг-атак. Базу фишинговых веб-адресов специалисты "Лаборатории Касперского" пополняют веб-адресами, предоставленными международной организацией по борьбе с фишингом The Anti-Phishing Working Group. База фишинговых веб-адресов входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security.

6. Установите флажок **Использовать эвристический анализ**, если вы хотите, чтобы приложение использовало эвристический анализ при проверке веб-страниц на наличие фишинговых ссылок.

   В процессе эвристического анализа Kaspersky Endpoint Security анализирует активность, которую приложения производят в операционной системе. Эвристический анализ позволяет обнаруживать угрозы, записей о которых еще нет в базах Kaspersky Endpoint Security.

   Для проверки ссылок кроме антивирусных баз и эвристического анализа вы также можете использовать репутационные базы Kaspersky Security Network.

7. Сохраните внесенные изменения.

Как включить или выключить функцию Анти-Фишинг в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от веб-угроз**.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Анти-Фишинг** установите флажок **Проверять веб-адрес по базе фишинговых веб-адресов**, если вы хотите, чтобы компонент Защита от веб-угроз проверял ссылки по базам фишинговых веб-адресов. В состав базы фишинговых веб-адресов включены веб-адреса известных на настоящее время веб-сайтов, которые используются для фишинг-атак. Базу фишинговых веб-адресов специалисты "Лаборатории Касперского" пополняют веб-адресами, предоставленными международной организацией по борьбе с фишингом The Anti-Phishing Working Group. База фишинговых веб-адресов входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security.

5. Установите флажок **Использовать эвристический анализ**, если вы хотите, чтобы приложение использовало эвристический анализ при проверке веб-страниц на наличие фишинговых ссылок.

   В процессе эвристического анализа Kaspersky Endpoint Security анализирует активность, которую приложения производят в операционной системе. Эвристический анализ позволяет обнаруживать угрозы, записей о которых еще нет в базах Kaspersky Endpoint Security.

   Для проверки ссылок кроме антивирусных баз и эвристического анализа вы также можете использовать репутационные базы Kaspersky Security Network.

6. Сохраните внесенные изменения.

Формирование списка доверенных веб-адресов

Защита от веб-угроз, кроме вредоносных и фишинговых веб-сайтов, может заблокировать и другие веб-сайты. Например, Защита от веб-угроз блокирует HTTP-трафик, который не соответствует стандартам RFC. Вы можете сформировать список веб-адресов, содержанию которых вы доверяете. Компонент Защита от веб-угроз не анализирует информацию, поступающую с доверенных веб-адресов, на присутствие вирусов и других приложений, представляющих угрозу. Такая возможность может быть использована, например, в том случае, если компонент Защита от веб-угроз препятствует загрузке файла с известного вам веб-сайта.

Под веб-адресом подразумевается адрес как отдельной веб-страницы, так и веб-сайта.

Как добавить доверенный веб-адрес в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Базовая защита** → **Защита от веб-угроз**.
5. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
6. В открывшемся окне перейдите на вкладку **Доверенные веб-адреса**.
7. Установите флажок **Не проверять веб-трафик с доверенных веб-адресов**.

   Если флажок установлен, компонент Защита от веб-угроз не проверяет содержимое веб-страниц / веб-сайтов, адреса которых включены в список доверенных веб-адресов. Вы можете добавить в список доверенных веб-адресов как конкретный адрес веб-страницы / веб-сайта, так и маску адреса веб-страницы / веб-сайта.
8. Сформируйте список адресов веб-сайтов / веб-страниц, содержимому которых вы доверяете.

   Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

   Вы также можете импортировать список доверенных веб-адресов из XML-файла.
9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как добавить доверенный веб-адрес в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона**.
5. В открывшемся окне перейдите по ссылке **Веб-адреса**.

   Откроется окно со списком доверенных веб-адресов.

6. Сформируйте список адресов веб-сайтов / веб-страниц, содержимому которых вы доверяете.

   Kaspersky Endpoint Security поддерживает символы * и ? для ввода маски.

   Вы также можете импортировать список доверенных веб-адресов из JSON-файла.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как добавить доверенный веб-адрес в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от веб-угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. Установите флажок **Не проверять веб-трафик с доверенных веб-адресов** .

   Если флажок установлен, компонент Защита от веб-угроз не проверяет содержимое веб-страниц / веб-сайтов, адреса которых включены в список доверенных веб-адресов. Вы можете добавить в список доверенных веб-адресов как конкретный адрес веб-страницы / веб-сайта, так и маску адреса веб-страницы / веб-сайта.

5. Сформируйте список адресов веб-сайтов / веб-страниц, содержимому которых вы доверяете.

   Kaspersky Endpoint Security поддерживает символы * и ? для ввода маски.

   Вы также можете импортировать список доверенных веб-адресов из XML-файла.

6. Сохраните внесенные изменения.

В результате Защита от веб-угроз не будет проверять трафик доверенных веб-адресов. Пользователь всегда может открыть доверенный веб-сайт и загрузить файл с веб-сайта. Если получить доступ к веб-сайту не удалось, проверьте параметры компонентов Проверка защищенных соединений, Веб-Контроль и Контроль сетевых портов. Если Kaspersky Endpoint Security определяет загруженный с доверенного веб-сайта файл как вредоносный, вам нужно добавить этот файл в исключения.

Вы также можете сформировать общий список исключений защищенных соединений. В этом случае Kaspersky Endpoint Security не будет проверять HTTPS-трафик доверенных веб-адресов при работе компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль.

Экспорт и импорт списка доверенных веб-адресов

Вы можете экспортировать список доверенных веб-адресов в файл в формате XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных веб-адресов. Также вы можете использовать функцию экспорта / импорта для резервного копирования списка доверенных веб-адресов или для миграции списка на другой сервер.

Как экспортировать / импортировать список доверенных веб-адресов в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита** → **Защита от веб-угроз**.
4. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне перейдите на вкладку **Доверенные веб-адреса**.

6. Для экспорта списка доверенных веб-адресов выполните следующие действия:

   a. Выберите доверенные веб-адреса, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

   Если вы не выбрали ни одного доверенного веб-адреса, Kaspersky Endpoint Security экспортирует все веб-адреса.

   b. Нажмите на ссылку **Экспортировать**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список доверенных веб-адресов, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

   Kaspersky Endpoint Security экспортирует список доверенных веб-адресов в XML-файл.

7. Для импорта списка доверенных адресов выполните следующие действия:

   a. Нажмите на ссылку **Импортировать**.

   В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных адресов.

   b. Откройте файл.

   Если на компьютере уже есть список доверенных адресов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

8. Сохраните внесенные изменения.

Как экспортировать / импортировать список доверенных веб-адресов в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Защита от веб-угроз**.

5. Для экспорта списка исключений в блоке **Список правил** выполните следующие действия:

   a. Выберите доверенные веб-адреса, которые вы хотите экспортировать.

   b. Нажмите на кнопку → **Экспортировать**.

   Kaspersky Endpoint Security экспортирует список доверенных веб-адресов в JSON-файл в папку для загрузки по умолчанию.

6. Для импорта списка исключений в блоке **Список правил** выполните следующие действия:

   a. Нажмите на кнопку → **Импортировать**.

   В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список доверенных адресов.

b. Откройте файл.

Если на компьютере уже есть список доверенных адресов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.

7. Сохраните внесенные изменения.

Защита от почтовых угроз

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других приложений, представляющих угрозу. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Защита от почтовых угроз может проверять и получаемые, и отправляемые сообщения. Приложение поддерживает протоколы POP3, SMTP, IMAP, NNTP в следующих почтовых клиентах:

- Microsoft Office Outlook;
- Mozilla Thunderbird;
- Windows Mail;
- МойОфис Почта;
- Органайзер Р7-Офис.

Для проверки защищенного трафика в почтовых клиентах Mozilla Thunderbird, МойОфис Почта и Органайзер Р7-Офис вам нужно включить использование хранилища сертификатов Windows для приложений на основе технологий Mozilla.

Другие протоколы и почтовые клиенты Защита от почтовых угроз не поддерживает.

Защита от почтовых угроз не всегда может получить доступ к сообщениям на *уровне протокола* (например, при использовании решения Microsoft Exchange). Поэтому дополнительно в состав Защиты от почтовых угроз включено расширение для Microsoft Office Outlook. Расширение позволяет проверять сообщения на *уровне почтового клиента*. Расширение компонента Защита от почтовых угроз поддерживает работу с 32- и 64-разрядными версиями Outlook 2010, 2013, 2016, 2019, 2021, 2024, 365. На компьютерах с архитектурой Arm расширение компонента Защита от почтовых угроз поддерживает работу с 32- и 64-разрядной версией Outlook 2016 и Outlook 2021, 2024, 365 для Arm64.

Компонент Защита от почтовых угроз не проверяет сообщения, если почтовый клиент открыт в браузере.

При обнаружении вредоносного файла во вложении Kaspersky Endpoint Security добавляет информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

Включение и выключение Защиты от почтовых угроз

По умолчанию компонент Защита от почтовых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для работы Защиты от почтовых угроз приложение применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности почты **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского" (см. таблицу ниже). Вы можете выбрать один из предустановленных уровней безопасности почты или настроить уровень безопасности почты самостоятельно. После того как вы изменили параметры уровня безопасности почты, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности почты.

Работая с почтовым клиентом Mozilla Thunderbird, компонент Защита от почтовых угроз не проверяет на вирусы и другие приложения, представляющие угрозу, сообщения, передаваемые по протоколу IMAP, в случае если используются фильтры, перемещающие сообщения из папки входящих сообщений.

Как включить или выключить компонент Защита от почтовых угроз в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита → Защита от почтовых угроз**.
4. Используйте флажок **Защита от почтовых угроз**, чтобы включить или выключить компонент.
5. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:
     - **Высокий**. Уровень безопасности почты, при котором компонент Защита от почтовых угроз максимально контролирует сообщения. Компонент Защита от почтовых угроз проверяет входящие и исходящие сообщения электронной почты, а также выполняет глубокий эвристический анализ. Высокий уровень безопасности почты рекомендуется применять для работы в опасной среде. Примером опасной среды может служить подключение к одному из бесплатных почтовых сервисов из домашней сети, не обеспечивающей централизованной защиты почты.
     - **Рекомендуемый**. Уровень безопасности почты, обеспечивающий оптимальный баланс между производительностью приложения и безопасностью почты. Компонент Защита от почтовых угроз проверяет входящие и исходящие сообщения электронной почты, а также выполняет эвристический анализ среднего уровня. Этот уровень безопасности почты рекомендован для использования специалистами "Лаборатории Касперского". Значения параметров для рекомендуемого уровня безопасности см. в таблице ниже.
     - **Низкий**. Уровень безопасности почты, при котором компонент Защита от почтовых угроз проверяет только входящие сообщения электронной почты, а также выполняет поверхностный эвристический анализ и не проверяет архивы, вложенные в сообщения. Если используется этот уровень безопасности почты, компонент Защита от почтовых угроз проверяет сообщения электронной почты максимально быстро и затрачивает минимум ресурсов операционной системы. Низкий уровень безопасности почты рекомендуется применять для работы в хорошо защищенной среде. Примером такой среды может служить локальная сеть организации с централизованным обеспечением безопасности почты.

- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка** и задайте параметры работы компонента (см. таблицу ниже).

  Вы можете восстановить значения предустановленных уровней безопасности по кнопке **По умолчанию**.

6. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами:

   - **Лечить. Удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

   - **Лечить. Блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение пытается вылечить обнаруженный объект. Если вылечить объект не удалось, приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

   - **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить компонент Защита от почтовых угроз в Web Console

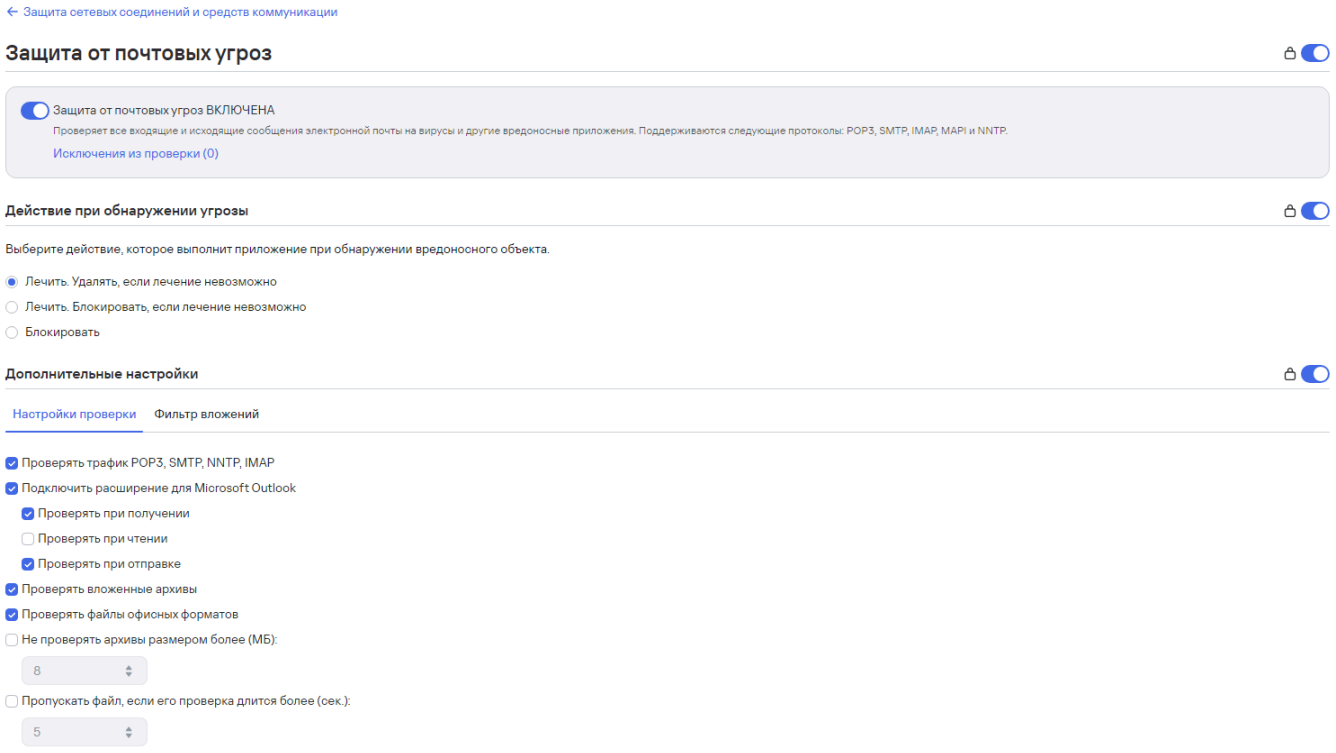
1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации → Защита от почтовых угроз**.



Параметры Защиты от почтовых угроз

5. Используйте переключатель **Защита от почтовых угроз ВКЛЮЧЕНА**, чтобы включить или выключить компонент.

6. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами:

   - **Лечить. Удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

   - **Лечить. Блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение пытается вылечить обнаруженный объект. Если вылечить объект не удалось, приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

   - **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

7. Если требуется, настройте дополнительные параметры Защиты от почтовых угроз.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить компонент Защита от почтовых угроз в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от почтовых угроз**.
3. Используйте переключатель **Защита от почтовых угроз**, чтобы включить или выключить компонент.
4. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:

   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:

     - **Высокий**. Уровень безопасности почты, при котором компонент Защита от почтовых угроз максимально контролирует сообщения. Компонент Защита от почтовых угроз проверяет входящие и исходящие сообщения электронной почты, а также выполняет глубокий эвристический анализ. Высокий уровень безопасности почты рекомендуется применять для работы в опасной среде. Примером опасной среды может служить подключение к одному из бесплатных почтовых сервисов из домашней сети, не обеспечивающей централизованной защиты почты.

     - **Рекомендуемый**. Уровень безопасности почты, обеспечивающий оптимальный баланс между производительностью приложения и безопасностью почты. Компонент Защита от почтовых угроз проверяет входящие и исходящие сообщения электронной почты, а также выполняет эвристический анализ среднего уровня. Этот уровень безопасности почты рекомендован для использования специалистами "Лаборатории Касперского". Значения параметров для рекомендуемого уровня безопасности см. в таблице ниже.

     - **Низкий**. Уровень безопасности почты, при котором компонент Защита от почтовых угроз проверяет только входящие сообщения электронной почты, а также выполняет поверхностный эвристический анализ и не проверяет архивы, вложенные в сообщения. Если используется этот уровень безопасности почты, компонент Защита от почтовых угроз проверяет сообщения электронной почты максимально быстро и затрачивает минимум ресурсов операционной системы. Низкий уровень безопасности почты рекомендуется применять для работы в хорошо защищенной среде. Примером такой среды может служить локальная сеть организации с централизованным обеспечением безопасности почты.

   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента (см. таблицу ниже).

     Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности**.

5. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами:

   - **Лечить. Удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

   - **Лечить. Блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение пытается вылечить обнаруженный объект. Если вылечить объект не удалось, приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

   - **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

6. Сохраните внесенные изменения.

Параметры Защиты от почтовых угроз, рекомендованные специалистами "Лаборатории Касперского", (рекомендованный уровень безопасности)

Параметр	Значение	Описание
Область защиты	**Входящие и исходящие сообщения**	*Область защиты* – это объекты, которые проверяет компонент во время своей работы: входящие и исходящие сообщения или только входящие сообщения. Для защиты компьютеров достаточно проверять только входящие сообщения. Вы можете включить проверку исходящих сообщений для предотвращения отправки зараженных файлов в архивах. Вы также можете включить проверку исходящих сообщений, если вы хотите запретить обмен файлами определенных форматов, например, аудио или видео.
Подключить расширение для Microsoft Outlook	**Вкл**	Если флажок установлен, включена проверка сообщений электронной почты, передающихся по протоколам POP3, SMTP, NNTP, IMAP на стороне расширения, интегрированного в Microsoft Outlook. В случае проверки почты с помощью расширения для Microsoft Outlook рекомендуется использовать режим кеширования Exchange (Cached Exchange Mode). Более подробную информацию о режиме кеширования Exchange и рекомендации по его использованию вы можете найти в базе знаний Microsoft .
Проверять вложенные архивы	**Вкл**	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять вложенные файлы форматов Microsoft Office	**Вкл**	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Фильтр вложений	**Переименовывать вложения указанных типов**	Если выбран этот вариант, компонент Защита от почтовых угроз заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_). Таким образом, чтобы открыть файл, пользователю нужно переименовать файл.

Параметр	Значение	Описание
Эвристический анализ	**Средний**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**	При обнаружении зараженного объекта во входящем или исходящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

Изменение действия над зараженными сообщениями электронной почты

По умолчанию компонент Защита от почтовых угроз автоматически пытается вылечить все обнаруженные зараженные сообщения электронной почты. Если лечение невозможно, то компонент Защита от почтовых угроз удаляет зараженные сообщения электронной почты.

Чтобы изменить действие над зараженными сообщениями электронной почты, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от почтовых угроз**.
3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое выполняет Kaspersky Endpoint Security при обнаружении зараженного сообщения:
   - **Лечить. Удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.
   - **Лечить. Блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение пытается вылечить обнаруженный объект. Если вылечить объект не удалось, приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.
   - **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

4. Сохраните внесенные изменения.

Формирование области защиты компонента Защита от почтовых угроз

Область защиты – это объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты компонента Защита от почтовых угроз являются параметры интеграции компонента Защита от почтовых угроз в почтовые клиенты, тип сообщений электронной почты и почтовые протоколы, трафик которых проверяет компонент Защита от почтовых угроз. По умолчанию Kaspersky Endpoint Security проверяет как входящие, так и исходящие сообщения электронной почты, трафик почтовых протоколов POP3, SMTP, NNTP и IMAP, а также интегрируется в почтовый клиент Microsoft Office Outlook.

Чтобы сформировать область защиты компонента Защита от почтовых угроз, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от почтовых угроз**.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Область защиты** выберите сообщения для проверки:

   - **Входящие и исходящие сообщения**.
   - **Только входящие сообщения**.

   Для защиты компьютеров достаточно проверять только входящие сообщения. Вы можете включить проверку исходящих сообщений для предотвращения отправки зараженных файлов в архивах. Вы также можете включить проверку исходящих сообщений, если вы хотите запретить обмен файлами определенных форматов, например, аудио или видео.

   Если вы выбираете проверку только входящих сообщений, рекомендуется однократно проверить все исходящие сообщения, поскольку существует вероятность того, что на вашем компьютере есть почтовые черви, которые используют электронную почту в качестве канала распространения. Это позволит избежать проблем, связанных с неконтролируемой рассылкой зараженных сообщений с вашего компьютера.

5. В блоке **Встраивание в операционную систему** выполните следующие действия:

   - Установите флажок **Проверять трафик POP3, SMTP, NNTP, IMAP**, если вы хотите, чтобы компонент Защита от почтовых угроз проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя.

     Снимите флажок **Проверять трафик POP3, SMTP, NNTP, IMAP**, если вы хотите, чтобы компонент Защита от почтовых угроз не проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя. В этом случае сообщения проверяет расширение компонента Защита от почтовых угроз, встроенное в почтовый клиент Microsoft Office Outlook, после их получения на компьютере пользователя, если установлен флажок **Подключить расширение для Microsoft Outlook**.

Если вы используете почтовый клиент, отличный от Microsoft Office Outlook, то при снятом флажке **Проверять трафик POP3, SMTP, NNTP, IMAP** компонент Защита от почтовых угроз не проверяет сообщения, передающиеся по почтовым протоколам POP3, SMTP, NNTP и IMAP.

- Установите флажок **Подключить расширение для Microsoft Outlook**, если вы хотите открыть доступ к настройке параметров компонента Защита от почтовых угроз из приложения Microsoft Office Outlook и включить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя с помощью расширения, интегрированного в приложение Microsoft Office Outlook.

  Снимите флажок **Подключить расширение для Microsoft Outlook**, если вы хотите закрыть доступ к настройке параметров компонента Защита от почтовых угроз из приложения Microsoft Office Outlook и выключить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя с помощью расширения, интегрированного в приложение Microsoft Office Outlook.

  Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft Office Outlook во время установки Kaspersky Endpoint Security.

6. Сохраните внесенные изменения.

Проверка составных файлов, вложенных в сообщения электронной почты

Вы можете включить или выключить проверку объектов, вложенных в сообщения, ограничить максимальный размер проверяемых объектов, вложенных в сообщения, и максимальную длительность проверки объектов, вложенных в сообщения.

Чтобы настроить проверку составных файлов, вложенных в сообщения электронной почты, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от почтовых угроз**.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Проверка составных файлов** настройте параметры проверки:

   - **Проверять вложенные файлы форматов Microsoft Office**. Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.

   - **Проверять вложенные архивы**. Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).

     Если во время проверки приложение обнаружило в тексте сообщения пароль к архиву, пароль будет использован для проверки содержания этого архива на наличие вредоносных приложений. Пароль при этом не сохраняется. При проверке архива выполняется его распаковка. Если во время распаковки архива произошел сбой в работе приложения, вы можете вручную удалить файлы, которые при распаковке сохраняются по следующему пути: %systemroot%\temp. Файлы имеют префикс PR.

   - **Не проверять архивы размером более N МБ (от 1 до 9999)**. Если флажок установлен, компонент Защита от почтовых угроз исключает из проверки вложенные в сообщения электронной почты архивы, размер которых больше заданного. Если флажок снят, компонент Защита от почтовых угроз проверяет архивы любого размера, вложенные в сообщения электронной почты.

   - **Ограничить время проверки архива до N сек (от 1 до 9999)**. Если флажок установлен, то время проверки архивов, вложенных в сообщения электронной почты, ограничено указанным периодом.

5. Сохраните внесенные изменения.

Фильтрация вложений в сообщениях электронной почты

Фильтр вложений не применяется для исходящих сообщений электронной почты.

Вредоносные приложения могут распространяться в виде вложений в сообщениях электронной почты. Вы можете настроить фильтрацию по типу вложений в сообщениях, чтобы автоматически переименовывать или удалять файлы указанных типов. Переименовав вложение определенного типа, Kaspersky Endpoint Security может защитить ваш компьютер от автоматического запуска вредоносного приложения.

Как настроить фильтрацию вложений в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите папку **Политики**.

3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

4. В окне политики выберите **Базовая защита → Защита от почтовых угроз**.

5. Нажмите на кнопку **Настройка**.

6. В открывшемся окне выберите вкладку **Фильтр вложений**.

7. На вкладке выполните одно из следующих действий:

   - **Не применять фильтр**. Если выбран этот вариант, компонент Защита от почтовых угроз не фильтрует файлы, вложенные в сообщения электронной почты.

   - **Переименовывать вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_). Таким образом, чтобы открыть файл, пользователю нужно переименовать файл.

   - **Удалять вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз удаляет из сообщений электронной почты вложенные файлы указанных типов.

8. Если на предыдущем шаге инструкции вы выбрали вариант **Переименовывать вложения указанных типов** или вариант **Удалять вложения указанных типов**, установите флажки напротив нужных типов файлов.

9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить фильтрацию вложений в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации → Защита от почтовых угроз**.

5. В разделе **Дополнительные настройки** выберите вкладку **Фильтр вложений**.

6. На вкладке выполните одно из следующих действий:

   - **Не изменять вложения**. Если выбран этот вариант, компонент Защита от почтовых угроз не фильтрует файлы, вложенные в сообщения электронной почты.

   - **Переименовывать вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_). Таким образом, чтобы открыть файл, пользователю нужно переименовать файл.

   - **Удалять вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз удаляет из сообщений электронной почты вложенные файлы указанных типов.

7. Если на предыдущем шаге инструкции вы выбрали вариант **Переименовывать вложения указанных типов** или вариант **Удалять вложения указанных типов**, установите флажки напротив нужных типов файлов.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить фильтрацию вложений в интерфейсе приложений

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от почтовых угроз**.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Фильтр вложений** выполните одно из следующих действий:

   - **Не применять фильтр**. Если выбран этот вариант, компонент Защита от почтовых угроз не фильтрует файлы, вложенные в сообщения электронной почты.

   - **Переименовывать вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_). Таким образом, чтобы открыть файл, пользователю нужно переименовать файл.

   - **Удалять вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз удаляет из сообщений электронной почты вложенные файлы указанных типов.

5. Если на предыдущем шаге инструкции вы выбрали вариант **Переименовывать вложения указанных типов** или вариант **Удалять вложения указанных типов**, установите флажки напротив нужных типов файлов.

6. Сохраните внесенные изменения.

Экспорт и импорт списка расширений для фильтра вложений

Вы можете экспортировать список расширений для работы фильтра вложений в файл в формате XML. Вы можете использовать функцию экспорта / импорта для резервного копирования списка расширений или для миграции списка на другой сервер.

Как экспортировать / импортировать список расширений для работы фильтра вложений в Консоли администрирования (MMC)

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации → Защита от почтовых угроз**.

5. Для экспорта списка расширений в блоке **Фильтр вложений** выполните следующие действия:

   a. Выберите расширения, которые вы хотите экспортировать.

   b. Нажмите на ссылку **Экспорт**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список расширений, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список расширений в XML-файл.

6. Для импорта списка расширений в блоке **Фильтр вложений** выполните следующие действия:

   a. Нажмите на ссылку **Импорт**.

   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список расширений.

   c. Откройте файл.

      Если на компьютере уже есть список расширений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

7. Сохраните внесенные изменения.

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Базовая защита → Защита от почтовых угроз**.

4. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне выберите вкладку **Фильтр вложений**.

6. Для экспорта списка расширений выполните следующие действия:

   a. Выберите расширения, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

   b. Нажмите на ссылку **Экспорт**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список расширений, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список расширений в XML-файл.

7. Для импорта списка расширений выполните следующие действия:

   a. Нажмите на ссылку **Импорт**.

   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список расширений.

   c. Откройте файл.

      Если на компьютере уже есть список расширений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

8. Сохраните внесенные изменения.

Проверка почты в Microsoft Office Outlook

Во время установки Kaspersky Endpoint Security в приложение Microsoft Office Outlook (далее также "Outlook") встраивается расширение компонента Защита от почтовых угроз. Расширение предназначено для проверки сообщений на уровне почтового клиента, а не протокола. Расширение позволяет проверять в почтовом клиенте не только сообщения, но и объекты полученные через интерфейс MAPI из хранилищ Microsoft Exchange (например, объекты в Календаре).

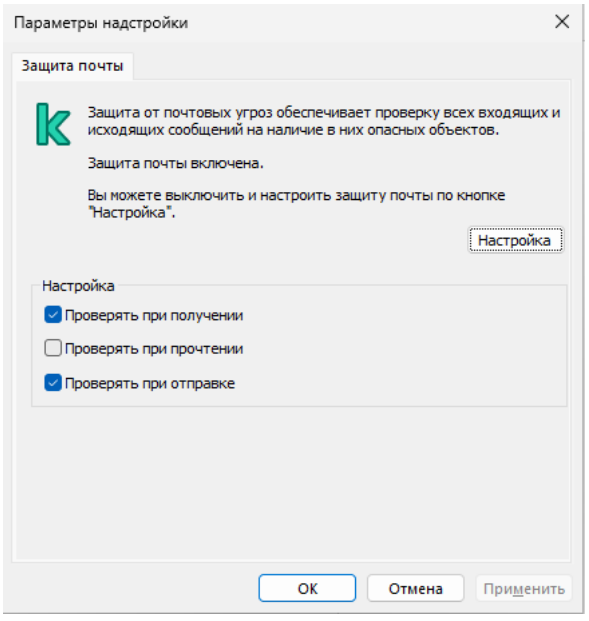
Вы можете перейти к настройке параметров компонента Защита от почтовых угроз из приложения Outlook, а также указать, в какой момент проверять сообщения электронной почты на присутствие вирусов и других приложений, представляющих угрозу.

Расширение компонента Защита от почтовых угроз поддерживает работу с 32- и 64-разрядными версиями Outlook 2010, 2013, 2016, 2019, 2021, 2024, 365.

На компьютерах с архитектурой Arm расширение компонента Защита от почтовых угроз поддерживает работу с 32- и 64-разрядной версией Outlook 2016 и Outlook 2021, 2024, 365 для Arm64.

В приложении Outlook входящие сообщения сначала проверяет компонент Защита от почтовых угроз (если в интерфейсе приложения Kaspersky Endpoint Security включена проверка трафика POP3 / SMTP / NNTP / IMAP), затем входящие сообщения проверяет расширение компонента Защита от почтовых угроз для Outlook. Если компонент Защита от почтовых угроз обнаруживает в сообщении вредоносный объект, он уведомляет вас об этом.

Настройка параметров компонента Защита от почтовых угроз из приложения Outlook доступна в том случае, если в интерфейсе приложения Kaspersky Endpoint Security подключено расширение для Microsoft Outlook (см. рис. ниже).



Параметры компонента Защита от почтовых угроз из приложения Outlook

Исходящие сообщения сначала проверяет расширение компонента Защита от почтовых угроз для Outlook, а затем проверяет компонент Защита от почтовых угроз.

В случае проверки почты с помощью расширения компонента Защита от почтовых угроз для Outlook рекомендуется использовать режим кеширования сервера Exchange (Use Cached Exchange Mode). Более подробную информацию о режиме кеширования Exchange и рекомендации по его использованию вы можете найти в базе знаний Microsoft.

Как настроить режим работы расширения компонента Защита от почтовых угроз для Outlook в Консоли администрирования (MMC)

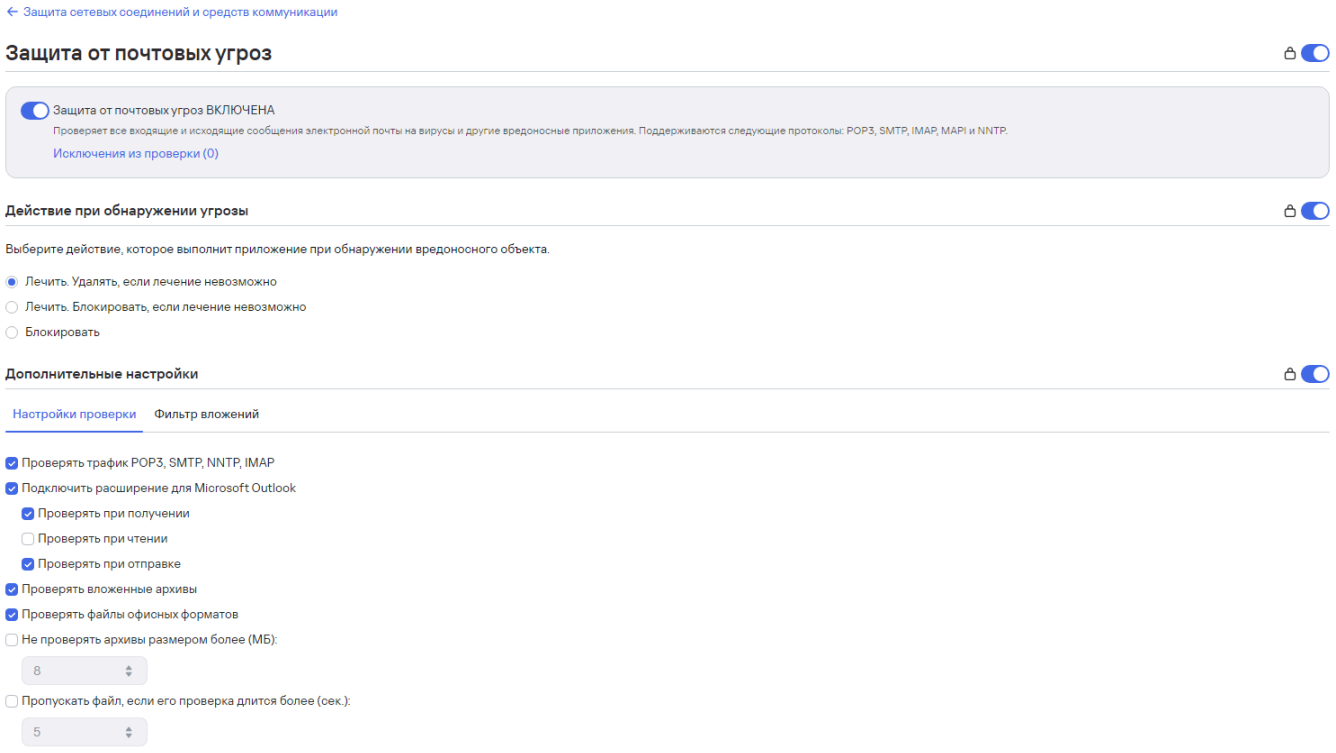
1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Базовая защита** → **Защита от почтовых угроз**.
5. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
6. В открывшемся окне в блоке **Встраивание в систему** установите флажок **Подключить расширение для Microsoft Outlook**.
7. Нажмите на кнопку **Настройка**.
8. В окне **Защита почты** выполните следующие действия:
   - Установите флажок **Проверять при получении**, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло входящие сообщения в момент их поступления в почтовый ящик.
   - Установите флажок **Проверять при прочтении**, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло входящие сообщения в тот момент, когда пользователь открывает их для чтения.
   - Установите флажок **Проверять при отправке**, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло исходящие сообщения в момент их отправки.
9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить режим работы расширения компонента Защита от почтовых угроз для Outlook в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации → Защита от почтовых угроз**.



Параметры Защиты от почтовых угроз

5. В блоке **Дополнительные настройки** выберите вкладку **Настройки проверки**.

6. Установите флажок **Подключить расширение для Microsoft Outlook**.

7. Настройте режим работы расширения:

   - Установите флажок **Проверять при получении**, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло входящие сообщения в момент их поступления в почтовый ящик.

   - Установите флажок **Проверять при чтении**, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло входящие сообщения в тот момент, когда пользователь открывает их для чтения.

   - Установите флажок **Проверять при отправке**, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло исходящие сообщения в момент их отправки.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Проверка почты в Thunderbird, МойОфис, Р7-Офис

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других приложений, представляющих угрозу. Для почтовых клиентов Mozilla Thunderbird, МойОфис Почта и Органайзер Р7-Офис приложение получает доступ к сообщениям только на *уровне протокола* (POP3, SMTP, IMAP, NNTP).

Для проверки защищенного трафика в почтовых клиентах Mozilla Thunderbird, МойОфис Почта и Органайзер Р7-Офис вам нужно включить использование хранилища сертификатов Windows для приложений на основе технологий Mozilla.

Компонент Защита от почтовых угроз не проверяет сообщения, если почтовый клиент открыт в браузере.

Защита от почтовых угроз в режиме реального времени

Защита от почтовых угроз может проверять и получаемые, и отправляемые сообщения. По умолчанию компонент Защита от почтовых угроз автоматически пытается вылечить все обнаруженные зараженные сообщения электронной почты. Если лечение невозможно, то компонент Защита от почтовых угроз удаляет зараженные сообщения электронной почты. При обнаружении вредоносного файла во вложении Kaspersky Endpoint Security добавляет информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

Работая с почтовым клиентом Mozilla Thunderbird, компонент Защита от почтовых угроз не проверяет на вирусы и другие приложения, представляющие угрозу, сообщения, передаваемые по протоколу IMAP, в случае если используются фильтры, перемещающие сообщения из папки входящих сообщений.

Поиск вредоносного ПО в почтовых базах данных

Защита от почтовых угроз предотвращает заражение компьютера на уровне протокола, но если компьютер был заражен до установки Kaspersky Endpoint Security, то приложение может обнаружить угрозу в почтовых базах данных с помощью задачи *Поиск вредоносного ПО*. Приложение не выполняет лечение и удаление зараженных файлов в почтовых базах данных, независимо от настроек задачи. Это связано с тем, что Kaspersky Endpoint Security не разбирает сообщения из Thunderbird, МойОфис и Р7-Офис на составные части (заголовок, тело, вложения) так же, как сообщения из Microsoft Office Outlook. Приложение только добавляет информацию об обнаруженных объектах в список активных угроз.

Для устранения активных угроз вам нужно выполнить следующие действия:

1. Найдите и удалите сообщение с обнаруженным объектом в интерфейсе почтового клиента вручную.

   Приложение показывает информацию об обнаруженном объекте в списке активных угроз.

   Пример карточки обнаруженного объекта:

	HEUR:Trojan.PDF.Phish.gen Объект: `C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. Выполните операцию сжатия почтовых баз данных.

   При удалении сообщения в интерфейсе почтовый клиент только ставит отметку об удалении. Почтовый клиент удаляет сообщение только после сжатия базы данных. Подробнее о сжатии почтовых баз данных см. в справке к почтовому клиенту (например, Mozilla Thunderbird).

3. Запустите задачу *Поиск вредоносного ПО* повторно и убедитесь, что угроза устранена.

Если удаление писем с зараженными файлами по какой-то причине в данный момент недоступно, вы можете обработать данные угрозы в интерфейсе Kaspersky Endpoint Security. Для файлов почтовых клиентов вам доступны два способа обработки угрозы: **Игнорировать** и **Добавить в исключения**. Чтобы при повторной проверке приложение не добавляло данные объекты в список активных угроз, добавьте их в список исключений из проверки.

Защита от сетевых угроз

Компонент *Защита от сетевых угроз* (также Intrusion Detection System (IDS) – система обнаружения вторжений) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, приложение блокирует сетевое соединение с атакующим компьютером. Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах приложения. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей приложения.

Включение и выключение Защиты от сетевых угроз

По умолчанию компонент Защита от сетевых угроз включен и работает в оптимальном режиме. Kaspersky Endpoint Security отслеживает во входящем сетевом трафике активность, характерную для сетевых атак, и блокирует атаки.

Как включить или выключить Защиту от сетевых угроз в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита → Защита от сетевых угроз**.
4. Используйте флажок **Защита от сетевых угроз**, чтобы включить или выключить компонент.
5. Для применения политики на компьютерах закройте замки , сохраните внесенные изменения.

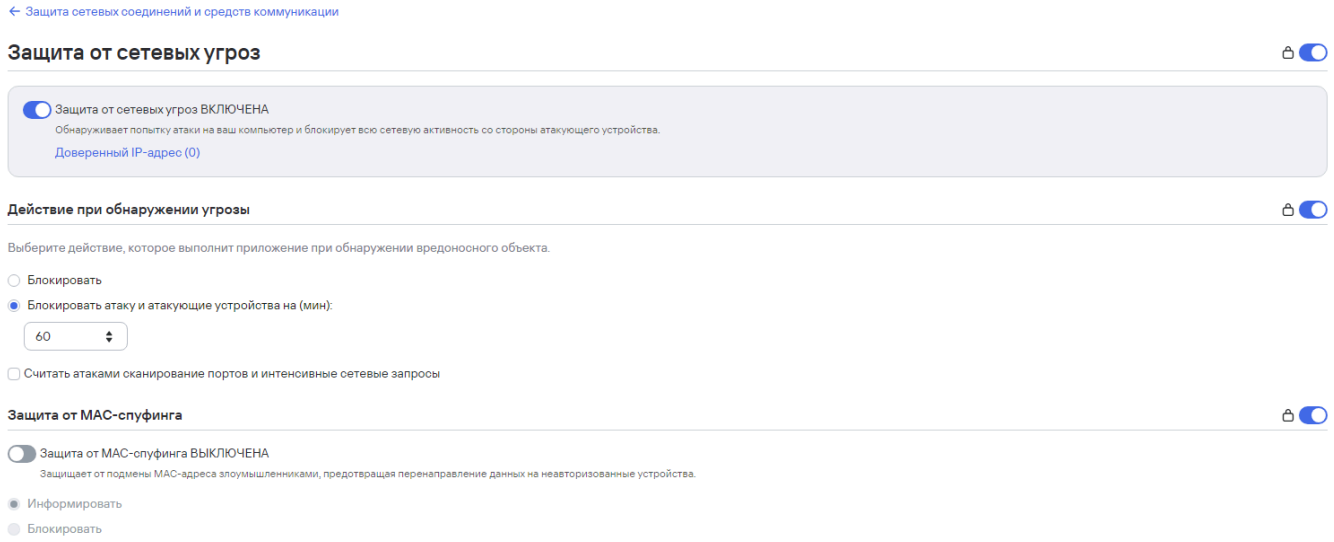
Как включить или выключить Защиту от сетевых угроз в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации → Защита от сетевых угроз**.



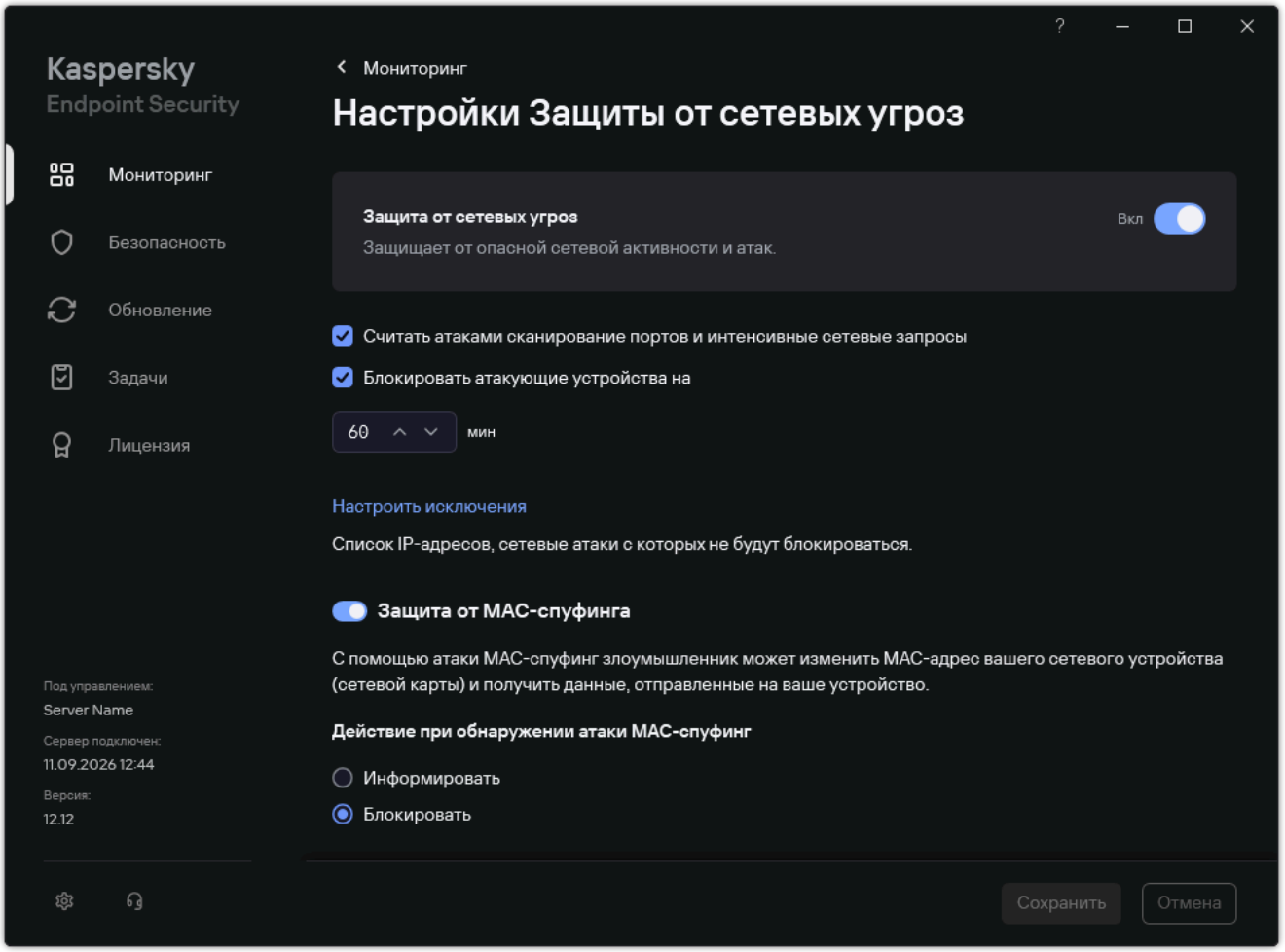
Параметры Защиты от сетевых угроз

5. Используйте переключатель **Защита от сетевых угроз ВКЛЮЧЕНА**, чтобы включить или выключить компонент.

6. Сохраните внесенные изменения.

Как включить или выключить Защиту от сетевых угроз в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.



Параметры Защиты от сетевых угроз

3. Используйте переключатель **Защита от сетевых угроз**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

Блокирование атакующего компьютера

Если компонент Защита от сетевых угроз включен, Kaspersky Endpoint Security автоматически блокирует сетевые атаки. Дополнительно приложение может заблокировать атакующий компьютер и ограничить отправку сетевых пакетов на определенный период времени. По умолчанию Kaspersky Endpoint Security блокирует компьютер на один час.

Как заблокировать атакующий компьютер в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита** → **Защита от сетевых угроз**.

4. В блоке **Настройки защиты от сетевых угроз** установите флажок **Блокировать атакующие устройства на N мин**.

   Если функция включена, компонент Защита от сетевых угроз добавляет атакующий компьютер в список блокирования. Это означает, что компонент Защита от сетевых угроз блокирует сетевое соединение с атакующим компьютером после первой попытки сетевой атаки в течение заданного времени, чтобы автоматически защитить компьютер пользователя от возможных будущих сетевых атак с этого адреса. Минимальное время, на которое атакующий компьютер можно добавить в список блокирования, составляет одну минуту. Максимальное – 999 минут.

5. Измените время блокирования атакующего компьютера в поле, расположенном справа от флажка **Блокировать атакующие устройства на N мин**.

6. Сохраните внесенные изменения.

Как заблокировать атакующий компьютер в Web Console

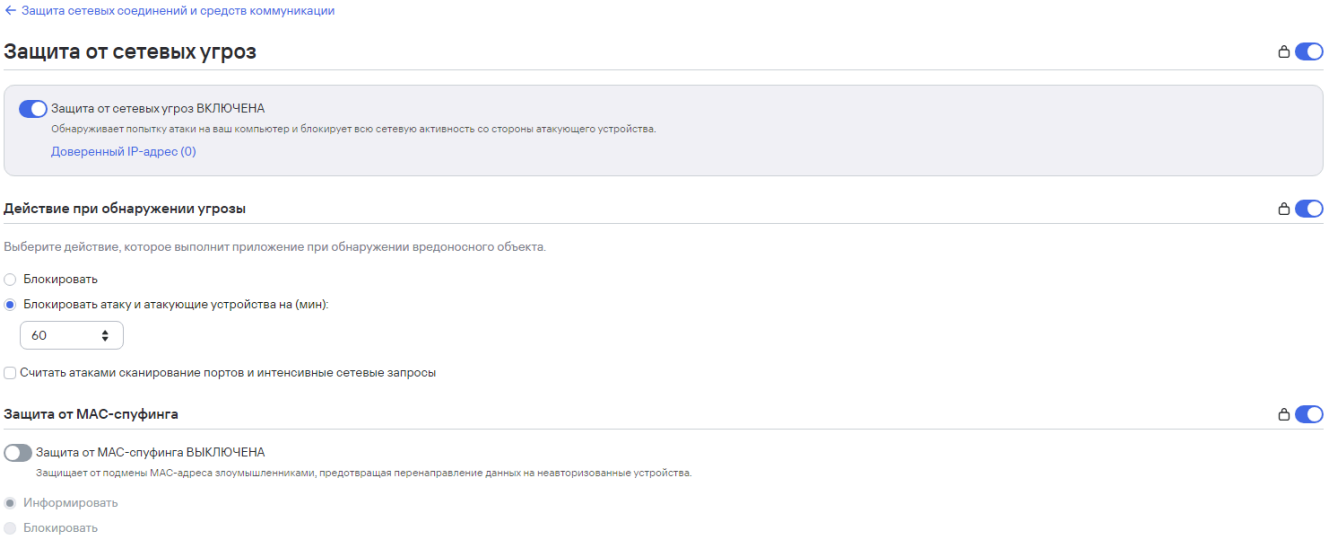
1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Защита от сетевых угроз**.



Параметры Защиты от сетевых угроз

5. В блоке **Действие при обнаружении угрозы** установите флажок **Блокировать атаку и атакующие устройства на (мин)**.

   Если функция включена, компонент Защита от сетевых угроз добавляет атакующий компьютер в список блокирования. Это означает, что компонент Защита от сетевых угроз блокирует сетевое соединение с атакующим компьютером после первой попытки сетевой атаки в течение заданного времени, чтобы автоматически защитить компьютер пользователя от возможных будущих сетевых атак с этого адреса. Минимальное время, на которое атакующий компьютер можно добавить в список блокирования, составляет одну минуту. Максимальное – 999 минут.

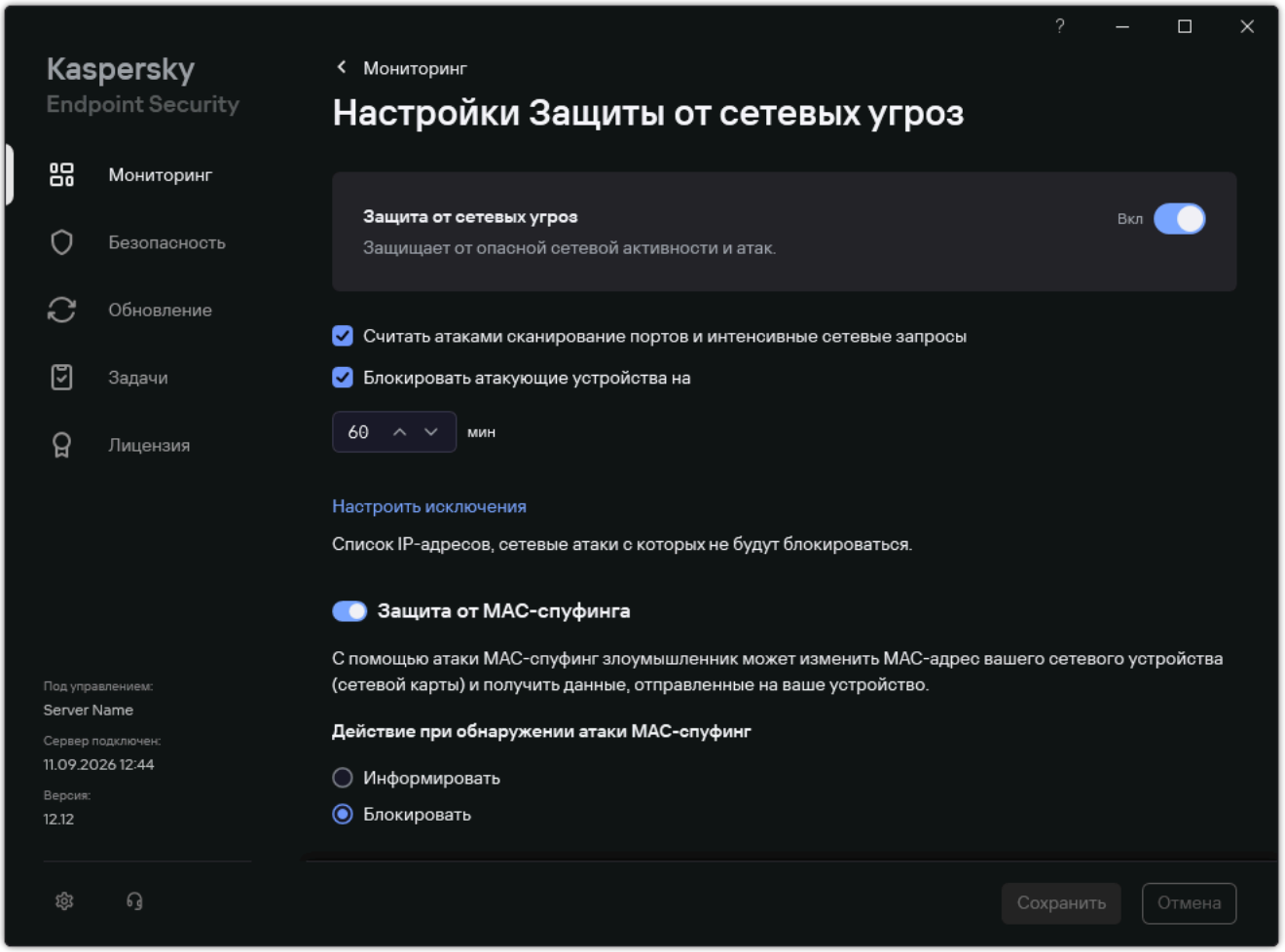
6. Измените время блокирования атакующего компьютера.

7. Сохраните внесенные изменения.

Как заблокировать атакующий компьютер в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.



Параметры Защиты от сетевых угроз

3. Включите переключатель **Блокировать атакующие устройства на N мин**.

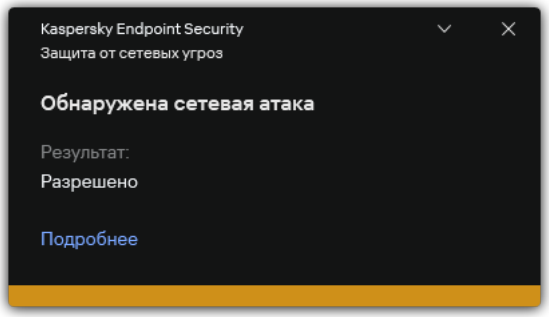
   Если функция включена, компонент Защита от сетевых угроз добавляет атакующий компьютер в список блокирования. Это означает, что компонент Защита от сетевых угроз блокирует сетевое соединение с атакующим компьютером после первой попытки сетевой атаки в течение заданного времени, чтобы автоматически защитить компьютер пользователя от возможных будущих сетевых атак с этого адреса. Минимальное время, на которое атакующий компьютер можно добавить в список блокирования, составляет одну минуту. Максимальное – 999 минут.

4. Измените время блокирования атакующего компьютера в поле, расположенном снизу от переключателя **Блокировать атакующие устройства на N мин**.

5. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security, обнаружив попытку сетевой атаки на компьютер пользователя, блокирует все соединения с атакующим компьютером. Kaspersky Endpoint Security создает событие *Обнаружена сетевая атака*. Событие содержит информацию об атакующем компьютере: IP- и MAC-адреса.

MAC-адрес атакующего компьютера вы можете просмотреть в интерфейсе приложения и в консоли Kaspersky Security Center версии 15.1 и выше.



Уведомление об обнаружении сетевой атаки

Kaspersky Endpoint Security разблокирует компьютер по истечению заданного периода времени. В консоли Kaspersky Security Center нет инструментов мониторинга заблокированных компьютеров кроме событий *Обнаружена сетевая атака* в отчете. Вы можете просмотреть список заблокированных компьютеров только в интерфейсе приложения. Для этого предназначен инструмент *Мониторинг сети*. Также с помощью инструмента Мониторинг сети вы можете разблокировать компьютер.

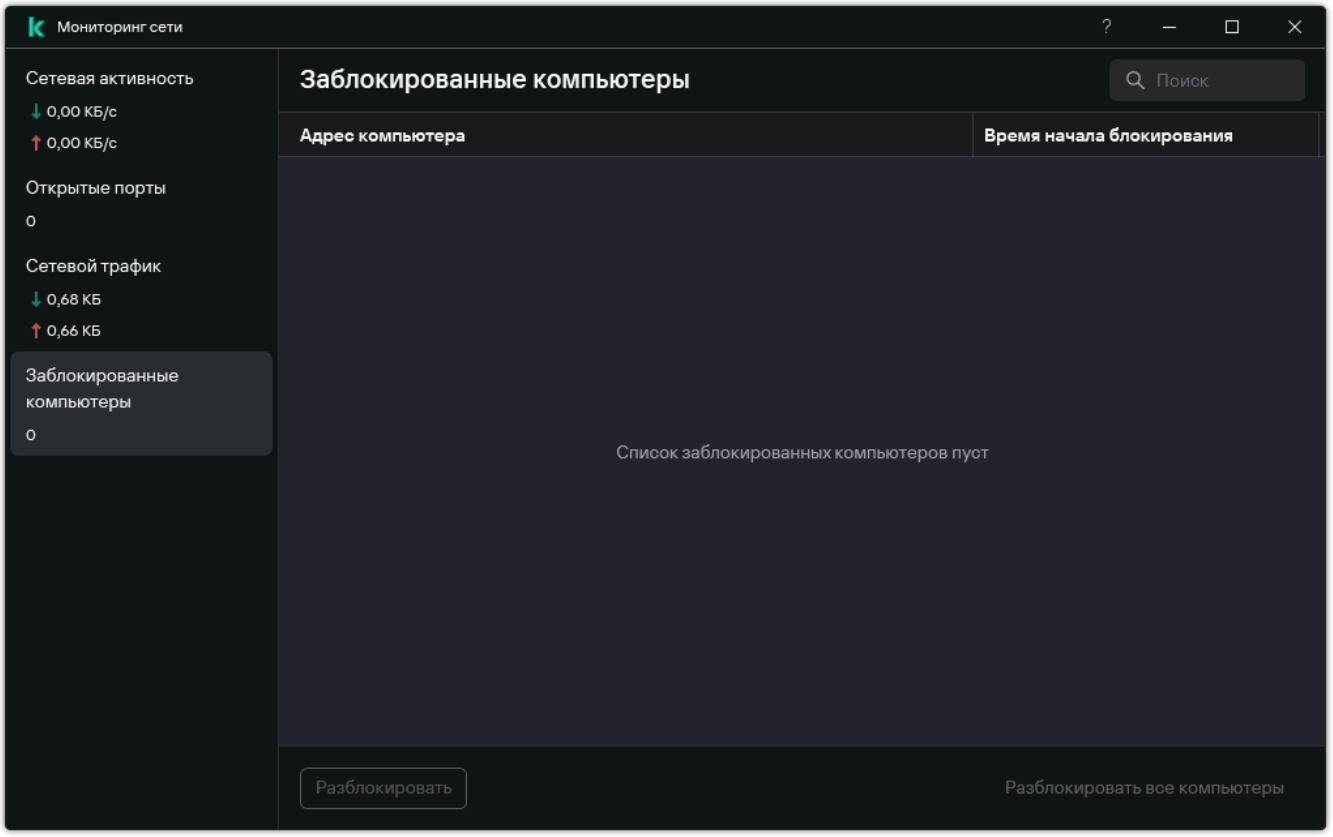
Чтобы разблокировать компьютер, выполните следующие действия:

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Мониторинг сети**.
2. Перейдите на вкладку **Заблокированные компьютеры**.

   Откроется список заблокированных компьютеров (см. рис. ниже).

   Kaspersky Endpoint Security очищает список блокирования при перезапуске приложения и при изменении параметров Защиты от сетевых угроз.

3. Выберите компьютер, который вы хотите разблокировать и нажмите **Разблокировать**.



Список заблокированных компьютеров

Настройка адресов исключений из блокирования

Kaspersky Endpoint Security может распознать сетевую атаку и заблокировать безопасное сетевое соединение, по которому передается большое количество пакетов (например, от камер наблюдения). Для работы с доверенными устройствами вы можете добавить IP-адреса этих устройств в список исключений. Также вы можете выбрать протокол и порт, по которым передаются данные, чтобы разрешить отдельную сетевую активность.

Как настроить адреса исключений из блокирования в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Базовая защита → Защита от сетевых угроз**.
5. В блоке **Настройки защиты от сетевых угроз** нажмите на кнопку **Исключения**.
6. В открывшемся окне нажмите на кнопку **Добавить**.
7. Введите IP-адрес компьютера, сетевые атаки с которого не должны блокироваться.

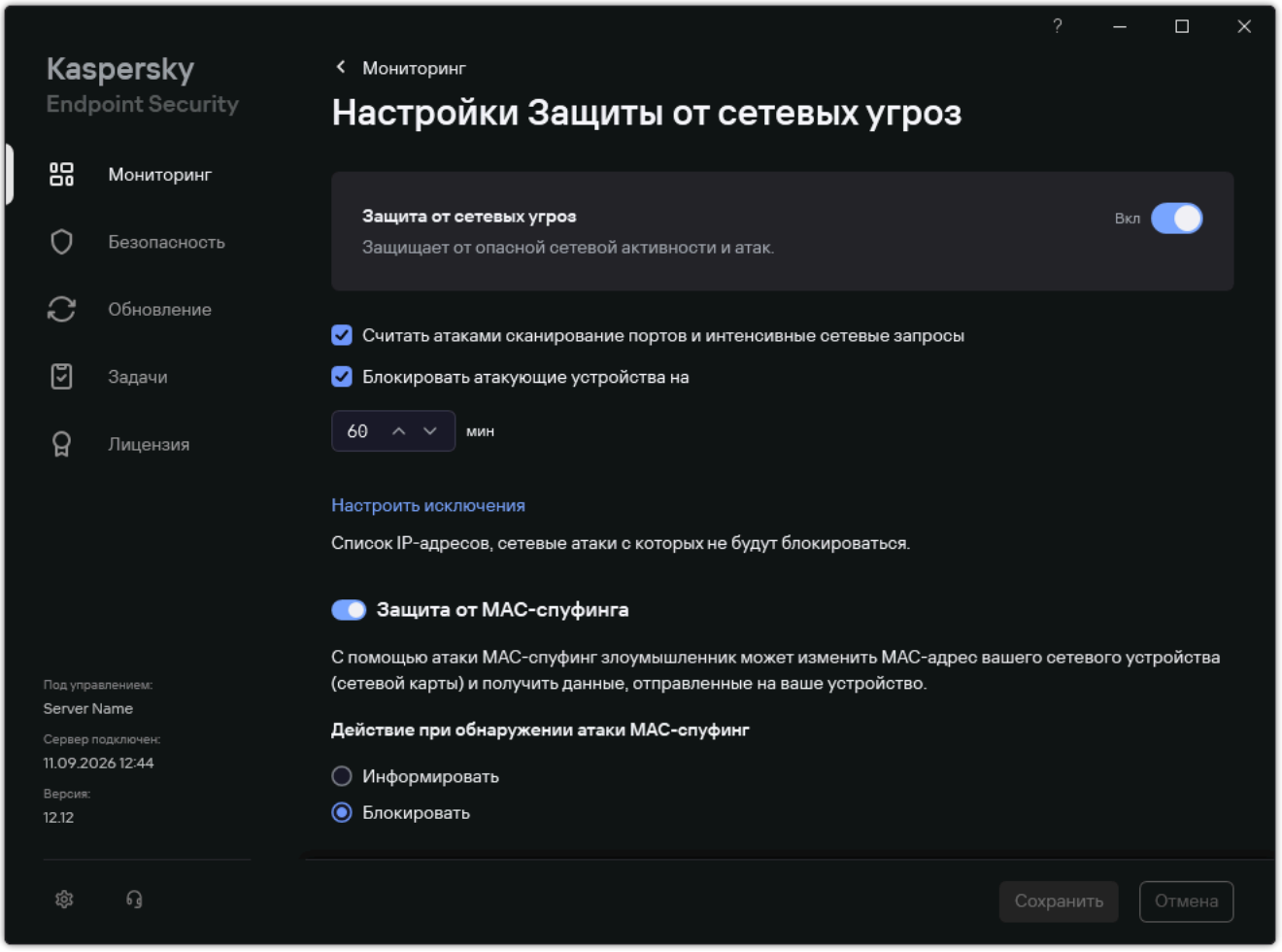
   Если требуется, выберите протокол и порты, по которым передаются данные.
8. Для применения политики на компьютерах закройте замки , сохраните внесенные изменения.

Как настроить адреса исключений из блокирования в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона**.
5. В открывшемся окне перейдите по ссылке **IP-адреса**.
   Откроется окно со списком доверенных IP-адресов.
6. В открывшемся окне нажмите на кнопку **Добавить**.
7. Введите IP-адрес компьютера, сетевые атаки с которого не должны блокироваться.
   Если требуется, укажите подсеть.
8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить адреса исключений из блокирования в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.



Параметры Защиты от сетевых угроз

3. Нажмите на ссылку **Настроить исключения**.

4. В открывшемся окне нажмите на кнопку **Добавить**.

5. Введите IP-адрес компьютера, сетевые атаки с которого не должны блокироваться.

   Если требуется, выберите протокол и порты, по которым передаются данные.

6. Сохраните внесенные изменения.

Экспорт и импорт списка исключений из блокирования

Вы можете экспортировать список исключений в файл формата XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных адресов. Также вы можете использовать функцию экспорта / импорта для резервного копирования списка исключений или для миграции списка на другой сервер.

Как экспортировать / импортировать список исключений в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Базовая защита** → **Защита от сетевых угроз**.

4. В блоке **Настройки защиты от сетевых угроз** нажмите на кнопку **Исключения**.

5. Для экспорта списка исключений выполните следующие действия:

   a. Выберите исключения, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

      Если вы не выбрали ни одного исключения, Kaspersky Endpoint Security экспортирует все исключения.

   b. Нажмите на кнопку → **Экспортировать**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список исключений, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список исключений в XML-файл.

6. Для импорта списка исключений выполните следующие действия:

   a. Нажмите на кнопку → **Импортировать**.

   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

   c. Откройте файл.

      Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

7. Сохраните внесенные изменения.

Как экспортировать / импортировать список исключений в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Защита от сетевых угроз**.
5. В верхней части окна перейдите по ссылке **Доверенный IP-адрес**.

   Откроется список исключений.
6. Для экспорта списка исключений выполните следующие действия:

   a. Выберите исключения, которые вы хотите экспортировать.

   b. Нажмите на кнопку → **Экспортировать**.

   Kaspersky Endpoint Security экспортирует список исключений в JSON-файл в папку для загрузки по умолчанию.
7. Для импорта списка исключений выполните следующие действия:

   a. Нажмите на кнопку → **Импортировать**.

   В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список исключений.

   b. Откройте файл.

   Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.
8. Сохраните внесенные изменения.

Настройка Защиты от сетевых угроз по типам

Kaspersky Endpoint Security позволяет управлять защитой от следующих типов сетевых атак:

- *Атака типа Интенсивные сетевые запросы (англ. Network Flooding)* – атака на сетевые ресурсы организации (например, веб-серверы). Атака заключается в отправке большого количества запросов для превышения пропускной способности сетевых ресурсов. Таким образом, пользователи не могут получить доступ к сетевым ресурсам организации.
- *Атака типа Сканирование портов* заключается в сканировании UDP- и TCP-портов, а также сетевых служб на компьютере. Атака позволяет определить степень уязвимости компьютера перед более опасными видами сетевых атак. Сканирование портов также позволяет злоумышленнику определить операционную систему на компьютере и выбрать подходящие для нее сетевые атаки.
- *Атака типа MAC-спуфинг* заключается в изменении MAC-адреса сетевого устройства (сетевой карты). В результате злоумышленник может перенаправить данные, отправленные на устройство, на другое устройство и получить доступ к этим данным. Kaspersky Endpoint Security позволяет блокировать атаки MAC-спуфинга и получать уведомления об атаках.

Вы можете выключить обнаружение этих типов атак, так как некоторые разрешенные приложения выполняют действия, характерные для таких атак. Таким образом, вы можете избежать ложных срабатываний.

По умолчанию Kaspersky Endpoint Security не отслеживает атаки типа Интенсивные сетевые запросы, Сканирование портов и MAC-спуфинг.

Настроить отдельные исключения для этих типов атак невозможно. Это значит, что даже при добавлении отдельных IP-адресов в доверенную зону Kaspersky Endpoint Security будет блокировать атакующий компьютер, если обнаружит такую атаку. Вы можете либо включить, либо выключить обнаружение этих атак.

На виртуальных машинах в инфраструктуре Microsoft Hyper-V не рекомендуем включать обнаружение атак типа MAC-спуфинг. Из-за особенностей работы платформы Microsoft Hyper-V Kaspersky Endpoint Security может заблокировать гипервизор из-за ложных срабатываний.

Как настроить Защиту от сетевых угроз по типам в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита** → **Защита от сетевых угроз**.
4. Используйте флажок **Считать атаками сканирование портов и интенсивные сетевые запросы**, чтобы включить или выключить обнаружение атак типа *Интенсивные сетевые запросы* и *Сканирование портов*.

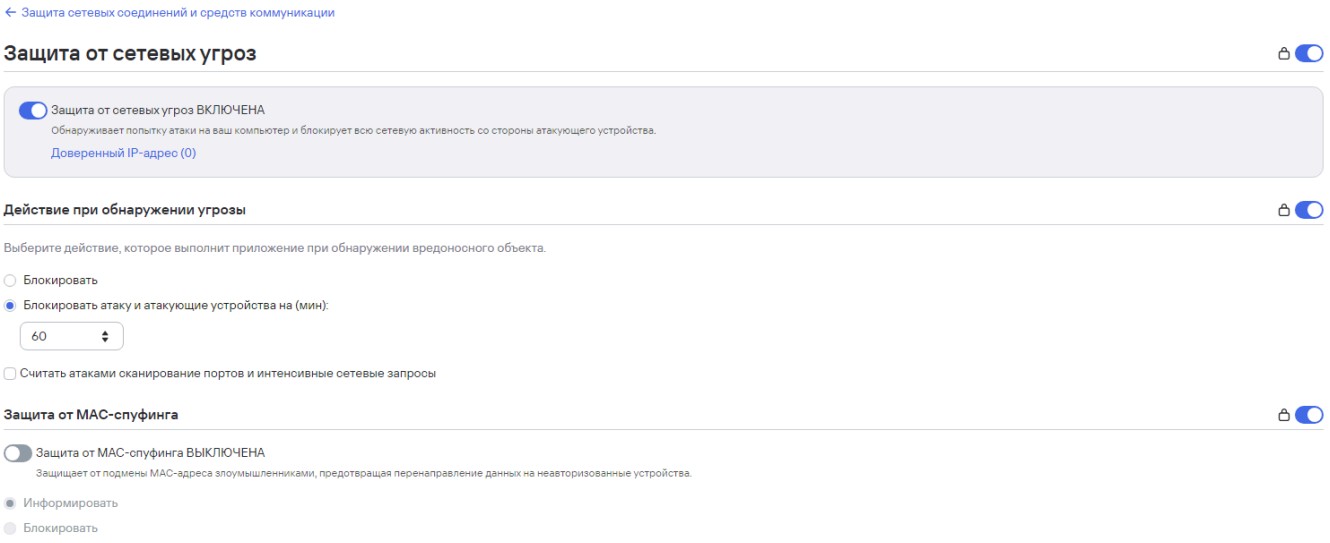
   Если функция включена, Kaspersky Endpoint Security проверяет сетевой трафик на наличие признаков сканирования портов и интенсивных сетевых запросов. При обнаружении атак данных типов приложение блокирует сетевое соединение с атакующим компьютером, уведомляет об атаке пользователя и отправляет соответствующее событие в Kaspersky Security Center. Также при обнаружении атак типа *Интенсивные сетевые запросы* приложение добавляет атакующий компьютер в список блокирования.
5. В блоке **Режим защиты от MAC-спуфинга** выберите один из следующих вариантов:
   - **Не отслеживать MAC-спуфинг**;
   - **Информировать**;
   - **Блокировать**.
6. Сохраните внесенные изменения.

Как настроить Защиту от сетевых угроз по типам в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации → Защита от сетевых угроз**



Параметры Защиты от сетевых угроз

5. Используйте флажок **Считать атаками сканирование портов и интенсивные сетевые запросы**, чтобы включить или выключить обнаружение атак типа *Интенсивные сетевые запросы* и *Сканирование портов*..

   Если функция включена, Kaspersky Endpoint Security проверяет сетевой трафик на наличие признаков сканирования портов и интенсивных сетевых запросов. При обнаружении атак данных типов приложение блокирует сетевое соединение с атакующим компьютером, уведомляет об атаке пользователя и отправляет соответствующее событие в Kaspersky Security Center. Также при обнаружении атак типа *Интенсивные сетевые запросы* приложение добавляет атакующий компьютер в список блокирования.

6. В блоке **Защита от MAC-спуфинга** настройте обнаружение атак типа MAC-спуфинг:

   a. Используйте переключатель **Защита от MAC-спуфинга ВКЛЮЧЕНА**, чтобы включить или выключить обнаружение атак.

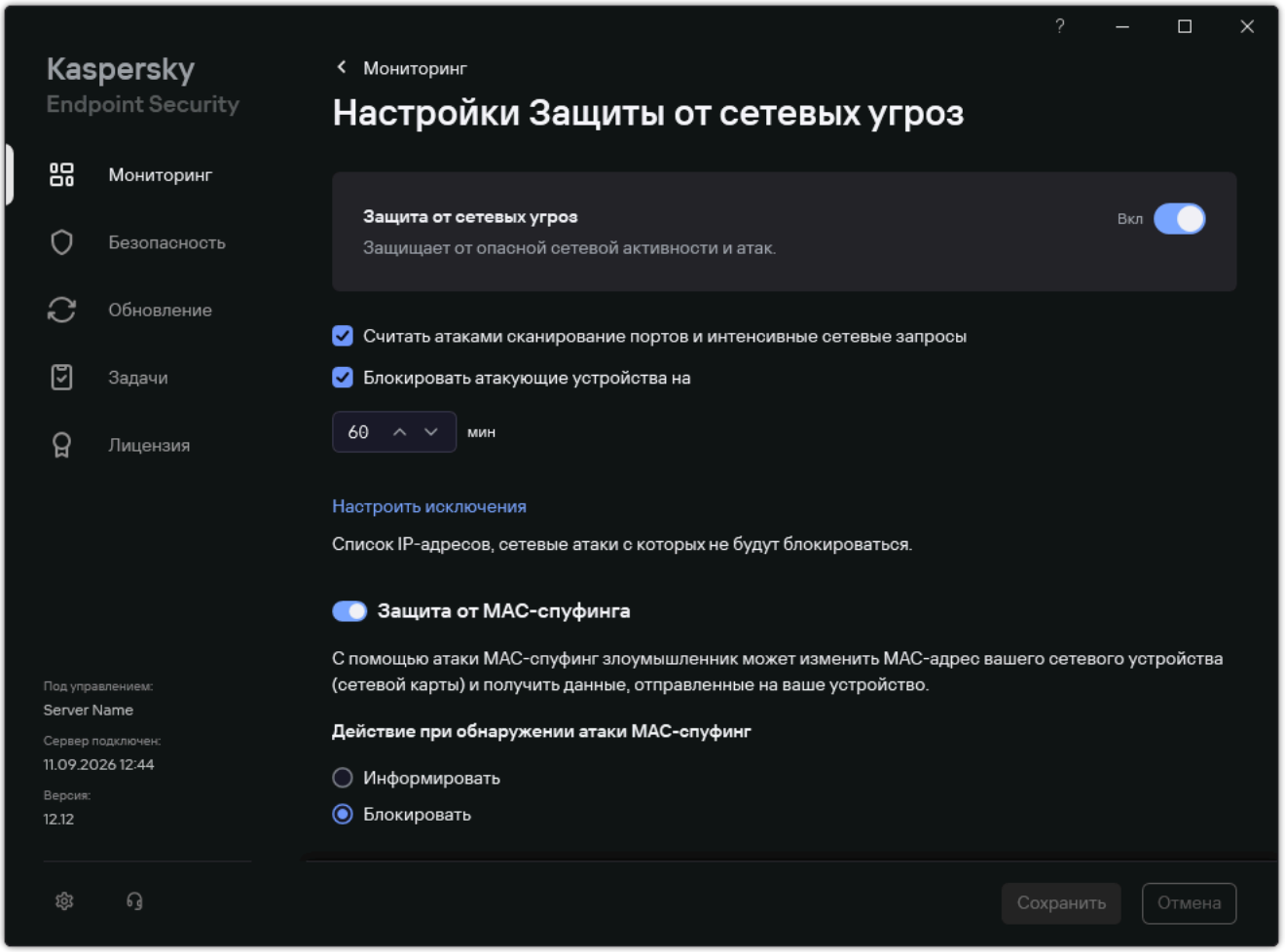
   b. Выберите действие при обнаружении атаки типа MAC-спуфинг:

   - **Информировать**;
   - **Блокировать**.

7. Сохраните внесенные изменения.

Как настроить Защиту от сетевых угроз по типам в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Защита от сетевых угроз**.



Параметры Защиты от сетевых угроз

3. Используйте переключатель **Считать атаками сканирование портов и интенсивные сетевые запросы**, чтобы включить или выключить обнаружение атак типа *Интенсивные сетевые запросы* и *Сканирование портов*.

   Если функция включена, Kaspersky Endpoint Security проверяет сетевой трафик на наличие признаков сканирования портов и интенсивных сетевых запросов. При обнаружении атак данных типов приложение блокирует сетевое соединение с атакующим компьютером, уведомляет об атаке пользователя и отправляет соответствующее событие в Kaspersky Security Center. Также при обнаружении атак типа *Интенсивные сетевые запросы* приложение добавляет атакующий компьютер в список блокирования.

4. Используйте переключатель **Защита от MAC-спуфинга**, чтобы включить или выключить обнаружение атак типа *MAC-спуфинг*.

5. В блоке **Действие при обнаружении атаки MAC-спуфинг** выберите один из следующих вариантов:

   - **Информировать**.
   - **Блокировать**.

6. Сохраните внесенные изменения.

Сетевой экран

Сетевой экран блокирует несанкционированные подключения к компьютеру во время работы в интернете или локальной сети. Также Сетевой экран контролирует сетевую активность приложений на компьютере. Это позволяет защитить локальную сеть организации от кражи персональных данных и других атак. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и предустановленных *сетевых правил*.

Для взаимодействия с Kaspersky Security Center приложение использует Агент администрирования. При этом Сетевой экран автоматически создает сетевые правила, необходимые для работы Агента администрирования и приложения. В результате Сетевой экран открывает некоторые порты на компьютере. Набор портов отличается в зависимости от роли компьютера (например, точка распространения). Подробнее о портах, которые будут открыты на компьютере, см. в справке Kaspersky Security Center.

Сетевые правила

Вы можете настроить сетевые правила на следующих уровнях:

- *Сетевые пакетные правила*. Используются для ввода ограничений на сетевые пакеты независимо от приложения. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных. Kaspersky Endpoint Security имеет предустановленные сетевые пакетные правила с разрешениями, рекомендованными специалистами "Лаборатории Касперского".

- *Сетевые правила приложений*. Используются для ограничения сетевой активности конкретного приложения. Учитываются не только характеристики сетевого пакета, но и конкретное приложение, которому адресован этот сетевой пакет, либо которое инициировало отправку этого сетевого пакета.

Контроль доступа приложений к ресурсам операционной системы, процессам и персональным данным обеспечивает компонент Предотвращение вторжений с помощью *прав приложений*.

Во время первого запуска приложения Сетевой экран выполняет следующие действия:

1. Проверяет безопасность приложения с помощью загруженных антивирусных баз.

2. Проверяет безопасность приложения в Kaspersky Security Network.

   Для более эффективной работы Сетевого экрана вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает приложение в одну из групп доверия: *Доверенные*, *Слабые ограничения*, *Сильные ограничения*, *Недоверенные*.

   Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля активности приложений. Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от уровня опасности, которую это приложение может представлять для компьютера.

Kaspersky Endpoint Security помещает приложение в группу доверия для компонентов Сетевой экран и Предотвращение вторжений. Изменить группу доверия только для Сетевого экрана или только для Предотвращения вторжений невозможно.

Если вы отказались принимать участие в KSN или отсутствует сеть, Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации приложения от KSN группа доверия может быть изменена автоматически.

4. Блокирует сетевую активность приложения в зависимости от группы доверия. Например, приложениям из группы доверия *Сильные ограничения* запрещены любые сетевые соединения.

При следующем запуске приложения Kaspersky Endpoint Security проверяет целостность приложения. Если приложение не было изменено, компонент применяет к нему текущие сетевые правила. Если приложение было изменено, Kaspersky Endpoint Security исследует приложение как при первом запуске.

Приоритеты сетевых правил

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если сетевая активность добавлена в несколько правил, Сетевой экран регулирует сетевую активность по правилу с высшим приоритетом.

Сетевые пакетные правила имеют более высокий приоритет, чем сетевые правила приложений. Если для одного и того же вида сетевой активности заданы и сетевые пакетные правила, и сетевые правила приложений, то эта сетевая активность обрабатывается по сетевым пакетным правилам.

Сетевые правила приложений имеют особенность. Сетевое правило приложений включает в себя правила доступа по статусу сети: *Публичная сеть*, *Локальная сеть*, *Доверенная сеть*. Например, для группы доверия *Сильные ограничения* по умолчанию запрещена любая сетевая активность приложения в сетях всех статусов. Если для отдельного приложения (родительское приложение) задано сетевое правило, то дочерние процессы других приложений будут выполнены в соответствии с сетевым правилом родительского приложения. Если сетевое правило для приложения отсутствует, дочерние процессы будут выполнены в соответствии с правилом доступа к сетям группы доверия.

Например, вы запретили любую сетевую активность всех приложений для сетей всех статусов, кроме браузера X. Если в браузере X (родительское приложение) запустить установку браузера Y (дочерний процесс), то установщик браузера Y получит доступ к сети и загрузит необходимые файлы. После установки браузеру Y будут запрещены любые сетевые соединения в соответствии с параметрами Сетевого экрана. Чтобы запретить установщику браузера Y сетевую активность в качестве дочернего процесса, необходимо добавить сетевое правило для установщика браузера Y.

Типы сетевых соединений

Сетевой экран позволяет контролировать сетевую активность в зависимости от типа сетевого соединения. Kaspersky Endpoint Security получает тип сетевого соединения от операционной системы компьютера. Тип сетевого соединения в операционной системе задает пользователь при настройке подключения. Вы можете изменить тип сетевого соединения в параметрах Kaspersky Endpoint Security. Сетевой экран будет контролировать сетевую активность в зависимости от типа сети в параметрах Kaspersky Endpoint Security, а не операционной системы.

Выделены следующие типы сетевого соединения:

- **Публичная сеть**. Сеть не защищена антивирусными приложениями, сетевыми экранами, фильтрами (например, Wi-Fi в кафе). Пользователю компьютера, подключенного к такой сети, Сетевой экран закрывает доступ к файлам и принтерам этого компьютера. Сторонние пользователи также не могут получить доступ к информации через папки общего доступа и удаленный доступ к рабочему столу этого компьютера. Сетевой экран фильтрует сетевую активность каждого приложения в соответствии с сетевыми правилами этого приложения.

  Сетевой экран по умолчанию присваивает тип *Публичная сеть* сети Интернет. Вы не можете изменить тип сети Интернет.

- **Локальная сеть**. Сеть для пользователей, которым ограничен доступ к файлам и принтерам этого компьютера (например, для локальной сети организации или для домашней сети).

- **Доверенная сеть**. Безопасная сеть, во время работы в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. Для сетей с этим статусом Сетевой экран разрешает любую сетевую активность в рамках этой сети.

Совместимость с Брандмауэром Защитника Windows

В операционную систему встроен собственный сетевой экран – *Брандмауэр Защитника Windows*. Поведение приложение отличается в зависимости от типа операционной системы:

- **Рабочая станция**. Совместная работа Сетевого экрана от "Лаборатории Касперского" и Брандмауэра Защитника Windows может привести к сбоям в работе системы. Поэтому в Kaspersky Endpoint Security встроен механизм, который исключает одновременную работу обоих Сетевых экранов. При включении Сетевого экрана от "Лаборатории Касперского", операционная система автоматически выключает Брандмауэр Защитника Windows. При выключении Сетевого экрана от "Лаборатории Касперского", операционная система автоматически включает Брандмауэр Защитника Windows обратно – это позволяет обеспечить защиту компьютера.

- **Сервер**. Сетевой экран от "Лаборатории Касперского" и Брандмауэр Защитника Windows несовместимы между собой. Инсталлятор Kaspersky Endpoint Security автоматически удаляет Брандмауэр Защитника Windows во время установки приложения.

Включение и выключение Сетевого экрана

По умолчанию Сетевой экран включен и работает в оптимальном режиме.

Как включить или выключить Сетевой экран в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Базовая защита → Сетевой экран**.
4. Используйте флажок **Сетевой экран**, чтобы включить или выключить компонент.
5. Сохраните внесенные изменения.

Как включить или выключить Сетевой экран в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации → Сетевой экран**.
5. Используйте переключатель **Сетевой экран ВКЛЮЧЕН**, чтобы включить или выключить компонент.
6. Сохраните внесенные изменения.

Как включить или выключить Сетевой экран в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Сетевой экран**.
3. Используйте переключатель **Сетевой экран**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Сетевой экран включен, Kaspersky Endpoint Security контролирует сетевую активность и блокирует несанкционированные сетевые подключения к компьютеру, а также блокирует несанкционированную сетевую активность приложений на компьютере. Также сетевую активность контролирует компонент Защита от сетевых угроз. Компонент Защита от сетевых угроз (англ. Intrusion Detection System, IDS) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак.

Kaspersky Endpoint Security регистрирует в отчетах события сетевых атак независимо от параметров Сетевого экрана. Даже если Сетевой экран блокирует сетевое подключение с помощью правил и тем самым предотвращает сетевую атаку, компонент Защита от сетевых угроз регистрирует события сетевой атаки. Это нужно для формирования статистический информации о сетевых атаках на компьютеры организации.

Изменение типа сетевого соединения

Сетевой экран по умолчанию присваивает тип *Публичная сеть* сети Интернет. Вы не можете изменить тип сети Интернет.

Чтобы изменить тип сетевого соединения, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Сетевой экран**.
3. Нажмите на кнопку **Доступные сети**.
4. Выберите сетевое соединение, тип которого вы хотите изменить.
5. В графе **Тип сети** выберите тип сетевого соединения:
   - **Публичная сеть**. Сеть не защищена антивирусными приложениями, сетевыми экранами, фильтрами (например, Wi-Fi в кафе). Пользователю компьютера, подключенного к такой сети, Сетевой экран закрывает доступ к файлам и принтерам этого компьютера. Сторонние пользователи также не могут получить доступ к информации через папки общего доступа и удаленный доступ к рабочему столу этого компьютера. Сетевой экран фильтрует сетевую активность каждого приложения в соответствии с сетевыми правилами этого приложения.
   - **Локальная сеть**. Сеть для пользователей, которым ограничен доступ к файлам и принтерам этого компьютера (например, для локальной сети организации или для домашней сети).
   - **Доверенная сеть**. Безопасная сеть, во время работы в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. Для сетей с этим статусом Сетевой экран разрешает любую сетевую активность в рамках этой сети.
6. Сохраните внесенные изменения.

Работа с сетевыми пакетными правилами

Вы можете выполнить следующие действия в процессе работы с сетевыми пакетными правилами:

- Создать новое сетевое пакетное правило.

  Вы можете создать новое сетевое пакетное правило, сформировав набор условий и действий над сетевыми пакетами и потоками данных.

- Включить и выключить сетевое пакетное правило.

  Все сетевые пакетные правила, созданные Сетевым экраном по умолчанию, имеют статус *Включено*. Если сетевое пакетное правило включено, Сетевой экран применяет это правило.

  Вы можете выключить любое сетевое пакетное правило, выбранное в списке сетевых пакетных правил. Если сетевое пакетное правило выключено, Сетевой экран временно не применяет это правило.

Новое сетевое пакетное правило, созданное пользователем, по умолчанию добавляется в список сетевых пакетных правил со статусом *Включено*.

- Изменить параметры существующего сетевого пакетного правила.

  После того как вы создали новое сетевое пакетное правило, вы всегда можете вернуться к настройке его параметров и изменить нужные.

- Изменить действие Сетевого экрана для сетевого пакетного правила.

  В списке сетевых пакетных правил вы можете изменить действие, которое Сетевой экран выполняет, обнаружив сетевую активность указанного сетевого пакетного правила.

- Изменить приоритет сетевого пакетного правила.

  Вы можете повысить или понизить приоритет выбранного в списке сетевого пакетного правила.

- Удалить сетевое пакетное правило.

  Вы можете удалить сетевое пакетное правило, если вы не хотите, чтобы Сетевой экран применял это правило при обнаружении сетевой активности, и чтобы оно отображалось в списке сетевых пакетных правил со статусом *Выключено*.

Создание сетевого пакетного правила

Сетевой экран фильтрует всю сетевую активность на компьютере в соответствии с сетевыми пакетными правилами. Сетевые пакетные правила содержат условия, в соответствии с которыми Сетевой экран контролирует сетевые соединения на компьютере (например, направление соединения, протокол). В сетевых пакетных правилах также указано действие Сетевого экрана с соединением, удовлетворяющим условиям правила (разрешить соединение или запретить соединение).

Рекомендации по созданию сетевых пакетных правил

Для фильтрации сетевой активности вы можете указать IP-адрес или диапазон IP-адресов. Также вы можете указать DNS-имя.

Если в правиле используется DNS-имя, Kaspersky Endpoint Security выполняет разрешение данного DNS-имени и в дальнейшем при работе с правилом использует полученный IP-адрес.

Kaspersky Endpoint Security может выполнять разрешение DNS-имен в следующих случаях:

- запуск приложения;

- изменение настроек Сетевого экрана.

В процессе разрешения DNS-имен с компьютера, на котором установлено приложение, может выполняться большое количество запросов к DNS-серверу. Чтобы избежать этого, мы рекомендуем использовать IP-адреса при создании правил.

В некоторых случаях использование DNS-имен в сетевых пакетных правилах может быть небезопасным, так как владелец DNS-сервера может изменить параметры DNS-записи. Также злоумышленник может подменить DNS-сообщения и обойти правила Сетевого экрана.

Вы можете контролировать сетевые соединения по DNS-именам с помощью правил Веб-Контроля. Если вам необходимо задать DNS-имя в правилах Сетевого экрана, выполните следующие действия:

- обеспечьте защиту локальной сети организации;
- убедитесь в безопасности используемых кеширующих и авторитативных DNS-серверов;
- включите защиту DNS-записи от изменений.

Создавая сетевые пакетные правила, следует помнить, что они имеют приоритет над сетевыми правилами приложений.

Способы создания сетевых пакетных правил

Вы можете создать сетевое пакетное правило следующими способами:

- С помощью инструмента Мониторинг сети.

  Мониторинг сети – это инструмент, предназначенный для просмотра информации о сетевой активности компьютера пользователя в реальном времени. Этот способ удобен, так как вам не нужно настраивать все параметры правила. Некоторые параметры Сетевой экран подставит автоматически из данных Мониторинга сети. Мониторинг сети доступен только в интерфейсе приложения.

- В параметрах Сетевого экрана.

  Этот способ позволяет выполнить тонкую настройку параметров Сетевого экрана. Вы можете создать правила для любой сетевой активности, даже если сетевой активности нет в реальном времени.

Как создать сетевое пакетное правило в интерфейсе приложения с помощью инструмента Мониторинг сети

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Мониторинг сети**.
2. Перейдите на вкладку **Сетевая активность**.

   На вкладке **Сетевая активность** отображаются все активные на текущий момент сетевые соединения с компьютером пользователя. Приводятся как сетевые соединения, инициированные компьютером пользователя, так и входящие сетевые соединения.
3. В контекстном меню сетевого соединения выберите пункт **Создать сетевое пакетное правило**.

   Откроются свойства сетевого правила.
4. Установите статус пакетного правила **Активно**.
5. В поле **Название** введите название сетевой службы вручную.
6. Настройте параметры сетевого правила (см. таблицу ниже).

   Вы можете выбрать предустановленный шаблон правила по ссылке **Шаблон сетевого правила**. Шаблоны правила описывают наиболее часто используемые сетевые соединения.

   Все параметры сетевого правила будут заполнены автоматически.
7. Установите флажок **Записывать события**, если вы хотите, чтобы действие сетевого правила было отражено в отчете.

8. Нажмите на кнопку **Сохранить**.

   Новое сетевое правило будет добавлено в список.

9. Кнопками **Вверх** / **Вниз** установите приоритет сетевого правила.

10. Сохраните внесенные изменения.

Как создать сетевое пакетное правило в интерфейсе приложения в параметрах Сетевого экрана

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Сетевой экран**.

3. Нажмите на кнопку **Пакетные правила**.

   Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.

4. В раскрывающемся списке **Добавить** выберите расположение правила в списке: в начале, в конце списка или рядом с выбранным правилом.

   Расположение правила в списке определяет приоритет правила. Правило в начале списка имеет наивысший приоритет.

5. Установите статус пакетного правила **Активно**.

6. В поле **Название** введите название сетевой службы вручную.

7. Настройте параметры сетевого правила (см. таблицу ниже).

   Вы можете выбрать предустановленный шаблон правила по ссылке **Шаблон сетевого правила**. Шаблоны правила описывают наиболее часто используемые сетевые соединения.

   Все параметры сетевого правила будут заполнены автоматически.

8. Установите флажок **Записывать события**, если вы хотите, чтобы действие сетевого правила было отражено в отчете.

9. Нажмите на кнопку **Сохранить**.

   Новое сетевое правило будет добавлено в список.

10. Кнопками **Вверх** / **Вниз** установите приоритет сетевого правила.

11. Сохраните внесенные изменения.

Как создать сетевое пакетное правило в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Базовая защита** → **Сетевой экран**.

4. В блоке **Настройки Сетевого экрана** нажмите на кнопку **Настройка**.

   Откроются список сетевых пакетных правил и список сетевых правил приложений.

5. Перейдите на вкладку **Сетевые пакетные правила**.

   Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.

6. В раскрывающемся списке **Добавить** выберите расположение правила в списке: в начале, в конце списка или рядом с выбранным правилом.

   Расположение правила в списке определяет приоритет правила. Правило в начале списка имеет наивысший приоритет.

7. В поле **Название** введите название сетевой службы вручную.

8. Настройте параметры сетевого правила (см. таблицу ниже).

   Вы можете выбрать предустановленный шаблон правила по кнопке . Шаблоны правила описывают наиболее часто используемые сетевые соединения.

   Все параметры сетевого правила будут заполнены автоматически.

9. Установите флажок **Записывать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете.

10. Сохраните новое сетевое правило.

11. Кнопками **Вверх** / **Вниз** установите приоритет сетевого правила.

12. Сохраните внесенные изменения.

Сетевой экран будет контролировать сетевые пакеты согласно правилу. Вы можете выключить пакетное правило из работы Сетевого экрана не удаляя его из списка. Для этого снимите флажок рядом с ним.

Как создать сетевое пакетное правило в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Сетевой экран**.

5. Выберите вкладку **Сетевые пакетные правила**.

   Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.

6. Нажмите на кнопку **Добавить**.

   Откроется форма нового сетевого правила.

7. В поле **Имя правила** введите название сетевой службы вручную.

8. Настройте параметры сетевого правила (см. таблицу ниже).

   Вы можете выбрать предустановленный шаблон правила по ссылке **Выбрать шаблон правила**. Шаблоны правила описывают наиболее часто используемые сетевые соединения.

   Все параметры сетевого правила будут заполнены автоматически.

9. Установите флажок **Записывать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете.

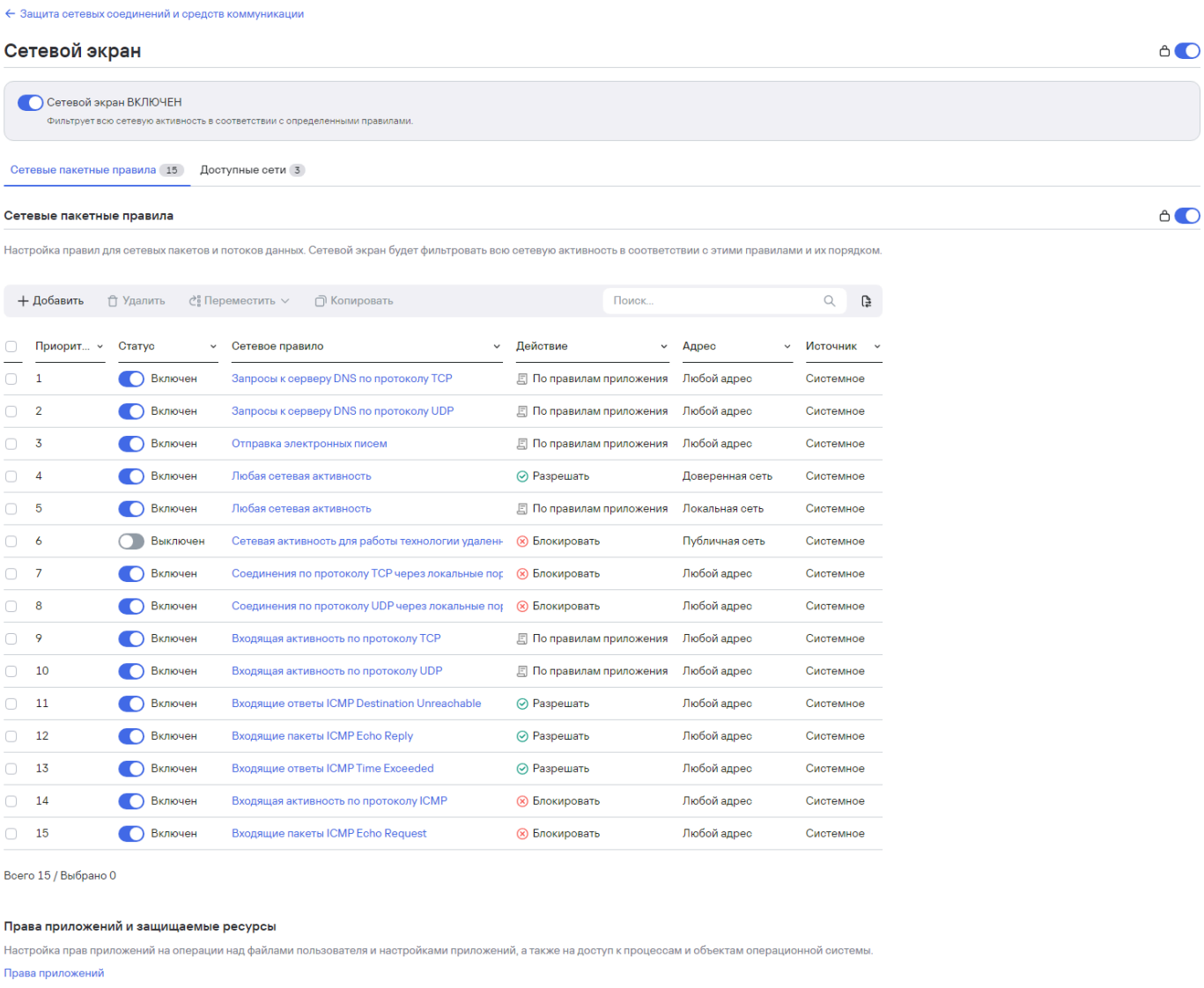
10. Сохраните сетевое правило.

    Новое сетевое правило будет добавлено в список.

11. С помощью кнопки **Переместить** установите приоритет сетевого правила.

12. Сохраните внесенные изменения.

Сетевой экран будет контролировать сетевые пакеты согласно правилу. Вы можете выключить пакетное правило из работы Сетевого экрана не удаляя его из списка. Используйте переключатель в графе **Статус**, чтобы включить или выключить пакетное правило.



Пакетные правила Сетевого экрана

Параметры сетевого пакетного правила

Параметр	Описание
Действие	**Разрешать**. **Запрещать**. **По правилам приложения**. Если выбран этот элемент, Сетевой экран применяет к сетевому соединению сетевые правила приложения.
Протокол	Контроль сетевой активности по выбранному протоколу: TCP, UDP, ICMP, ICMPv6, IGMP и GRE. Если в качестве протокола выбран протокол ICMP или ICMPv6, вы можете задать тип и код ICMP-пакета. Если в качестве протокола выбран протокол TCP или UDP, вы можете указать номера портов компьютера пользователя и удаленного компьютера, соединение между которыми следует контролировать. Диапазон возможных значений номеров порта: 0–65535. В каждом поле вы можете указать несколько значений, разделенных `,`, или задать диапазон значений через `-`. Например: • `100,101`; • `100-130`; • `100,110-130`.

Параметр	Описание
Направление	**Входящее (пакет)**. Сетевой экран применяет сетевое правило ко всем входящим сетевым пакетам. **Входящее**. Сетевой экран применяет сетевое правило ко всем сетевым пакетам в рамках соединения, которое инициировал удаленный компьютер. **Входящее / Исходящее**. Сетевой экран применяет сетевое правило ко всем входящим и исходящим сетевым пакетам. **Исходящее (пакет)**. Сетевой экран применяет сетевое правило ко всем исходящим сетевым пакетам. **Исходящее**. Сетевой экран применяет сетевое правило ко всем сетевым пакетам в рамках соединения, которое инициировал компьютер пользователя.
Сетевые адаптеры	Сетевые адаптеры, которые могут передавать / получать сетевые пакеты. Указание параметров сетевых адаптеров позволяет различать сетевые пакеты, отправленные или полученные сетевыми адаптерами с одинаковыми IP-адресами.
Время жизни (TTL)	Ограничение контроля сетевых пакетов по времени их жизни (англ. Time to Live, TTL).
Удаленные адреса	Сетевые адреса удаленных компьютеров, которые могут передавать / получать сетевые пакеты. К заданному диапазону удаленных сетевых адресов Сетевой экран применяет сетевое правило. Вы можете включить в сетевое правило все IP-адреса, создать отдельный список IP-адресов, указать диапазон IP-адресов или выбрать подсеть (Доверенные сети, Локальные сети, Публичные сети). Также вместо IP-адреса вы можете указать DNS-имя компьютера. Используйте DNS-имена только для компьютеров локальной сети или внутренних сервисов. Для работы с облачными сервисами (например, Microsoft Azure) и другими интернет-ресурсами предназначен компонент Веб-Контроль. Если в сетевом пакетном правиле вы добавили DNS-имя, для которого не удалось определить IP-адрес, Kaspersky Endpoint Security предупредит вас об этом. В списке сетевых пакетных правил в Web Console будет добавлена графа с описанием ошибки. В Консоли администрирования (MMC) описание ошибки недоступно. Такое пакетное правило будет выделено цветом.
Локальные адреса	Сетевые адреса компьютеров, которые могут передавать / получать сетевые пакеты. К заданному диапазону локальных сетевых адресов Сетевой экран применяет сетевое правило. Вы можете включить в сетевое правило все IP-адреса, создать отдельный список IP-адресов или указать диапазон IP-адресов. Приложение сохраняет локальные адреса, только если задан список удаленных адресов. То есть для параметра **Удаленные адреса** выбрано значение **Адреса из списка** и добавлен хотя бы один адрес. Для приложений не всегда возможно получить локальный адрес. В этом случае этот параметр игнорируется.

Включение и выключение сетевого пакетного правила

Чтобы включить или выключить сетевое пакетное правило, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Сетевой экран**.
3. Нажмите на кнопку **Пакетные правила**.

   Откроется список сетевых пакетных правил, установленных Сетевым экраном по умолчанию.
4. Выберите в списке нужное сетевое пакетное правило.
5. Используйте переключатель в графе **Статус**, чтобы включить или выключить правило.
6. Сохраните внесенные изменения.

Изменение действия Сетевого экрана для сетевого пакетного правила

Чтобы изменить действие Сетевого экрана для сетевого пакетного правила, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Сетевой экран**.
3. Нажмите на кнопку **Пакетные правила**.

   Откроется список сетевых пакетных правил, установленных Сетевым экраном по умолчанию.
4. Выберите его в списке сетевых пакетных правил и нажмите на кнопку **Изменить**.
5. В раскрывающемся списке **Действие** выберите действие, которое должен выполнять Сетевой экран, обнаружив этот вид сетевой активности:

   - **Разрешать**.
   - **Запрещать**.
   - **По правилам приложения**. Если выбран этот элемент, Сетевой экран применяет к сетевому соединению сетевые правила приложения.
6. Сохраните внесенные изменения.

Изменение приоритета сетевого пакетного правила

Приоритет выполнения сетевого пакетного правила определяется его положением в списке сетевых пакетных правил. Первое сетевое пакетное правило в списке сетевых пакетных правил обладает самым высоким приоритетом.

Каждое сетевое пакетное правило, которое вы создали вручную, добавляется в конец списка сетевых пакетных правил и имеет самый низкий приоритет.

Сетевой экран выполняет правила в порядке их расположения в списке сетевых пакетных правил, сверху вниз. Согласно каждому обрабатываемому сетевому пакетному правилу, применяемому к определенному сетевому соединению, Сетевой экран либо разрешает, либо блокирует сетевой доступ к адресу и порту, указанным в настройках этого сетевого соединения.

Чтобы изменить приоритет сетевого пакетного правила, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Сетевой экран**.
3. Нажмите на кнопку **Пакетные правила**.

   Откроется список сетевых пакетных правил, установленных Сетевым экраном по умолчанию.
4. Выберите в списке сетевое пакетное правило, приоритет которого вы хотите изменить.

5. Кнопками **Вверх** / **Вниз** установите приоритет сетевого правила.

6. Сохраните внесенные изменения.

Экспорт и импорт сетевых пакетных правил

Вы можете экспортировать список сетевых пакетных правил в файл в формате XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных правил. Вы можете использовать функцию экспорта / импорта для резервного копирования списка сетевых пакетных правил или для миграции списка на другой сервер.

Как экспортировать / импортировать список сетевых пакетных правил в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Базовая защита** → **Сетевой экран**.

4. В блоке **Настройки Сетевого экрана** нажмите на кнопку **Настройка**.

   Откроются список сетевых пакетных правил и список сетевых правил приложений.

5. Перейдите на вкладку **Сетевые пакетные правила**.

6. Для экспорта списка сетевых пакетных правил выполните следующие действия:

   a. Выберите правила, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

      Если вы не выбрали ни одного правила, Kaspersky Endpoint Security экспортирует все правила.

   b. Нажмите на ссылку **Экспортировать**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список правил, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл.

7. Для импорта списка сетевых пакетных правил выполните следующие действия:

   a. Нажмите на ссылку **Импортировать**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

   b. Откройте файл.

      Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

8. Сохраните внесенные изменения.

Как экспортировать / импортировать список сетевых пакетных правил в Web Console и Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Сетевой экран**.
5. Для экспорта списка правил в блоке **Сетевые пакетные правила** выполните следующие действия:

   a. Выберите правила, которые вы хотите экспортировать.

   b. Нажмите на кнопку → **Экспортировать**.

   Kaspersky Endpoint Security экспортирует список правил в JSON-файл в папку для загрузки по умолчанию.
6. Для импорта списка правил в блоке **Сетевые пакетные правила** выполните следующие действия:

   a. Нажмите на кнопку → **Импортировать**.

   В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список правил.

   b. Откройте файл.

   Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.
7. Сохраните внесенные изменения.

Описание сетевых пакетных правил в XML

Сетевой экран позволяет экспортировать сетевые пакетные правила в XML-формат. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных правил.

XML-файл содержит два основных узла: `Rules` и `Resources`. В узле `Rules` перечислены сетевые пакетные правила. Узел включает в себя как правила, установленные по умолчанию – *предустановленные правила*, так и правила, добавленные пользователем – *пользовательские правила*.

Разметка сетевого пакетного правила

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

Параметры сетевого пакетного правила в XML-формате

Параметр	Описание	Значение
`<key name="0000">`	Приоритет правила. Чем меньше значение, тем выше приоритет.	Integer Значение приоритета должно состоять из 4 цифр. Узлы должны быть расположены в XML-файле по порядку начиная со значения `0000`.
`RuleId`	Идентификатор правила.	**Предустановленные правила** `100` – **Запросы к серверу DNS по протоколу TCP**. `101` – **Запросы к серверу DNS по протоколу UDP**. `102` – **Отправка электронных писем**. `110` – **Любая сетевая активность** (Доверенные сети). `125` – **Любая сетевая активность** (Локальные сети). `130` – **Сетевая активность для работы технологии удаленного рабочего стола**. `131` – **Соединения по протоколу TCP через локальные порты**. `132` – **Соединения по протоколу UDP через локальные порты**. `133` – **Входящая активность по протоколу TCP**. `134` – **Входящая активность по протоколу UDP**. `137` – **Входящие ответы ICMP Destination Unreachable**. `138` – **Входящие пакеты ICMP Echo Reply**. `140` – **Входящие ответы ICMP Time Exceeded**. `142` – **Входящая активность по протоколу ICMP**. `266` – **Входящие пакеты ICMPv6 Echo Request**.
`RuleState`	Статус правила.	`0` – предустановленное правило выключено; `1` – предустановленное правило включено; `2` – пользовательское правило выключено; `3` – пользовательское правило включено.
`RuleTypeId`	Идентификатор типа правила.	`4` – сетевое пакетное правило.
`AppIdEx`	Идентификатор приложения, которому принадлежит сетевое пакетное правило.	Если правило не принадлежит ни одному из приложений, то значение `0`.
`ResIdEx`	Основной идентификатор ресурса с параметрами правила. С помощью этого идентификатора вы можете найти блок с параметрами правила в узле `Resources`.	Integer
`ResIdEx2`	Идентификатор типа сети.	`0` – **Любой адрес**. `50` – **Доверенные сети**. `51` – **Локальные сети**. `52` – **Публичные сети**. `<Network Identifier>` – **Адреса из списка** (адреса заданы вручную).
`AccessFlag`	Значение параметра **Действие**.	`0` – **Разрешать**. `2` – **По правилам приложения**. `3` – **Запрещать**. `4` – **Разрешать** и **Записывать в отчет**. `6` – **По правилам приложения** и **Записывать в отчет**. `7` – **Запрещать** и **Записывать в отчет**.
`</key>`		

В узле `Resources` содержатся параметры сетевых пакетных правил. Параметры пользовательских сетевых пакетных правил приведены в блоке `<key name="0004">`.

Разметка пользовательского сетевого пакетного правила

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

Параметры пользовательского сетевого пакетного правила

Параметр	Описание	Значение
`<key name="Data">`	Идентификатор блока параметров.	Integer
`RemotePorts`	Значение параметра **Удаленные порты**.	Список диапазонов удаленных портов.
`LocalPorts`	Значение параметра **Локальные порты**.	Список диапазонов локальных портов.

Параметр	Описание	Значение
`AdapterBindings`	Значение параметра **Сетевые адаптеры**.	`IpAddresses` – значение параметра **IP-адреса**. `MacAddresses` – значение параметра **MAC-адреса**. `AdapterName` – имя сетевого адаптера. `InterfaceType` – значение параметра **Тип интерфейса**: • `0` – **Другое**. • `1` – **LoopBack**. • `2` – **Проводная сеть (Ethernet)**. • `3` – **Беспроводная сеть (Wi-Fi)**. • `4` – **Туннель**. • `5` – **PPP-соединение**. • `6` – **PPPoE-соединение**. • `7` – **VPN-соединение**. • `8` – **Модемное соединение**.
`unique`	Внутренний идентификатор структуры.	Integer Рекомендуем оставить этот параметр без изменений.
`Proto`	Значение параметра **Протокол**.	`0` – выключен. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.
`Direction`	Значение параметра **Направление**.	`1` – **Входящее (пакет)**. `2` – **Исходящее (пакет)**. `3` – **Входящее / Исходящее**. `4` – **Входящее**. `5` – **Исходящее**.

Параметр	Описание	Значение
`IcmpType`	Значение параметра **ICMP-тип**.	**Протокол ICMP** `0` – **Отклик на эхо-запрос** (ICMP) или выключен. `3` – **Цель недоступна** (ICMP). `4` – **Сдерживание (подавление) источника**. `5` – **Перенаправление маршрута**. `6` – **Альтернативный адрес хоста**. `8` – **Эхо-запрос**. `9` – **Объявление маршрутизатора**. `10` – **Запрос объявления маршрутизатора**. `11` – **Истекло время жизни пакета**. `12` – **Проблема с параметром**. `13` – **Запрос счетчика времени**. `14` – **Отклик на запрос счетчика времени**. `15` – **Запрос информации**. `16` – **Отклик на запрос информации**. `17` – **Запрос маски сети**. `18` – **Отклик на запрос маски сети**. `30` – **Отслеживание маршрута**. `31` – **Ошибка преобразования датаграммы**. `32` – **Перенаправление мобильного хоста**. `33` – **Запрос "Где ты" для IPv6**. `34` – **Ответ "Я здесь" для IPv6**. `35` – **Запрос перенаправления для мобильного узла**. `36` – **Отклик на запрос перенаправления для мобильного узла**. `37` – **Запрос имени домена**. `38` – **Отклик на запрос имени домена**. `40` – **Photuris**. **Протокол ICMPv6** `1` – **Цель недоступна**. `2` – **Размер пакета слишком велик**. `3` – **Истекло время жизни пакета**. `4` – **Проблема с параметром**. `128` – **Эхо-запрос**. `129` – **Отклик на эхо-запрос**. `130` – **Опрос потребителей многоадресных сообщений**. `131` – **Потребитель ожидает многоадресные сообщения с адреса**. `132` – **Потребитель многоадресных сообщений завершил прослушивание адреса**. `133` – **Запрос объявления маршрутизатора**. `134` – **Объявление маршрутизатора**. `135` – **Запрос объявления соседа**. `136` – **Объявление соседа**. `137` – **Перенаправление сообщения**. `138` – **Перенумерация роутера**. `139` – **Запрос информации об узле ICMP**. `141` – **Запрос объявления инверсного обнаружения соседнего узла**. `142` – **Объявление инверсного обнаружения соседнего узла**. `143` – **Потребитель ожидает многоадресные сообщения с адреса, версия 2**.

Параметр	Описание	Значение
		`144` – **Запрос на обнаружение адреса домашнего агента**. `145` – **Отклик на обнаружение адреса домашнего агента**. `146` – **Запрос мобильного префикса**. `147` – **Объявление мобильного префикса**. `148` – **Запрос сертификационного пути**. `149` – **Объявление сертификационного пути**. `151` – **Объявление маршрутизатора многоадресных сообщений**. `152` – **Запрос объявления маршрутизатора многоадресных сообщений**. `153` – **Прекращение функционирования в режиме маршрутизатора многоадресных сообщений**.
`IcmpCode`	Значение параметра **ICMP-код**.	`0` – **Код 0** или выключен. `1` – **Код 1**. `2` – **Код 2**.
`Flags`	Указатель атрибутов структуры.	Integer Рекомендуем оставить этот параметр без изменений.
`TTL`	Значение параметра **Время жизни (TTL)**.	Значение в секундах. Если выключен, значение `0`.
`</key>`		
`Id`	Основной идентификатор ресурса (см. узел `Rules`).	Integer
`ParentID`	Идентификатор родительской группы.	Integer Рекомендуем оставить этот параметр без изменений.
`Flags`	Статус правила.	`6` – правило выключено. `38` – правило включено.
`Name`	Название сетевого пакетного правила.	String

Работа с сетевыми правилами приложений

Kaspersky Endpoint Security по умолчанию группирует все приложения, установленные на компьютере пользователя, по названию производителей программного обеспечения, файловую и сетевую активность которого он контролирует. Группы приложений, в свою очередь, сгруппированы в группы доверия. Все приложения и группы приложений наследуют свойства своей родительской группы: правила контроля приложений, сетевые правила приложения, а также приоритет их выполнения.

Как и компонент Предотвращение вторжений, компонент Сетевой экран по умолчанию применяет сетевые правила группы приложений для фильтрации сетевой активности всех помещенных в группу приложений. Сетевые правила группы приложений определяют, какими правами доступа к различным сетевым соединениям обладают приложения, входящие в эту группу.

Сетевой экран по умолчанию создает набор сетевых правил для каждой группы приложений, которые Kaspersky Endpoint Security обнаружил на компьютере. Вы можете изменить действие Сетевого экрана для сетевых правил группы приложений, созданных по умолчанию. Вы не можете изменить, удалить или выключить сетевые правила группы приложений, созданные по умолчанию, а также изменить их приоритет.

Вы также можете создать сетевое правило для отдельного приложения. Такое правило будет иметь более высокий приоритет, чем сетевое правило группы, в которую входит это приложение.

Создание сетевого правила приложения

По умолчанию для контроля работы приложения применяются сетевые правила, определенные для той группы доверия, в которую Kaspersky Endpoint Security поместил приложение при первом ее запуске. При необходимости вы можете создать сетевые правила для всей группы доверия, для отдельного приложения или группы приложений внутри группы доверия.

Сетевые правила, заданные вручную, имеют более высокий приоритет, чем сетевые правила, определенные для группы доверия. То есть, если правила приложения, заданные вручную, отличаются от правил приложений, определенных для группы доверия, Сетевой экран контролирует работу приложения в соответствии с правилами приложений, заданными вручную.

Сетевой экран по умолчанию создает следующие сетевые правила для каждого приложения:

- Любая сетевая активность в Доверенных сетях.
- Любая сетевая активность в Локальных сетях.
- Любая сетевая активность в Публичных сетях.

Kaspersky Endpoint Security контролирует сетевую активность приложений по предустановленным сетевым правилам следующим образом:

- "Доверенные" и "Слабые ограничения" – любая сетевая активность разрешена.
- "Сильные ограничения" и "Недоверенные" – любая сетевая активность запрещена.

Предустановленные правила приложений невозможно изменить или удалить.

Вы можете создать сетевое правило приложения следующими способами:

- С помощью инструмента Мониторинг сети.

  Мониторинг сети – это инструмент, предназначенный для просмотра информации о сетевой активности компьютера пользователя в реальном времени. Этот способ удобен, так как вам не нужно настраивать все параметры правила. Некоторые параметры Сетевой экран подставит автоматически из данных Мониторинга сети. Мониторинг сети доступен только в интерфейсе приложения.

- В параметрах Сетевого экрана.

  Этот способ позволяет выполнить тонкую настройку параметров Сетевого экрана. Вы можете создать правила для любой сетевой активности, даже если сетевой активности нет в реальном времени.

Создавая сетевые правила приложений, следует помнить, что сетевые пакетные правила имеют приоритет над сетевыми правилами приложений.

Как создать сетевое правило приложения в интерфейсе приложения с помощью инструмента Мониторинг сети

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Мониторинг сети**.
2. Перейдите на вкладку **Сетевая активность** или **Открытые порты**.

   На вкладке **Сетевая активность** отображаются все активные на текущий момент сетевые соединения с компьютером пользователя. Приводятся как сетевые соединения, инициированные компьютером пользователя, так и входящие сетевые соединения.

   На вкладке **Открытые порты** перечислены все открытые сетевые порты на компьютере пользователя.
3. В контекстном меню сетевого соединения выберите пункт **Создать сетевое правило приложения**.

   Откроется окно свойств и правил приложения.
4. Выберите вкладку **Сетевые правила**.

   Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.
5. Нажмите на кнопку **Добавить**.

   Откроются свойства сетевого правила.
6. В поле **Название** введите название сетевой службы вручную.
7. Настройте параметры сетевого правила (см. таблицу ниже).

   Вы можете выбрать предустановленный шаблон правила по ссылке **Шаблон сетевого правила**. Шаблоны правила описывают наиболее часто используемые сетевые соединения.

   Все параметры сетевого правила будут заполнены автоматически.
8. Установите флажок **Записывать события**, если вы хотите, чтобы действие сетевого правила было отражено в отчете.
9. Нажмите на кнопку **Сохранить**.

   Новое сетевое правило будет добавлено в список.
10. Кнопками **Вверх** / **Вниз** установите приоритет сетевого правила.
11. Сохраните внесенные изменения.

Как создать сетевое правило приложения в интерфейсе приложения в параметрах Сетевого экрана

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Сетевой экран**.

3. Нажмите на кнопку **Правила приложений**.

   Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.

4. В списке приложений выберите приложение или группу приложений, для которого вы хотите создать сетевое правило.

5. По правой клавише мыши откройте контекстное меню и выберите пункт **Подробности и правила**.

   Откроется окно свойств и правил приложения.

6. Выберите вкладку **Сетевые правила**.

7. Нажмите на кнопку **Добавить**.

   Откроются свойства сетевого правила.

8. В поле **Название** введите название сетевой службы вручную.

9. Настройте параметры сетевого правила (см. таблицу ниже).

   Вы можете выбрать предустановленный шаблон правила по ссылке **Шаблон сетевого правила**. Шаблоны правила описывают наиболее часто используемые сетевые соединения.

   Все параметры сетевого правила будут заполнены автоматически.

10. Установите флажок **Записывать события**, если вы хотите, чтобы действие сетевого правила было отражено в отчете.

11. Нажмите на кнопку **Сохранить**.

    Новое сетевое правило будет добавлено в список.

12. Кнопками **Вверх** / **Вниз** установите приоритет сетевого правила.

13. Сохраните внесенные изменения.

Как создать сетевое правило приложения в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Базовая защита** → **Сетевой экран**.

4. В блоке **Настройки Сетевого экрана** нажмите на кнопку **Настройка**.

   Откроются список сетевых пакетных правил и список сетевых правил приложений.

5. Перейдите на вкладку **Сетевые правила приложений**.

6. Нажмите на кнопку **Добавить**.

7. В открывшемся окне задайте параметры поиска приложения, для которого вы хотите создать сетевое правило.

   Вы можете ввести название приложения или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.

8. Нажмите на кнопку **Обновить**.

   Kaspersky Endpoint Security выполнит поиск приложения в консолидированном списке приложений, установленных на управляемых компьютерах. Kaspersky Endpoint Security покажет список приложений, которые удовлетворяют параметрам поиска.

9. Выберите нужное приложение.

10. В раскрывающемся списке **Переместить приложение в группу доверия** выберите пункт **Исходные группы** и нажмите на кнопку **OK**.

    Приложение будет добавлено в исходную группу.

11. Выберите нужное приложение и в контекстном меню приложения выберите пункт **Права приложения**.

    Откроется окно свойств и правил приложения.

12. Выберите вкладку **Сетевые правила**.

    Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.

13. Нажмите на кнопку **Добавить**.

    Откроются свойства сетевого правила.

14. В поле **Название** введите название сетевой службы вручную.

15. Настройте параметры сетевого правила (см. таблицу ниже).

    Вы можете выбрать предустановленный шаблон правила по кнопке . Шаблоны правила описывают наиболее часто используемые сетевые соединения.

    Все параметры сетевого правила будут заполнены автоматически.

16. Установите флажок **Записывать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете.

17. Сохраните новое сетевое правило.

18. Кнопками **Вверх** / **Вниз** установите приоритет сетевого правила.

19. Сохраните внесенные изменения.

Как создать сетевое правило приложения в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Сетевой экран**.

5. В блоке **Права приложений и защищаемые ресурсы** нажмите на ссылку **Права приложений**.

   Откроется окно настройки прав приложений и список защищаемых ресурсов.

6. Перейдите на вкладку **Права приложений**.

   Откроется список групп доверия в левой части окна и их свойства в правой части.

7. В блоке **Приложения** нажмите на кнопку **Добавить**.

   Запустится мастер добавления приложения в группу доверия.

8. Выберите группу доверия, в которую вы хотите поместить приложение.

9. Выберите тип **Приложение**. Перейдите к следующему шагу.

   Если вы хотите создать сетевое правило для нескольких приложений, выберите тип **Группа** и задайте имя группы приложений.

10. В открывшемся списке приложений выберите приложения, для которых вы хотите создать сетевое правило.

    Используйте фильтр. Вы можете ввести название приложения или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

11. Завершите работу мастера.

    Приложение будет добавлено в группу доверия.

12. В левой части окна выберите нужное приложение.

13. В правой части окна в раскрывающемся списке выберите пункт **Сетевые правила**.

    Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.

14. Нажмите на кнопку **Добавить**.

    Откроются свойства правила приложения.

15. В поле **Имя правила** введите название сетевой службы вручную.

16. Настройте параметры сетевого правила (см. таблицу ниже).

    Вы можете выбрать предустановленный шаблон правила по ссылке **Выбрать шаблон правила**. Шаблоны правила описывают наиболее часто используемые сетевые соединения.

    Все параметры сетевого правила будут заполнены автоматически.

17. Установите флажок **Записывать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете.

18. Сохраните сетевое правило.

    Новое сетевое правило будет добавлено в список.

19. С помощью кнопки **Переместить** установите приоритет сетевого правила.

20. Сохраните внесенные изменения.

Параметры сетевого правила приложения

Параметр	Описание
Действие	**Разрешать**. **Запрещать**.
Протокол	Контроль сетевой активности по выбранному протоколу: TCP, UDP, ICMP, ICMPv6, IGMP и GRE. Если в качестве протокола выбран протокол ICMP или ICMPv6, вы можете задать тип и код ICMP-пакета. Если в качестве протокола выбран протокол TCP или UDP, вы можете указать номера портов компьютера пользователя и удаленного компьютера, соединение между которыми следует контролировать. Диапазон возможных значений номеров порта: 0–65535. В каждом поле вы можете указать несколько значений, разделенных `,`, или задать диапазон значений через `-`. Например: • `100,101`; • `100-130`; • `100,110-130`.
Направление	**Входящее**. **Входящее / Исходящее**. **Исходящее**.
Удаленные адреса	Сетевые адреса удаленных компьютеров, которые могут передавать / получать сетевые пакеты. К заданному диапазону удаленных сетевых адресов Сетевой экран применяет сетевое правило. Вы можете включить в сетевое правило все IP-адреса, создать отдельный список IP-адресов, указать диапазон IP-адресов или выбрать подсеть (Доверенные сети, Локальные сети, Публичные сети). Также вместо IP-адреса вы можете указать DNS-имя компьютера. Используйте DNS-имена только для компьютеров локальной сети или внутренних сервисов. Для работы с облачными сервисами (например, Microsoft Azure) и другими интернет-ресурсами предназначен компонент Веб-Контроль. Если в сетевом пакетном правиле вы добавили DNS-имя, для которого не удалось определить IP-адрес, Kaspersky Endpoint Security предупредит вас об этом. В списке сетевых пакетных правил в Web Console будет добавлена графа с описанием ошибки. В Консоли администрирования (MMC) описание ошибки недоступно. Такое пакетное правило будет выделено цветом.
Локальные адреса	Сетевые адреса компьютеров, которые могут передавать / получать сетевые пакеты. К заданному диапазону локальных сетевых адресов Сетевой экран применяет сетевое правило. Вы можете включить в сетевое правило все IP-адреса, создать отдельный список IP-адресов или указать диапазон IP-адресов. Приложение сохраняет локальные адреса, только если задан список удаленных адресов. То есть для параметра **Удаленные адреса** выбрано значение **Адреса из списка** и добавлен хотя бы один адрес. Для приложений не всегда возможно получить локальный адрес. В этом случае этот параметр игнорируется.

Включение и выключение сетевого правила приложений

Чтобы включить или выключить сетевое правило приложений, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Сетевой экран**.
3. Нажмите на кнопку **Правила приложений**.

   Откроется список правил приложений.
4. В списке приложений выберите приложение или группу приложений, для которой вы хотите создать или изменить сетевое правило.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Подробности и правила**.

   Откроется окно свойств и правил приложения.
6. Выберите вкладку **Сетевые правила**.

7. В списке сетевых правил группы приложений выберите нужное вам сетевое правило.

   Откроется окно свойств сетевого правила.

8. Установите статус сетевого правила **Активно** или **Неактивно**.

   Вы не можете выключить сетевое правило группы приложений, если оно создано Сетевым экраном по умолчанию.

9. Сохраните внесенные изменения.

Изменение действия Сетевого экрана для сетевого правила приложений

Вы можете изменить действие Сетевого экрана для всех сетевых правил приложения или группы приложений, которые были созданы по умолчанию, а также изменить действие Сетевого экрана для одного сетевого правила приложения или группы приложений, которое было создано вручную.

Чтобы изменить действие Сетевого экрана для всех сетевых правил приложения или группы приложений, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Сетевой экран**.

3. Нажмите на кнопку **Правила приложений**.

   Откроется список правил приложений.

4. В списке выберите приложение или группу приложений, если вы хотите изменить действие Сетевого экрана для всех ее сетевых правил, созданных по умолчанию. Сетевые правила, созданные вручную, останутся без изменений.

5. По правой клавише мыши откройте контекстное меню и выберите пункт **Сетевые правила** и выберите действие, которое вы хотите назначить:

   - **Наследовать**.
   - **Разрешить**.
   - **Блокировать**.

6. Сохраните внесенные изменения.

Чтобы изменить действие Сетевого экрана для одного сетевого правила приложения или группы приложений, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Сетевой экран**.

3. Нажмите на кнопку **Правила приложений**.

   Откроется список правил приложений.

4. В списке выберите приложение или группу приложений, для которого вы хотите изменить действие одного сетевого правила.

5. По правой клавише мыши откройте контекстное меню и выберите пункт **Подробности и правила**.

   Откроется окно свойств и правил приложения.

6. Выберите вкладку **Сетевые правила**.

7. Выберите сетевое правило, для которого вы хотите изменить действие Сетевого экрана.

8. В графе **Разрешение** по правой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:

   - **Наследовать**.
   - **Разрешить**.
   - **Запретить**.
   - **Записывать в отчет**.

9. Сохраните внесенные изменения.

Изменение приоритета сетевого правила приложений

Приоритет выполнения сетевого правила определяется его положением в списке сетевых правил. Сетевой экран выполняет правила в порядке их расположения в списке сетевых правил, сверху вниз. Согласно каждому обрабатываемому сетевому правилу, применяемому к определенному сетевому соединению, Сетевой экран либо разрешает, либо блокирует сетевой доступ к адресу и порту, указанным в настройках этого сетевого соединения.

Созданные вручную сетевые правила имеют более высокий приоритет, чем сетевые правила, созданные по умолчанию.

Вы не можете изменить приоритет сетевых правил группы приложений, созданных по умолчанию.

Чтобы изменить приоритет сетевого правила, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Базовая защита** и нажмите на плитку **Сетевой экран**.

3. Нажмите на кнопку **Правила приложений**.

   Откроется список правил приложений.

4. В списке приложений выберите приложение или группу приложений, для которого вы хотите изменить приоритет сетевого правила.

5. По правой клавише мыши откройте контекстное меню и выберите пункт **Подробности и правила**.

   Откроется окно свойств и правил приложения.

6. Выберите вкладку **Сетевые правила**.

7. Выберите сетевое правило, приоритет которого вы хотите изменить.

8. Кнопками **Вверх** / **Вниз** установите приоритет сетевого правила.

9. Сохраните внесенные изменения.

Мониторинг сети

Мониторинг сети – это инструмент, предназначенный для просмотра информации о сетевой активности компьютера пользователя в реальном времени.

Чтобы запустить Мониторинг сети,

в главном окне приложения в разделе **Мониторинг** нажмите на плитку **Мониторинг сети**.

Откроется окно Мониторинга сети. В этом окне информация о сетевой активности компьютера пользователя представлена на четырех вкладках:

- На вкладке **Сетевая активность** отображаются все активные на текущий момент сетевые соединения с компьютером пользователя. Приводятся как сетевые соединения, инициированные компьютером пользователя, так и входящие сетевые соединения. На этой вкладке вы также можете создавать сетевые пакетные правила для работы Сетевого экрана.
- На вкладке **Открытые порты** перечислены все открытые сетевые порты на компьютере пользователя. На этой вкладке вы также можете создавать сетевые пакетные правила и правила приложения для работы Сетевого экрана.
- На вкладке **Сетевой трафик** отображается объем входящего и исходящего сетевого трафика между компьютером пользователя и другими компьютерами сети, в которой пользователь работает в текущий момент.
- На вкладке **Заблокированные компьютеры** представлен список IP-адресов удаленных компьютеров, сетевую активность которых компонент Защита от сетевых угроз заблокировал, обнаружив попытку сетевой атаки с этого IP-адреса.

Защита от эксплойтов

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимое приложение. При обработке этих данных уязвимое приложение выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО. Если попытка запустить исполняемый файл из уязвимого приложения не была произведена пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла или информирует пользователя.

Компонент Защита от эксплойтов дополнительно контролирует сетевые порты для процессов приложений, которые могут представлять угрозу безопасности компьютера. Приложение получает данные о таких процессах с антивирусными базами.

Включение и выключение Защиты от эксплойтов

По умолчанию компонент Защита от эксплойтов включен и работает в оптимальном режиме. Kaspersky Endpoint Security будет отслеживать исполняемые файлы, запускаемые уязвимыми приложениями. Если Kaspersky Endpoint Security обнаруживает, что исполняемый файл из уязвимого приложения был запущен не пользователем, то Kaspersky Endpoint Security выполняет выбранное действие (например, блокирует операцию).

Как включить или выключить Защиту от эксплойтов в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Продвинутая защита → Защита от эксплойтов**
4. Используйте флажок **Защита от эксплойтов**, чтобы включить или выключить компонент.
5. В блоке **При обнаружении эксплойта** выберите нужное действие:
   - **Блокировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security блокирует операции этого эксплойта и создает в журнале запись, содержащую информацию об этом эксплойте.
   - **Информировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security создает в журнале запись, содержащую информацию об этом эксплойте, и добавляет информацию об этом эксплойте в список активных угроз.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить Защиту от эксплойтов в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз → Защита на основе анализа поведения → Защита от эксплойтов**.
5. Используйте переключатель **Защита от эксплойтов**, чтобы включить или выключить компонент.

6. В блоке **Действие при обнаружении угрозы** выберите нужное действие:

   - **Блокировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security блокирует операции этого эксплойта и создает в журнале запись, содержащую информацию об этом эксплойте.

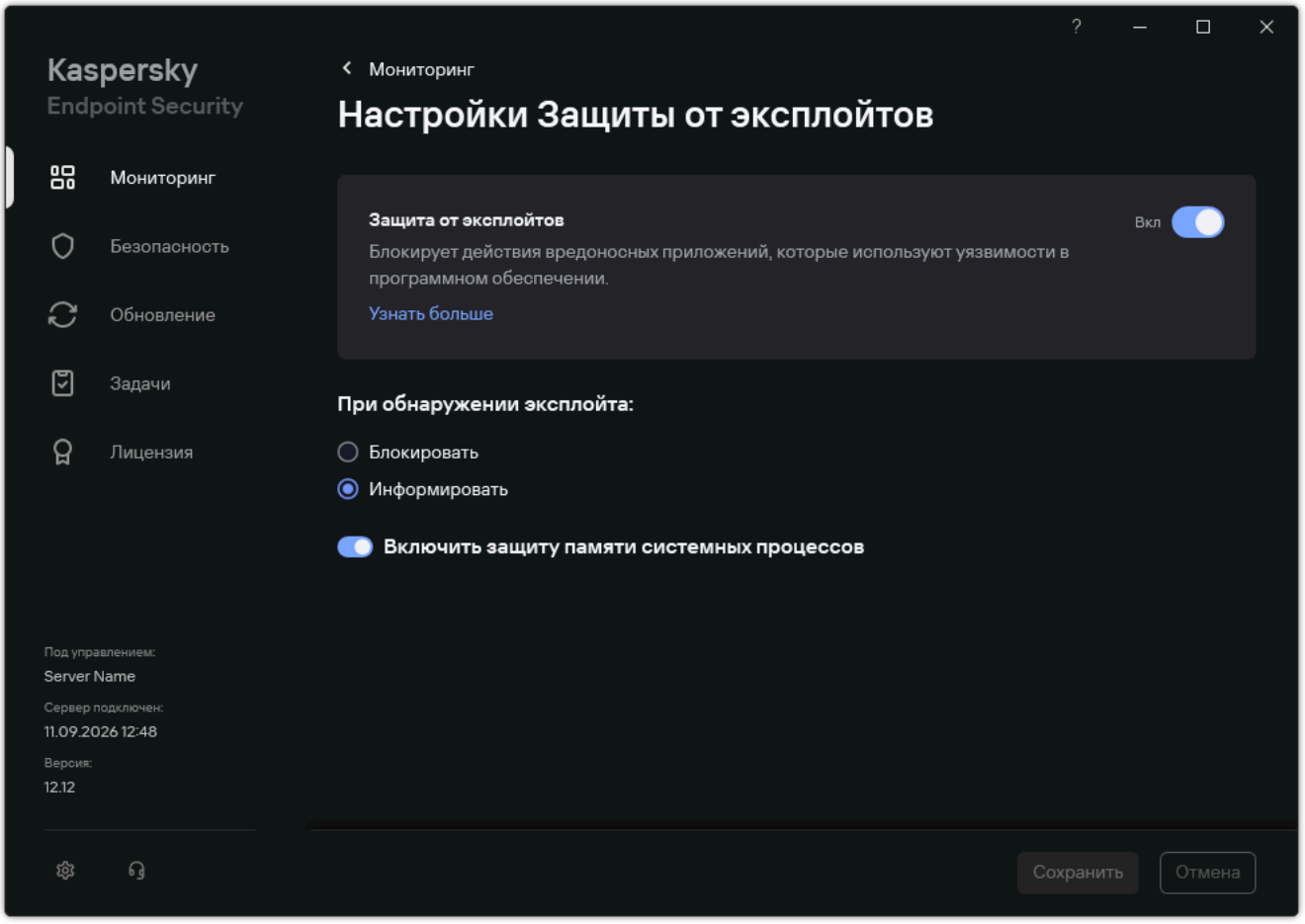
   - **Информировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security создает в журнале запись, содержащую информацию об этом эксплойте, и добавляет информацию об этом эксплойте в список активных угроз.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить Защиту от эксплойтов в интерфейсе приложении

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от эксплойтов**.



Параметры Защиты от эксплойтов

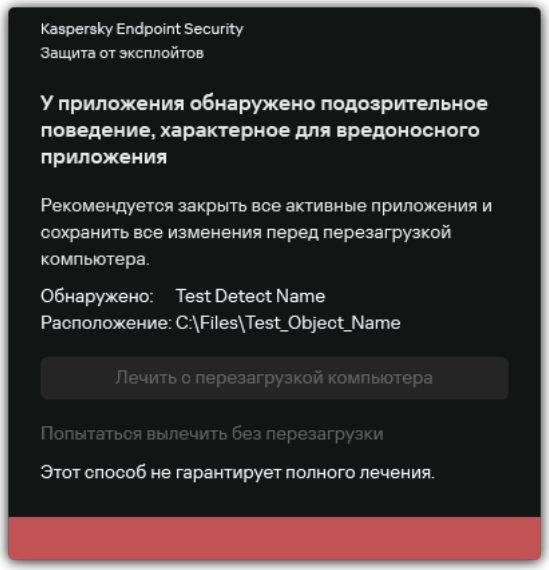
3. Используйте переключатель **Защита от эксплойтов**, чтобы включить или выключить компонент.

4. В блоке **При обнаружении эксплойта** выберите нужное действие:

   - **Блокировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security блокирует операции этого эксплойта и создает в журнале запись, содержащую информацию об этом эксплойте.

   - **Информировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security создает в журнале запись, содержащую информацию об этом эксплойте, и добавляет информацию об этом эксплойте в список активных угроз.

5. Сохраните внесенные изменения.



Уведомление об активной угрозе

Защита памяти системных процессов

По умолчанию защита памяти системных процессов включена. Kaspersky Endpoint Security блокирует сторонние процессы, которые осуществляют попытки доступа к системным процессам.

Как включить или выключить защиту памяти системных процессов в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита → Защита от эксплойтов**.

4. Используйте флажок **Включить защиту памяти системных процессов**, чтобы включить или выключить функцию.

5. Сохраните внесенные изменения.

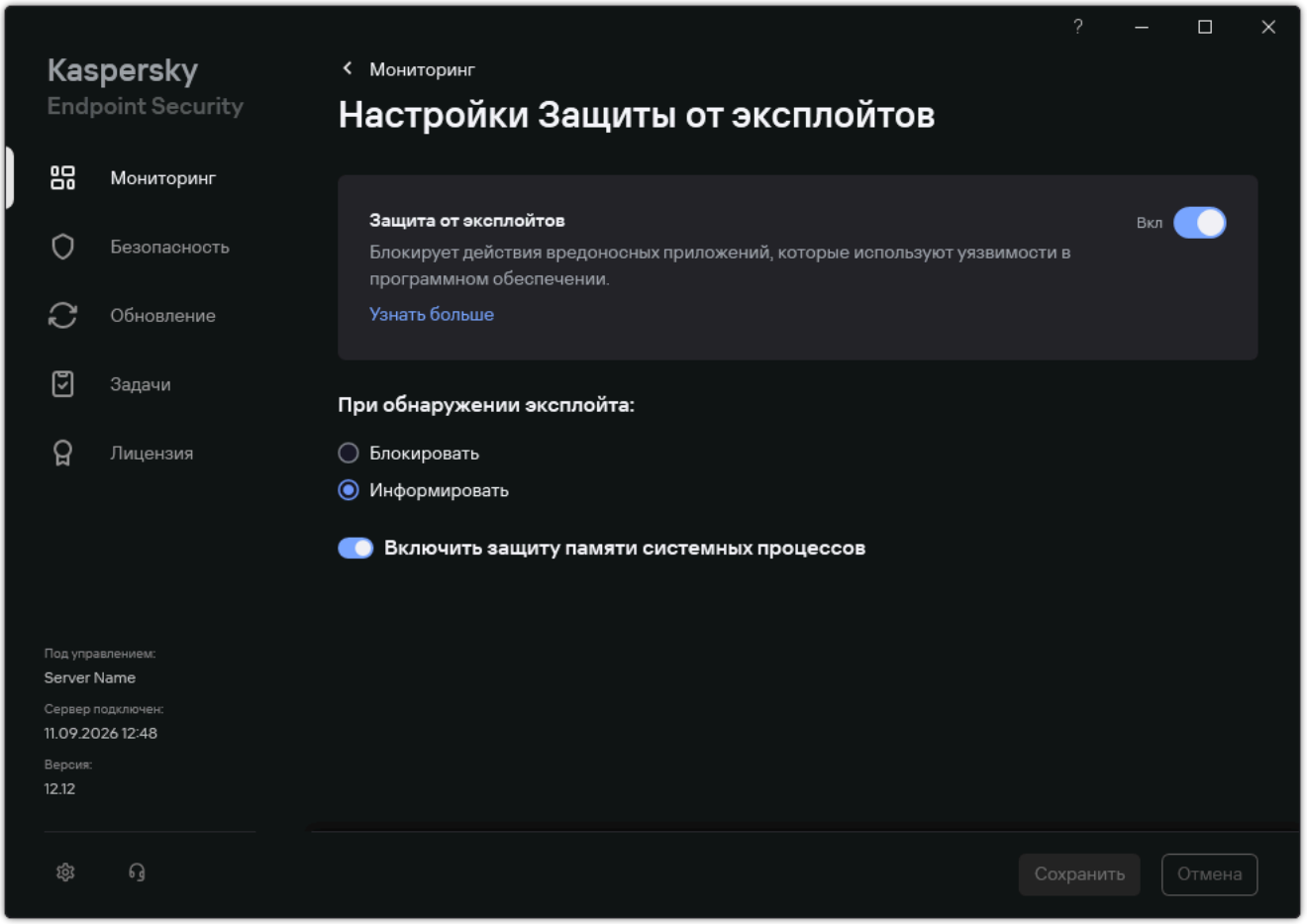
Как включить или выключить защиту памяти системных процессов в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Защита на основе анализа поведения** → **Защита от эксплойтов**.
5. Используйте переключатель **Защита памяти системных процессов ВКЛЮЧЕНА**, чтобы включить или выключить функцию.
6. Сохраните внесенные изменения.

Как включить ли выключить защиту памяти системных процессов в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от эксплойтов**.



Параметры Защиты от эксплойтов

3. Используйте переключатель **Включить защиту памяти системных процессов**, чтобы включить или выключить функцию.
4. Сохраните внесенные изменения.

Анализ поведения

Компонент Анализ поведения получает данные о действиях приложений на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы. Компонент Анализ поведения использует шаблоны опасного поведения приложений. Если активность приложения совпадает с одним из шаблонов опасного поведения, Kaspersky Endpoint Security выполняет выбранное ответное действие. Функциональность Kaspersky Endpoint Security, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

Компонент Анализ поведения дополнительно контролирует сетевые порты для процессов приложений, которые могут представлять угрозу безопасности компьютера. Приложение получает данные о таких процессах с антивирусными базами.

По умолчанию Анализ поведения включен и работает в режиме, рекомендованном специалистами "Лаборатории Касперского". При обнаружении вредоносной активности Kaspersky Endpoint Security удаляет исполняемый файл вредоносного приложения.

Не рекомендуется выключать Анализ поведения без необходимости, так как это снижает эффективность работы компонентов защиты. Компоненты защиты могут запрашивать данные, полученные компонентом Анализ поведения, для обнаружения угроз.

Как включить или выключить Анализ поведения в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Продвинутая защита** → **Анализ поведения**.
5. Используйте флажок **Анализ поведения**, чтобы включить или выключить компонент.
6. В блоке **Действие при обнаружении вредоносной активности** выберите нужное действие:
   - **Удалять**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security удаляет исполняемый файл вредоносного приложения и создает резервную копию файла в резервном хранилище.
   - **Блокировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security завершает работу этого приложения.
   - **Информировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security добавляет информацию о вредоносной активности этого приложения в список активных угроз.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить Анализ поведения в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

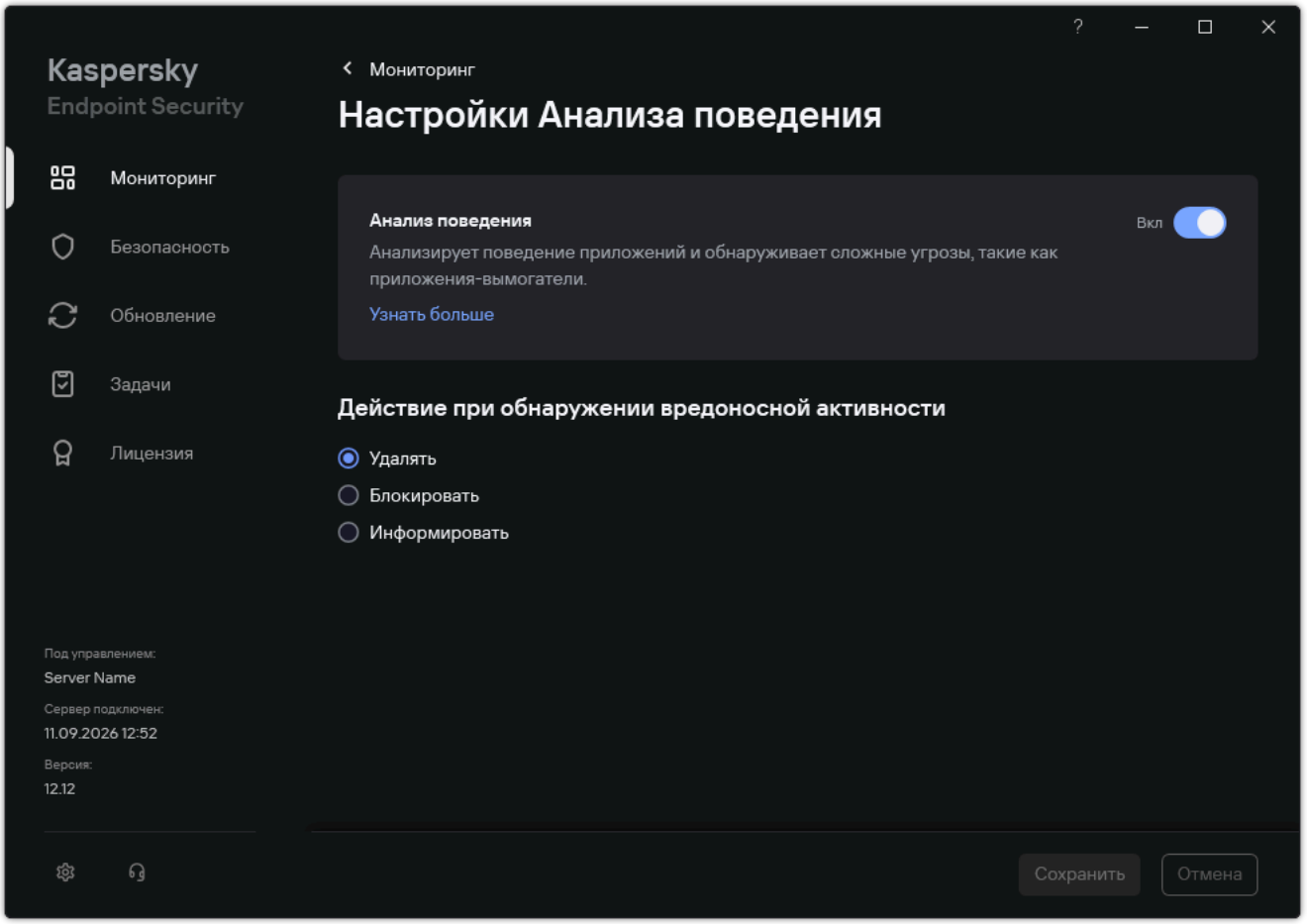
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз → Защита на основе анализа поведения → Анализ поведения**
5. Используйте переключатель **Анализ поведения ВКЛЮЧЕН**, чтобы включить или выключить компонент.
6. В блоке **Действие при обнаружении угрозы** выберите нужное действие:

   - **Удалить**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security удаляет исполняемый файл вредоносного приложения и создает резервную копию файла в резервном хранилище.
   - **Блокировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security завершает работу этого приложения.
   - **Информировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security добавляет информацию о вредоносной активности этого приложения в список активных угроз.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить Анализ поведения в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Анализ поведения**.



Параметры Анализа поведения

3. Используйте переключатель **Анализ поведения**, чтобы включить или выключить компонент.

4. В блоке **Действие при обнаружении вредоносной активности** выберите нужное действие:

   - **Удалять**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security удаляет исполняемый файл вредоносного приложения и создает резервную копию файла в резервном хранилище.

   - **Блокировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security завершает работу этого приложения.

   - **Информировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security добавляет информацию о вредоносной активности этого приложения в список активных угроз.

5. Сохраните внесенные изменения.

В результате, если Анализ поведения включен, Kaspersky Endpoint Security будет анализировать активность приложений в операционной системе, используя шаблоны опасного поведения.

Защита от шифрования

Начиная с версии Kaspersky Endpoint Security для Windows 12.12 функция защиты папок общего доступа от внешнего шифрования, которая входила в состав компонента Анализ поведения, выделена в отдельный компонент Защита от шифрования.

Компонент обеспечивает отслеживание операций только над теми файлами, которые расположены на запоминающих устройствах с файловой системой NTFS и не зашифрованы системой EFS.

Компонент Защита от шифрования обеспечивает анализ активности в папках общего доступа. Если активность совпадает с одним из шаблонов поведения, характерного для внешнего шифрования, Kaspersky Endpoint Security выполняет выбранное действие.

Для работы компонента Защита от шифрования необходимо включить компонент Анализ поведения.

При обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security выполняет следующие действия:

- блокирует доступ на изменение файлов для сессии, которая инициировала вредоносную активность (файл доступен только на чтение);
- создает резервные копии подверженных изменению файлов;
- добавляет запись в отчеты локального интерфейса приложения и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности;
- если при этом включен компонент Откат вредоносных действий, то выполняется восстановление измененных файлов из резервных копий.

Включение и выключение защиты папок общего доступа от внешнего шифрования

По умолчанию функция защиты папок общего доступа от внешнего шифрования включена и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для настройки функции вы можете сформировать область защиты, а также задать исключения, если требуется. По умолчанию приложение автоматически определяет папки общего доступа и отслеживает файловую активность во всех папках. При обнаружении попытки внешнего шифрования файлов в папках общего доступа Kaspersky Endpoint Security блокирует сессию удаленного пользователя на один час (по умолчанию).

После установки Kaspersky Endpoint Security функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки компьютера.

Как включить или выключить защиту папок общего доступа от внешнего шифрования в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Продвинутая защита → Защита от шифрования**.
4. Используйте флажок **Защита от шифрования**, чтобы включить или выключить анализ активности, характерную для внешнего шифрования.
5. Выберите нужное действие приложения при обнаружении попытки изменения файлов в папках общего доступа:
   - **Блокировать соединение на N мин**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security блокирует доступ на изменение файлов для сессии, которая инициировала вредоносную активность, и создает резервные копии измененных файлов.

     Если включен компонент Откат вредоносных действий и выбран вариант **Блокировать соединение на N мин**, то выполняется восстановление измененных файлов из резервных копий.

   - **Информировать**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security добавляет информацию об этой попытке изменения файлов в папках общего доступа в список активных угроз, добавляет запись в отчеты локального интерфейса приложения и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.
6. Если требуется сформируйте область защиты и задайте исключения.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить защиту папок общего доступа от внешнего шифрования в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз → Защита на основе анализа поведения → Защита от шифрования**.
5. Используйте переключатель **Защита от шифрования ВКЛЮЧЕНА**, чтобы включить или выключить анализ активности, характерную для внешнего шифрования.

6. Выберите нужное действие приложения при обнаружении попытки изменения файлов в папках общего доступа:

   - **Блокировать соединение на (мин) N мин**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security блокирует доступ на изменение файлов для сессии, которая инициировала вредоносную активность, и создает резервные копии измененных файлов.

     Если включен компонент Откат вредоносных действий и выбран вариант **Блокировать соединение на (мин) N мин**, то выполняется восстановление измененных файлов из резервных копий.

   - **Информировать**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security добавляет информацию об этой попытке изменения файлов в папках общего доступа в список активных угроз, добавляет запись в отчеты локального интерфейса приложения и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.

7. Если требуется сформируйте область защиты и задайте исключения.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить защиту папок общего доступа от внешнего шифрования в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от шифрования**.

3. Используйте флажок **Защита папок общего доступа от внешнего шифрования**, чтобы включить или выключить анализ активности, характерную для внешнего шифрования.

4. Используйте флажок **Защита папок общего доступа от внешнего шифрования**, чтобы включить или выключить анализ активности, характерную для внешнего шифрования.

5. Выберите нужное действие приложения при обнаружении попытки изменения файлов в папках общего доступа:

   - **Блокировать соединение на (мин) N мин**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security блокирует доступ на изменение файлов для сессии, которая инициировала вредоносную активность, и создает резервные копии измененных файлов.

     Если включен компонент Откат вредоносных действий и выбран вариант **Блокировать соединение на (мин) N мин**, то выполняется восстановление измененных файлов из резервных копий.

   - **Информировать**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security добавляет информацию об этой попытке изменения файлов в папках общего доступа в список активных угроз, добавляет запись в отчеты локального интерфейса приложения и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.

6. Если требуется сформируйте область защиты и задайте исключения.

7. Сохраните внесенные изменения.

Настройка периода блокировки недоверенного компьютера

Недоверенный компьютер – удаленный компьютер, с которого ведется вредоносная активность или шифрование данных. По умолчанию Kaspersky Endpoint Security блокирует сессию удаленного пользователя на один час. По истечении периода блокировки Kaspersky Endpoint Security удаляет компьютер из списка заблокированных и восстанавливает доступ к папке общего доступа.

Как настроить период блокировки недоверенного компьютера в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита → Защита от шифрования**.

4. В блоке **Действие при обнаружении угрозы** выберите вариант **Блокировать соединение на N мин**.

5. Настройте период блокировки удаленного компьютера, с которого ведется вредоносная активность или шифрование данных.

6. Сохраните внесенные изменения.

Как настроить период блокировки недоверенного компьютера в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз → Защита на основе анализа поведения → Защита от шифрования**.

5. В блоке **Действие при обнаружении угрозы** настройте период блокировки удаленного компьютера, с которого ведется вредоносная активность или шифрование данных.

6. Сохраните внесенные изменения.

Как настроить период блокировки недоверенного компьютера в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от шифрования**.

3. В блоке **Действие при обнаружении угрозы** выберите вариант **Блокировать соединение на (мин)**.

4. Настройте период блокировки удаленного компьютера, с которого ведется вредоносная активность или шифрование данных.

5. Сохраните внесенные изменения.

В результате удаленный компьютер будет заблокирован. Для разблокировки удаленного компьютера вы можете перезапустить Kaspersky Endpoint Security.

Формирование области защиты

Область защиты – список путей к папкам общего доступа, в которых Kaspersky Endpoint Security отслеживает файловую активность. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. По умолчанию приложение автоматически определяет папки общего доступа и отслеживает файловую активность во всех папках.

Исключение папки из области защиты позволит сократить количество ложных срабатываний, если в вашей организации используется шифрование данных при обмене файлами с помощью папок общего доступа. Например, Анализ поведения может создавать ложные срабатывания при работе пользователя с файлами с расширением ENC в папке общего доступа. Такая активность совпадает с шаблоном поведения, характерного для внешнего шифрования. Если вы зашифровали файлы в папке общего доступа для защиты данных, добавьте эту папку в исключения.

Вы также можете исключить компьютеры, попытки внешнего шифрования с которого, не должны обрабатываться.

Как сформировать область защиты в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита** → **Защита от шифрования**.

4. В блоке **Область защиты** выберите вариант **Только указанные общие папки**.

5. В списке папок нажмите на кнопку **Добавить**.

6. В открывшемся окне введите путь к папке общего доступа, которую вы хотите включить область защиты (например, `C:\Share`).

   Для добавления папки общего доступа в область защиты используйте локальный путь.

7. Нажмите на кнопку **OK**.

8. Если требуется, задайте исключения из области защиты:

   a. В блоке **Исключения из проверки** нажмите на кнопку **По маске**.

   b. В открывшемся окне нажмите на кнопку **Добавить**.

c. В открывшемся окне укажите расширение файла в формате `*.<file extension>` или путь к папке. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

Приложение не поддерживает некоторые расширения файлов для исключений. Таким образом, вы можете указать исключение в следующем виде `*.docx` или `**\Folder\**`.

Вы можете исключить объект из проверки, не удаляя его из списка объектов области защиты. Для этого снимите флажок рядом с ним.

9. Сохраните внесенные изменения.

Как сформировать область защиты в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз → Защита на основе анализа поведения → Защита от шифрования**.
5. В блоке **Область защиты** выберите вариант **Только указанные общие папки**.
6. В списке папок нажмите на кнопку **Добавить**.
7. В открывшемся окне введите путь к папке общего доступа, которую вы хотите включить область защиты (например, `C:\Share`).

   Для добавления папки общего доступа в область защиты используйте локальный путь.
8. Нажмите на кнопку **OK**.
9. Если требуется, задайте исключения из области защиты:

   a. В верхней части окна перейдите по ссылке **Исключения из проверки**.

   b. В открывшемся окне нажмите на кнопку **Добавить**.

   c. В открывшемся окне укажите расширение файла в формате `*.<file extension>` или путь к папке. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

   Приложение не поддерживает некоторые расширения файлов для исключений. Таким образом, вы можете указать исключение в следующем виде `*.docx` или `**\Folder\**`.

   Вы можете исключить объект из проверки, не удаляя его из списка объектов области защиты. Для этого снимите флажок рядом с ним.
10. Сохраните внесенные изменения.

Как сформировать область защиты в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от шифрования**.
3. В блоке **Область защиты** выберите вариант **Только указанные общие папки**.
4. В списке папок нажмите на кнопку **Добавить**.
5. В открывшемся окне введите путь к папке общего доступа, которую вы хотите включить область защиты (например, `C:\Share`).

   > Для добавления папки общего доступа в область защиты используйте локальный путь.

6. Нажмите на кнопку **OK**.
7. Если требуется, задайте исключения из области защиты:

   a. В верхней части окна перейдите по ссылке **Исключения по маске**.

   b. В открывшемся окне нажмите на кнопку **Добавить**.

   c. В открывшемся окне укажите расширение файла в формате `*.<file extension>` или путь к папке. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

   Приложение не поддерживает некоторые расширения файлов для исключений. Таким образом, вы можете указать исключение в следующем виде `*.docx` или `**\Folder\**`.

   Вы можете исключить объект из проверки, не удаляя его из списка объектов области защиты. Для этого снимите флажок рядом с ним.

8. Сохраните внесенные изменения.

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.
3. В блоке **Исключения** перейдите по ссылке **Настроить исключения**.
4. Нажмите на кнопку **Добавить**.
5. Выберите папку общего доступа, нажав на кнопку **Обзор**.

Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `?:\Users\*\Folder\`.

6. В блоке **Компоненты защиты** выберите компонент **Анализ поведения**.

7. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

8. Установите статус для исключения **Активно**.

   Вы можете в любое время остановить работу исключения с помощью переключателя.

9. Сохраните внесенные изменения.

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Доверенная зона**.

5. В открывшемся окне перейдите по ссылке **Исключения из Поиска вредоносного ПО**.

6. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список исключений для всех компьютеров организации. Списки исключений родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Исключения родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление исключений родительской политики невозможно.

7. Установите флажок **Разрешить использование локальных исключений**, если вы хотите чтобы у пользователя была возможность создать локальный список исключений. Таким образом, кроме общего списка исключений, сформированного в политике, пользователь может создавать собственный локальный список исключений. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера.

   Если флажок снят, пользователю доступен только общий список исключений, сформированный в политике. Также, если флажок снят, Kaspersky Endpoint Security скрывает для просмотра общий список исключений из проверки в интерфейсе приложения.

8. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категория**. Вы можете группировать исключения из проверки в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно исключение из проверки.

   - **Новое исключение**. Kaspersky Endpoint Security добавляет новое исключение из проверки в корень списка.

   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные исключения из проверки*. Также в приложение добавлены предустановленные исключения из проверки для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные исключения из проверки.

9. Выберите способ добавления исключения **Путь к файлу или папке**.

10. Введите путь к папке общего доступа.

    Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски:

    - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

    - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

    - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

    Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `C:\Users\*\Folder\`.

11. В блоке **Применить исключение к** выберите компонент **Анализ поведения**.

12. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

13. Установите статус для исключения **Добавить в исключения**.

    Вы можете в любое время остановить работу исключения с помощью переключателя.

14. Сохраните внесенные изменения.

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Общие настройки** → **Исключения и типы объектов**.

4. В блоке **Исключения из проверки и доверенные приложения** → **Исключения из проверки** нажмите на кнопку **Настройка**.

   Откроется окно со списком исключений.

5. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список исключений для всех компьютеров организации. Списки исключений родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Исключения родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление исключений родительской политики невозможно.

6. Установите флажок **Разрешить использование локальных исключений**, если вы хотите чтобы у пользователя была возможность создать локальный список исключений. Таким образом, кроме общего списка исключений, сформированного в политике, пользователь может создавать собственный локальный список исключений. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера.

   Если флажок снят, пользователю доступен только общий список исключений, сформированный в политике. Также, если флажок снят, Kaspersky Endpoint Security скрывает для просмотра общий список исключений из проверки в интерфейсе приложения.

7. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категорию**. Вы можете группировать исключения из проверки в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно исключение из проверки.

   - **Новое исключение**. Kaspersky Endpoint Security добавляет новое исключение из проверки в корень списка.

   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные исключения из проверки*. Также в приложение добавлены предустановленные исключения из проверки для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные исключения из проверки.

8. Нажмите на кнопку **Добавить**.

9. В блоке **Свойства** установите флажок **Файл или папка**.

10. По ссылке **Выберите файл или папку**, расположенной в блоке **Описание исключения из проверки (нажмите на подчеркнутые элементы для их изменения)**, откройте окно **Имя файла или папки**.

11. Выберите папку общего доступа, нажав на кнопку **Обзор**.

Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `?:\Users\*\Folder\`.

12. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

13. По ссылке, расположенной в блоке **Описание исключения из проверки (нажмите на подчеркнутые элементы для их изменения)**, откройте окно **Компоненты защиты**.

14. Установите флажок напротив компонента **Анализ поведения**.

15. Сохраните внесенные изменения.

Добавление доверенных компьютеров для внешнего шифрования данных

Если в вашей организации используется внешнее шифрование данных при обмене файлами, вам нужно сформировать список доверенных компьютеров. Kaspersky Endpoint Security не отслеживает шифрование данных с доверенных компьютеров.

Для работы функциональности исключений адресов из защиты папок общего доступа от внешнего шифрования необходимо включить службу Аудит входа в систему. По умолчанию служба Аудит входа в систему выключена (подробную информацию о включении службы Аудит входа в систему см. на сайте корпорации Microsoft).

Функциональность исключений адресов из защиты папок общего доступа не работает на удаленном компьютере, если этот удаленный компьютер был включен до запуска Kaspersky Endpoint Security. Вы можете перезагрузить этот удаленный компьютер после запуска Kaspersky Endpoint Security, чтобы обеспечить работу функциональности исключений адресов из защиты папок общего доступа на этом удаленном компьютере.

Как добавить доверенный компьютер для внешнего шифрования данных в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Продвинутая защита → Защита от шифрования**.
5. В блоке **Исключения из проверки** нажмите на кнопку **По имени или IP-адресу**.
6. В открывшемся окне нажмите на кнопку **По имени или IP-адресу**.
7. Введите IP-адреса компьютеров, диапазон IP-адресов или имена компьютеров, попытки внешнего шифрования с которых не должны обрабатываться.

   Примеры:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как добавить доверенный компьютер для внешнего шифрования данных в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона**.
5. В правой части окна перейдите по ссылке **Исключения из Защиты от шифрования**.
6. В открывшемся окне нажмите на кнопку **Добавить**.
7. Введите IP-адреса компьютеров, диапазон IP-адресов или имена компьютеров, попытки внешнего шифрования с которых не должны обрабатываться.

   Примеры:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`

- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как добавить доверенный компьютер для внешнего шифрования данных в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Защита от шифрования**.
3. В верхней части окна перейдите по ссылке **Исключения по имени или IP-адресу**.
4. В открывшемся окне нажмите на кнопку **Добавить**.
5. Введите IP-адреса компьютеров, диапазон IP-адресов или имена компьютеров, попытки внешнего шифрования с которых не должны обрабатываться.

   Примеры:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

6. Сохраните внесенные изменения.

Экспорт и импорт списка исключений из защиты папок общего доступа от внешнего шифрования

Вы можете экспортировать список исключений в файл формата XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных адресов. Также вы можете использовать функцию экспорта / импорта для резервного копирования списка исключений или для миграции списка на другой сервер.

Как экспортировать / импортировать список исключений в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Продвинутая защита** → **Защита от шифрования**.
4. В блоке **Исключения из проверки** нажмите на кнопку **По имени или IP-адресу**.

5. Для экспорта списка исключений выполните следующие действия:

   a. Выберите исключения, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

      Если вы не выбрали ни одного исключения, Kaspersky Endpoint Security экспортирует все исключения.

   b. Нажмите на кнопку → **Экспортировать**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список исключений, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список исключений в XML-файл.

6. Для импорта списка исключений выполните следующие действия:

   a. Нажмите на кнопку → **Импортировать**.

   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

   c. Откройте файл.

      Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

7. Сохраните внесенные изменения.

Как экспортировать / импортировать список исключений в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз** → **Защита на основе анализа поведения** → **Защита от шифрования**.

5. Перейдите по ссылке **Исключения по имени или IP-адресу**.

6. Для экспорта списка исключений выполните следующие действия:

   a. Выберите исключения, которые вы хотите экспортировать.

   b. Нажмите на кнопку → **Экспортировать**.

      Kaspersky Endpoint Security экспортирует список исключений в JSON-файл в папку для загрузки по умолчанию.

7. Для импорта списка исключений выполните следующие действия:

   a. Нажмите на кнопку → **Импортировать**.

      В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список исключений.

b. Откройте файл.

Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.

8. Сохраните внесенные изменения.

Откат вредоносных действий

Компонент Откат вредоносных действий позволяет Kaspersky Endpoint Security отменять действия, произведенные вредоносными приложениями в операционной системе.

Во время отката действий вредоносного приложения в операционной системе Kaspersky Endpoint Security обрабатывает следующие типы активности вредоносного приложения:

- **Файловая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет исполняемые файлы, созданные вредоносным приложением (на всех носителях, кроме сетевых дисков);
  - удаляет исполняемые файлы, созданные приложениями, в которые внедрилось вредоносное приложение;
  - восстанавливает измененные или удаленные вредоносным приложением файлы.

  Функциональность восстановления файлов имеет ряд ограничений.

- **Реестровая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет разделы и ключи реестра, созданные вредоносным приложением;
  - не восстанавливает измененные или удаленные вредоносным приложением разделы и ключи реестра.

- **Системная активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - завершает процессы, которые запускало вредоносное приложение;
  - завершает процессы, в которые внедрялось вредоносное приложение;
  - не возобновляет процессы, которые остановило вредоносное приложение.

- **Сетевая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - запрещает сетевую активность вредоносного приложения;
  - запрещает сетевую активность тех процессов, в которые внедрялось вредоносное приложение.

Откат действий вредоносного приложения может быть запущен компонентом Защита от файловых угроз, Анализ поведения или при поиске вредоносного ПО.

Откат действий вредоносного приложения затрагивает строго ограниченный набор данных. Откат не оказывает негативного влияния на работу операционной системы и целостность информации на вашем компьютере.

Как включить или выключить компонент Откат вредоносных действий в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Продвинутая защита → Откат вредоносных действий**.
4. Используйте флажок **Откат вредоносных действий**, чтобы включить или выключить компонент.
5. Сохраните внесенные изменения.

Как включить или выключить компонент Откат вредоносных действий в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз → Защита на основе анализа поведения → Откат вредоносных действий**.
5. Используйте переключатель **Откат вредоносных действий ВКЛЮЧЕН**, чтобы включить или выключить компонент.
6. Сохраните внесенные изменения.

Как включить или выключить компонент Откат вредоносных действий в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Откат вредоносных действий**.
3. Используйте переключатель **Откат вредоносных действий**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Откат вредоносных действий включен, Kaspersky Endpoint Security будет откатывать действия, которые вредоносные приложения совершили в операционной системе.

Kaspersky Security Network



Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть Kaspersky Security Network.

Функциональность KSN может быть недоступна в приложении на территории США.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, приложение Kaspersky Endpoint Security получает от служб KSN сведения о репутации проверяемых веб-адресов, а также сведения о категории и репутации проверяемых файлов. Подробнее о настройке доступа к KSN см. в справке Kaspersky Security Center.

Использование Kaspersky Security Network является добровольным. Приложение предлагает использовать KSN во время первоначальной настройки приложения. Начать или прекратить использование KSN можно в любой момент.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского". Файл ksn_<ID языка>.txt с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения.

Инфраструктура репутационных баз "Лаборатории Касперского"

Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения для работы с репутационными базами "Лаборатории Касперского":

- *Kaspersky Security Network (KSN)* – это решение, которое используют большинство приложений "Лаборатории Касперского". Участники KSN получают информацию от "Лаборатории Касперского", а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.

- *Kaspersky Private Security Network (KPSN)* – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров. KPSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

  - отсутствие подключения локальных рабочих мест к сети Интернет;

  - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

Включение и выключение использования Kaspersky Security Network

По умолчанию Kaspersky Endpoint Security использует расширенный режим KSN. *Расширенный режим KSN* – режим работы приложения, при котором Kaspersky Endpoint Security передает в "Лабораторию Касперского" дополнительные данные.

Как включить или выключить использование KSN в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита** → **Kaspersky Security Network**.

4. Используйте переключатель **Kaspersky Security Network**, чтобы включить или выключить компонент.

   Если вы включили использование KSN, Kaspersky Endpoint Security покажет Положение о Kaspersky Security Network. Если вы согласны, примите условия использования KSN.

5. Если требуется, выключите флажок **Включить расширенный режим KSN**. По умолчанию расширенный режим KSN включен.

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить использование KSN в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки → Kaspersky Security Network**.
5. Используйте переключатель **Использование Kaspersky Security Network (KSN) ВКЛЮЧЕНО**, чтобы включить или выключить компонент.

   Если вы включили использование KSN, Kaspersky Endpoint Security покажет Положение о Kaspersky Security Network. Если вы согласны, примите условия использования KSN.
6. Если требуется, выключите переключатель **Использовать расширенный режим KSN**. По умолчанию расширенный режим KSN включен.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить использование KSN в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Kaspersky Security Network**.
3. Используйте переключатель **Kaspersky Security Network**, чтобы включить или выключить компонент.

   Если вы включили использование KSN, Kaspersky Endpoint Security покажет Положение о Kaspersky Security Network. Если вы согласны, примите условия использования KSN.
4. Если требуется, выключите переключатель **Включить расширенный режим KSN**. По умолчанию расширенный режим KSN включен.
5. Сохраните внесенные изменения.

В результате, если использование KSN включено, Kaspersky Endpoint Security использует информацию о репутации файлов, веб-ресурсов и приложений, полученную из Kaspersky Security Network.

Ограничения работы с Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров. Kaspersky Private Security Network позволяет использовать собственную базу данных репутаций объектов (файлов или веб-адресов) с помощью локальной репутационной базы. Репутация объекта, добавленного в локальную репутационную базу, имеет приоритет выше, чем в KSN / KPSN. То есть, если Kaspersky Endpoint Security при проверке компьютера запросит репутацию файла в KSN / KPSN, и в локальной репутационной базе файл имеет репутацию *Недоверенные*, а в KSN / KPSN объект имеет репутацию *Доверенные*, то Kaspersky Endpoint Security обнаружит файл как *Недоверенные* и выполнит действие, заданное для обнаруженных угроз.

Однако в некоторых случаях Kaspersky Endpoint Security может не запрашивать репутацию объекта в KSN / KPSN. В результате Kaspersky Endpoint Security не получит данные из локальной репутационной базы KPSN. Kaspersky Endpoint Security может не запрашивать репутацию объекта в KSN / KPSN, например, по следующим причинам:

- Приложения "Лаборатории Касперского" используют офлайн репутационные базы. Офлайн репутационные базы предназначены для оптимизации ресурсов при работе приложений "Лаборатории Касперского" и защите критически важных объектов компьютера. Офлайн репутационные базы формируют специалисты "Лаборатории Касперского" на основании данных Kaspersky Security Network. приложения "Лаборатории Касперского" обновляют офлайн репутационные базы с антивирусными базами приложения. Если информация о проверяемом объекте содержится в офлайн репутационных базах, приложение не запрашивает репутацию этого объекта в KSN / KPSN.

- В параметрах приложения настроены исключения из проверки (доверенная зона). В этом случае приложение не учитывает репутацию объекта в локальной репутационной базе.

- Приложение использует технологии оптимизации проверки, например, технологии iSwift, iChecker или кеширование запросов репутации в KSN / KPSN. В этом случае приложение может не запрашивать репутацию ранее проверенных объектов.

- Для оптимизации нагрузки приложение проверяет файлы определенного формата и размера. Список форматов и ограничения по размеру определяют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами приложения. Также вы можете настроить параметры оптимизации проверки в интерфейсе приложения, например, для компонента Защита от файловых угроз.

- Kaspersky Endpoint Security в режиме Легкого агента взаимодействует с серверами KSN с помощью прокси-сервера KSN. Взаимодействие с KSN напрямую не поддерживается.

Включение и выключение облачного режима для компонентов защиты

Облачный режим – режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию антивирусных баз. Работу приложения с облегченными антивирусными базами обеспечивает Kaspersky Security Network. Облегченная версия антивирусных баз позволяет снизить нагрузку на оперативную память компьютера примерно в два раза. Если вы не участвуете в Kaspersky Security Network или облачный режим выключен, Kaspersky Endpoint Security загружает полную версию антивирусных баз с серверов "Лаборатории Касперского".

При использовании Kaspersky Private Security Network функциональность облачного режима доступна начиная с версии Kaspersky Private Security Network 3.0.

Если приложение работает в режиме Легкого агента, облачный режим недоступен.

Как включить или выключить облачный режим для компонентов защиты в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Продвинутая защита** → **Kaspersky Security Network**.

4. Используйте флажок **Включить облачный режим**, чтобы включить или выключить компонент.
5. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить облачный режим для компонентов защиты в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Kaspersky Security Network**.
5. Используйте переключатель **Использовать облачный режим**, чтобы включить или выключить компонент.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить или выключить облачный режим для компонентов защиты в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .
2. В окне параметров приложения в блоке **Продвинутая защита** и нажмите на плитку **Kaspersky Security Network**.
3. Используйте переключатель **Включить облачный режим**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security загружает облегченную или полную версию антивирусных баз в ходе ближайшего обновления.

Если облегченная версия антивирусных баз недоступна для использования, Kaspersky Endpoint Security автоматически переключается на использование полной версии антивирусных баз.

Настройка KSN Proxy

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN напрямую или при помощи службы KSN Proxy.

Если приложение работает в режиме Легкого агента, взаимодействие с KSN напрямую не поддерживается. Kaspersky Endpoint Security взаимодействует с серверами KSN с помощью прокси-сервера KSN.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.
- Служба KSN Proxy кеширует обработанные данные, снижая тем самым нагрузку на канал связи с внешней сетью и ускоряя получение компьютером пользователя запрошенной информации.

По умолчанию после включения использования KSN и принятия Положения об использовании KSN приложение использует прокси-сервер для связи с Kaspersky Security Network. В качестве прокси-сервера приложение использует Сервер администрирования Kaspersky Security Center и TCP-порт 13111. Таким образом, если KSN Proxy недоступен, вам нужно проверить следующие параметры:

- На Сервере администрирования запущена служба `ksnproxy`.
- На компьютере Сетевой экран не блокирует порт 13111.

Вы можете настроить использование KSN Proxy: включить или выключить KSN Proxy, настроить порт для соединения. Для этого вам нужно открыть свойства Сервера администрирования. Подробнее о настройке KSN Proxy см. в справке Kaspersky Security Center. Также вы можете включить или выключить KSN Proxy для отдельных компьютеров в политике Kaspersky Endpoint Security.

Как включить или выключить KSN Proxy в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Продвинутая защита** → **Kaspersky Security Network**.
4. В блоке **Настройки KSN Proxy** используйте флажок **Использовать Сервер администрирования как прокси-сервер KSN**, чтобы включить или выключить KSN Proxy.
5. Если требуется, установите флажок **Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен**.

   Если флажок установлен, Kaspersky Endpoint Security использует серверы KSN, когда служба KSN Proxy недоступна. Серверы KSN могут быть расположены как в "Лаборатории Касперского", так и на сторонних серверах, в случае использования Kaspersky Private Security Network.
6. Сохраните внесенные изменения.

Как включить или выключить KSN Proxy в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Kaspersky Security Network**.
5. Используйте флажок **Использовать Сервер администрирования как прокси-сервер KSN**, чтобы включить или выключить KSN Proxy.

6. Если требуется, установите флажок **Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен**.

   Если флажок установлен, Kaspersky Endpoint Security использует серверы KSN, когда служба KSN Proxy недоступна. Серверы KSN могут быть расположены как в "Лаборатории Касперского", так и на сторонних серверах, в случае использования Kaspersky Private Security Network. По умолчанию флажок снят.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Адрес KSN Proxy совпадает с адресом Сервера администрирования. При изменении доменного имени Сервера администрирования необходимо обновить адрес KSN Proxy вручную.

Чтобы настроить адрес KSN Proxy, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
3. В контекстном меню папки **Инсталляционные пакеты** выберите пункт **Свойства**.
4. В открывшемся окне укажите новый адрес прокси-сервера KSN на вкладке **Общие**.
5. Сохраните внесенные изменения.

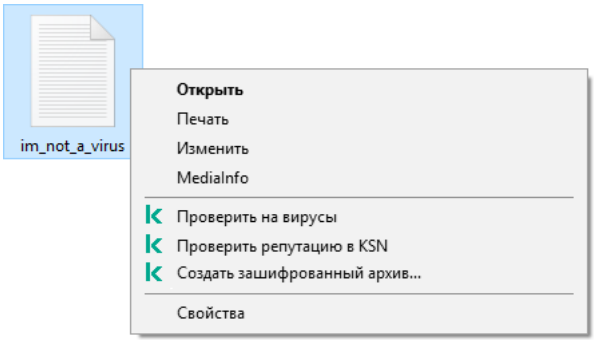
Проверка репутации файла в Kaspersky Security Network

Если вы сомневаетесь в безопасности файла, вы можете проверить его репутацию в Kaspersky Security Network.

Проверка репутации файла доступна, если вы приняли условия Положения о Kaspersky Security Network.

Чтобы проверить репутацию файла в Kaspersky Security Network,

откройте контекстное меню файла и выберите пункт **Проверить репутацию в KSN** (см. рис. ниже).



Контекстное меню файла

Kaspersky Endpoint Security отображает репутацию файла:

Доверенная (Kaspersky Security Network). Приложение считает файл доверенным при выполнении одного или более следующих условий:

- файл обладает цифровой подписью доверенного производителя;
- файл имеет репутацию доверенного в Kaspersky Security Network;
- пользователь поместил файл в группу "Доверенные".

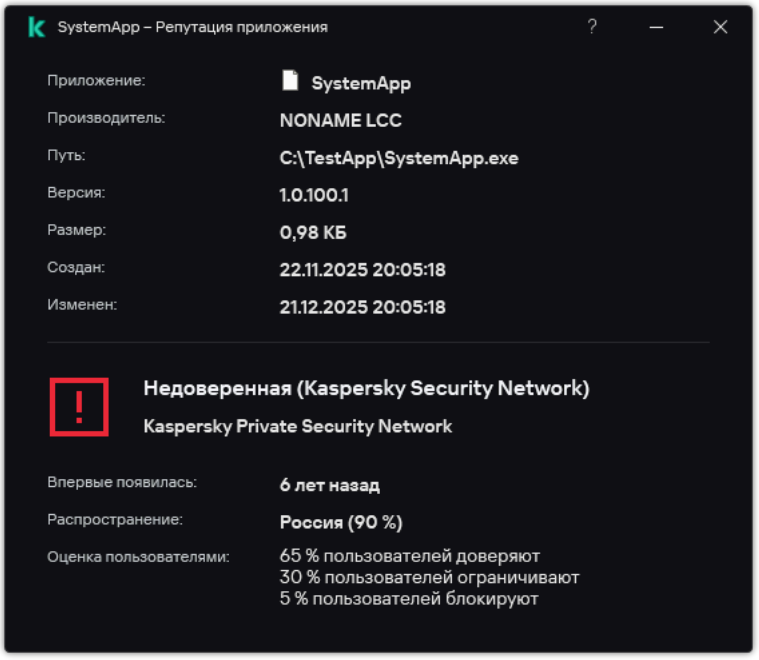
Легальное приложение, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие приложения не имеют вредоносных функций, но могут быть использованы злоумышленниками. Подробную информацию о легальных приложениях, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского". Вы можете добавить эти приложения в список доверенных.

Недоверенная (Kaspersky Security Network). Вирус или другое приложение, представляющее угрозу.

Неизвестен (Kaspersky Security Network). В Kaspersky Security Network отсутствует информация о файле. Вы можете проверить файл с помощью антивирусных баз (пункт контекстного меню **Проверить на вирусы**).

Kaspersky Endpoint Security отображает решение KSN, которое было использовано для определения репутации файла: *Kaspersky Security Network* или *Kaspersky Private Security Network*.

Также Kaspersky Endpoint Security отображает дополнительную информацию о файле (см. рис. ниже).



Репутация файла в Kaspersky Security Network

Проверка защищенных соединений

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов (хранилище сертификатов Windows). Kaspersky Endpoint Security использует этот сертификат для проверки защищенных соединений. Также Kaspersky Endpoint Security включает использование системного хранилища доверенных сертификатов в приложениях Firefox и Thunderbird для проверки трафика этих приложений.

Компоненты Веб-Контроль, Защита от почтовых угроз, Защита от веб-угроз, Анализ поведения, Защита от эксплойтов могут расшифровывать и проверять сетевой трафик, передаваемый по защищенным соединениям с использованием следующих протоколов:

- SSL 3.0;
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Включение проверки защищенных соединений

По умолчанию Kaspersky Endpoint Security проверяет защищенные соединения не всегда, а только по запросу компонентов защиты.

Как включить проверку защищенных соединений в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Общие настройки** → **Настройки сети**.
5. В блоке **Проверка защищенных соединений** выберите режим проверки защищенных соединений:
   - **Проверять защищенные соединения**. Kaspersky Endpoint Security не имеет доступ к содержанию сайтов, адрес которых начинается с `https://`.
   - **Проверять защищенные соединения по запросу компонентов защиты**. Kaspersky Endpoint Security проверяет зашифрованный трафик только по запросу компонентов Защита от веб-угроз, Защита от почтовых угроз и Веб-Контроль.
   - **Всегда проверять защищенные соединения**. Kaspersky Endpoint Security проверяет зашифрованный сетевой трафик, даже если компоненты защиты выключены.

Kaspersky Endpoint Security не проверяет защищенные соединения, установленные доверенными приложениями, для которых выключена проверка трафика. Также Kaspersky Endpoint Security не проверяет защищенные соединения из предустановленного списка доверенных сайтов. Предустановленный список доверенных сайтов составляют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами приложения. Вы можете просмотреть предустановленный список доверенных сайтов только в интерфейсе Kaspersky Endpoint Security. В консоли Kaspersky Security Center просмотреть список невозможно.

6. Если требуется, добавьте исключения из проверки: доверенные адреса и приложения.
7. Настройте параметры проверки защищенных соединений (см. таблицу ниже).
8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить проверку защищенных соединений в Web Console и Cloud Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки сети**.
5. В блоке **Проверка защищенных соединений** включите переключатель **Проверка защищенных соединений ВКЛЮЧЕНА**.

   Если переключатель выключен, Kaspersky Endpoint Security не имеет доступ к содержанию сайтов, адрес которых начинается с `https://`.
6. Перейдите по ссылке **Настройки** и выберите режим проверки защищенных соединений:

   - **Проверять защищенные соединения по запросу компонентов защиты**. Kaspersky Endpoint Security проверяет зашифрованный трафик только по запросу компонентов Защита от веб-угроз, Защита от почтовых угроз и Веб-Контроль.
   - **Всегда проверять защищенные соединения**. Kaspersky Endpoint Security проверяет зашифрованный сетевой трафик, даже если компоненты защиты выключены.

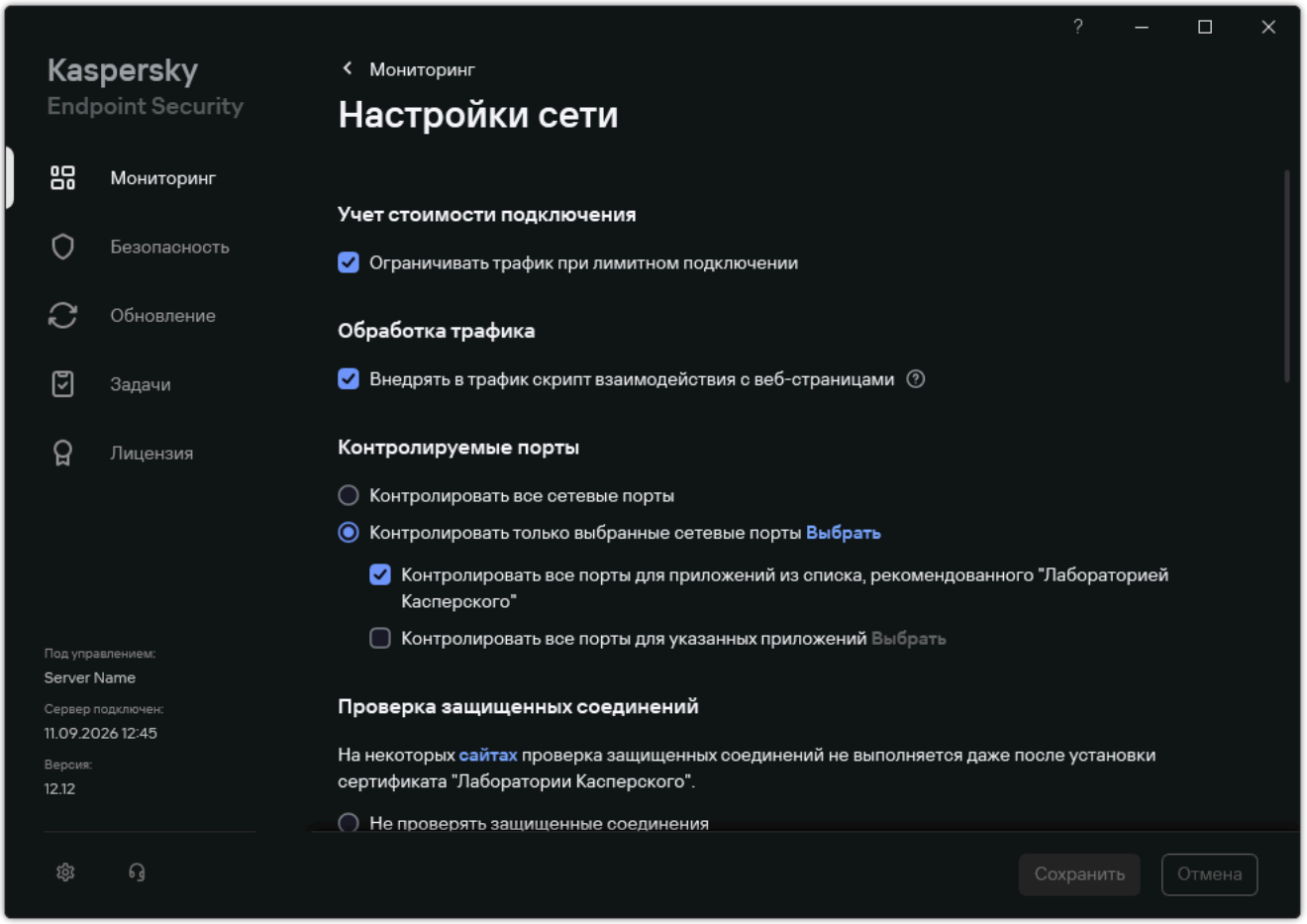
Kaspersky Endpoint Security не проверяет защищенные соединения, установленные доверенными приложениями, для которых выключена проверка трафика. Также Kaspersky Endpoint Security не проверяет защищенные соединения из предустановленного списка доверенных сайтов. Предустановленный список доверенных сайтов составляют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами приложения. Вы можете просмотреть предустановленный список доверенных сайтов только в интерфейсе Kaspersky Endpoint Security. В консоли Kaspersky Security Center просмотреть список невозможно.

7. Если требуется, добавьте исключения из проверки: доверенные адреса и приложения.
8. Настройте параметры проверки защищенных соединений (см. таблицу ниже).
9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить проверку защищенных соединений в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.



Параметры проверки защищенных соединений

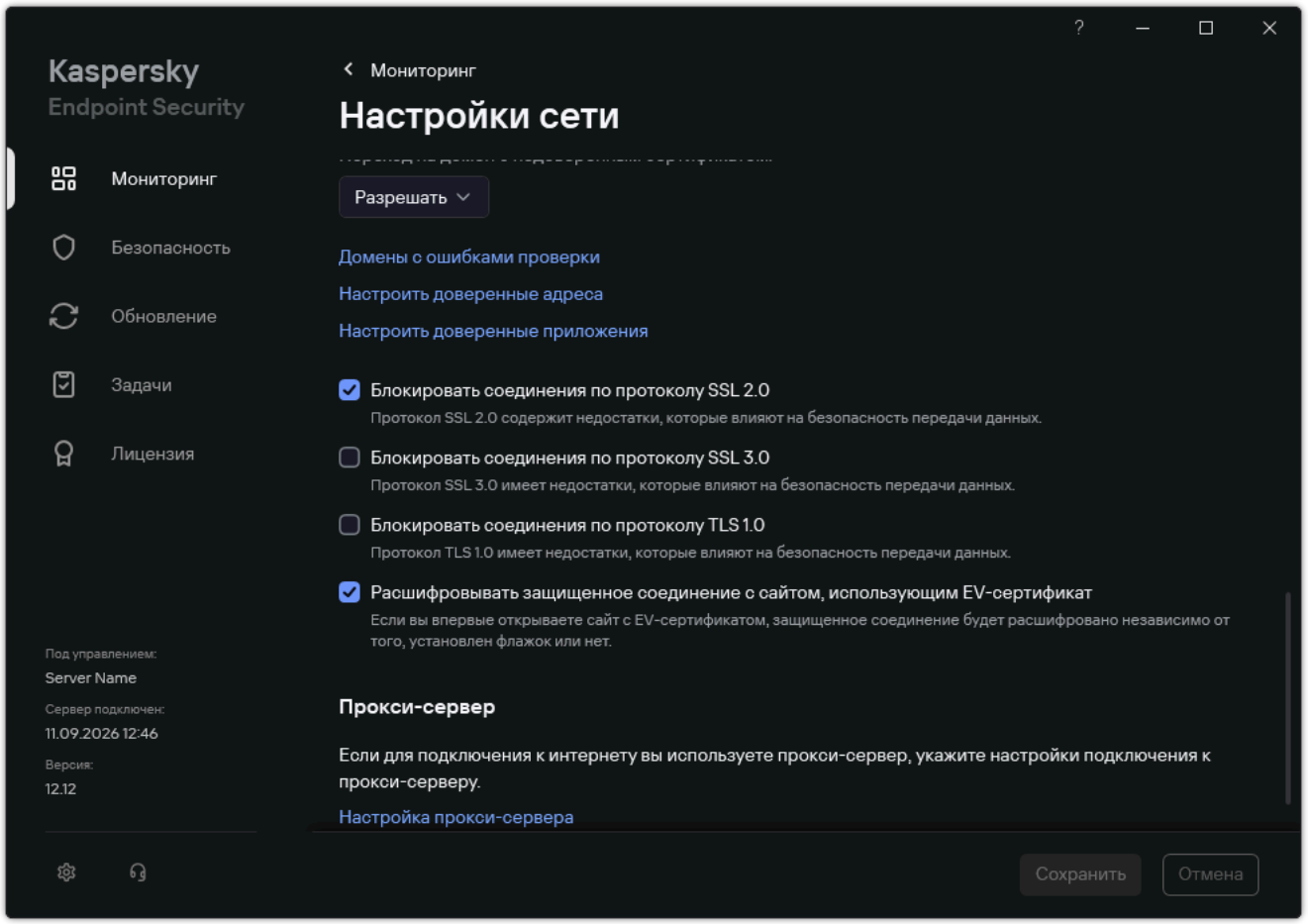
3. В блоке **Проверка защищенных соединений** выберите режим проверки защищенных соединений:

   - **Не проверять защищенные соединения**. Kaspersky Endpoint Security не имеет доступ к содержанию сайтов, адрес которых начинается с `https://`.
   - **Проверять защищенные соединения по запросу компонентов защиты**. Kaspersky Endpoint Security проверяет зашифрованный трафик только по запросу компонентов Защита от веб-угроз, Защита от почтовых угроз и Веб-Контроль.
   - **Всегда проверять защищенные соединения**. Kaspersky Endpoint Security проверяет зашифрованный сетевой трафик, даже если компоненты защиты выключены.

   Kaspersky Endpoint Security не проверяет защищенные соединения, установленные доверенными приложениями, для которых выключена проверка трафика. Также Kaspersky Endpoint Security не проверяет защищенные соединения из предустановленного списка доверенных сайтов. Предустановленный список доверенных сайтов составляют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами приложения. Вы можете просмотреть предустановленный список доверенных сайтов только в интерфейсе Kaspersky Endpoint Security. В консоли Kaspersky Security Center просмотреть список невозможно.

4. Если требуется, добавьте исключения из проверки: доверенные адреса и приложения.

5. Настройте параметры проверки защищенных соединений (см. таблицу ниже).



Дополнительные параметры проверки защищенных соединений

6. Сохраните внесенные изменения.

Параметры проверки защищенных соединений

Параметр	Описание
Доверенные корневые сертификаты	Список доверенных корневых сертификатов. Kaspersky Endpoint Security позволяет устанавливать доверенные корневые сертификаты на компьютеры пользователей, если, например, вам нужно развернуть новый центр сертификации. Приложение позволяет добавить сертификат в специальное хранилище сертификатов Kaspersky Endpoint Security. При этом сертификат будет доверенным только для приложения Kaspersky Endpoint Security. То есть пользователь будет иметь доступ к веб-сайту с новым сертификатом в браузере. Если другое приложение попытается получить доступ к веб-сайту, вы можете получить ошибку соединения из-за проблем с сертификатом. Для добавления сертификата в системное хранилище сертификатов, вы можете использовать групповые политики Active Directory.
Переход на домен с недоверенным сертификатом	• **Разрешать**. При переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security разрешает установку сетевого соединения. При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security отображает HTML-страницу с предупреждением и информацией о причине, по которой этот домен не рекомендован для посещения. По ссылке из HTML-страницы с предупреждением пользователь может получить доступ к запрошенному веб-ресурсу. Если стороннее приложение или служба устанавливает соединение с доменом с недоверенным сертификатом, Kaspersky Endpoint Security создаст собственный сертификат для проверки трафика. Новый сертификат будет иметь статус *Недоверенный*. Это нужно, чтобы предупредить стороннее приложение о недоверенном соединении, так как показать HTML-страницу в этом случае невозможно и соединение может быть установлено в фоновом режиме. • **Блокировать**. При переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security блокирует сетевое соединение. При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security отображает HTML-страницу с информацией о причине, по которой переход на этот домен заблокирован.

Параметр	Описание
Использовать хранилище сертификатов Windows для проверки защищенного трафика в приложениях на базе технологий Mozilla	Приложения Mozilla Firefox и Thunderbird, а также почтовые клиенты МойОфис Почта и Органайзер Р7-Офис по умолчанию используют собственное хранилище сертификатов, а не хранилище сертификатов Windows. Если флажок **Использовать хранилище сертификатов Windows для проверки защищенного трафика в приложениях на базе технологий Mozilla** снят, Kaspersky Endpoint Security не проверяет HTTPS-трафик данных приложений. Если флажок установлен, Kaspersky Endpoint Security настраивает в данных приложениях использование хранилища сертификатов Windows для обеспечения проверки их трафика. Для проверки трафика в приложениях на базе технологий Mozilla должна быть включена проверка защищенных соединений. Вы можете настроить данный параметр только в Консоли администрирования (MMC) или Web Console.
Использовать хранилище сертификатов Windows для проверки защищенного трафика в приложениях Java	Java-приложения по умолчанию используют собственное хранилище сертификатов, а не хранилище сертификатов Windows. Если флажок **Использовать хранилище сертификатов Windows для проверки защищенного трафика в приложениях Java** снят, Kaspersky Endpoint Security не проверяет HTTPS-трафик данных приложений. Если флажок установлен, Kaspersky Endpoint Security настраивает для Java-приложений использование хранилища сертификатов Windows для обеспечения проверки их трафика. Для проверки трафика в Java-приложениях должна быть включена проверка защищенных соединений. Вы можете настроить данный параметр только в Консоли администрирования (MMC) или Web Console.
Переход на домен с ошибкой проверки защищенного соединения	• **Блокировать**. При возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security блокирует это сетевое соединение. • **Разрешать и добавлять домен в исключения**. При возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security добавляет домен, при переходе на который возникла ошибка, в список доменов с ошибками проверки и не контролирует зашифрованный сетевой трафик при переходе на этот домен. Вы можете просмотреть список доменов с ошибками проверки защищенных соединений только в локальном интерфейсе приложения. Чтобы сбросить содержание списка, нужно выбрать элемент **Блокировать**. Также Kaspersky Endpoint Security формирует событие об ошибке проверки защищенного соединения.
Блокировать соединения по протоколу SSL 2.0	Если флажок установлен, то приложение контролирует и блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. При этом приложение не контролирует сетевой трафик по этому протоколу.
Блокировать соединения по протоколу SSL 3.0	Если флажок установлен, то приложение блокирует сетевые соединения, устанавливаемые по протоколу SSL 3.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу SSL 3.0. Приложение контролирует сетевой трафик по этому протоколу. Все компоненты приложения работают без ограничений.
Блокировать соединения по протоколу TLS 1.0	Если флажок установлен, то приложение блокирует сетевые соединения, устанавливаемые по протоколу TLS 1.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу TLS 1.0. Приложение контролирует сетевой трафик по этому протоколу. Все компоненты приложения работают без ограничений.

Параметр	Описание
Расшифровывать защищенное соединение с сайтом, использующим EV-сертификат	EV-сертификаты (англ. Extended Validation Certificate) подтверждают подлинность веб-сайтов и повышают безопасность соединения. Браузеры сообщают о наличии на веб-сайте EV-сертификата с помощью значка замка в адресной строке браузера. Также браузеры могут полностью или частично окрашивать адресную строку в зеленый цвет. Если флажок установлен, приложение расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если флажок снят, приложение не имеет доступа к содержанию HTTPS-трафика. Поэтому приложение контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://bing.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.

Установка доверенных корневых сертификатов

Kaspersky Endpoint Security позволяет устанавливать доверенные корневые сертификаты на компьютеры пользователей, если, например, вам нужно развернуть новый центр сертификации. Приложение позволяет добавить сертификат в специальное хранилище сертификатов Kaspersky Endpoint Security. При этом сертификат будет доверенным только для приложения Kaspersky Endpoint Security. То есть пользователь будет иметь доступ к веб-сайту с новым сертификатом в браузере. Если другое приложение попытается получить доступ к веб-сайту, вы можете получить ошибку соединения из-за проблем с сертификатом. Для добавления сертификата в системное хранилище сертификатов, вы можете использовать групповые политики Active Directory.

Как установить доверенные корневые сертификаты в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Настройки сети**.
4. В блоке **Доверенные корневые сертификаты** нажмите на кнопку **Добавить**.
5. В открывшемся окне выберите доверенный корневой сертификат.

   Kaspersky Endpoint Security поддерживает сертификаты с расширением PEM, DER и CRT.
6. Сохраните внесенные изменения.

Как установить доверенные корневые сертификаты в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки сети**.
5. Перейдите по ссылке **Доверенные корневые сертификаты**.

6. В открывшемся окне нажмите на кнопку **Добавить** и выберите доверенный корневой сертификат.

   Kaspersky Endpoint Security поддерживает сертификаты с расширением PEM, DER и CRT.

7. Сохраните внесенные изменения.

Как установить доверенные сертификаты в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.
3. В блоке **Проверка защищенных соединений** нажмите на кнопку **Показать сертификаты**.
4. В открывшемся окне нажмите на кнопку **Добавить** и выберите доверенный корневой сертификат.

   Kaspersky Endpoint Security поддерживает сертификаты с расширением PEM, DER и CRT.

5. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security при проверке трафика кроме системного хранилища сертификатов будет использовать собственное хранилище сертификатов.

Проверка защищенных соединений с недоверенным сертификатом

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов (хранилище сертификатов Windows). Kaspersky Endpoint Security использует этот сертификат для проверки защищенных соединений. При переходе на домен с недоверенным сертификатом вы можете разрешить или заблокировать пользователю доступ к этому домену (см. инструкцию ниже).

Если вы разрешили пользователю переходить на домены с недоверенным сертификатом, Kaspersky Endpoint Security выполняет следующие действия:

- При переходе на домен с недоверенным сертификатом в *браузере*, Kaspersky Endpoint Security использует сертификат "Лаборатории Касперского" для проверки трафика. Kaspersky Endpoint Security отображает HTML-страницу с предупреждением и информацией о причине, по которой этот домен не рекомендован для посещения (см. рис. ниже). По ссылке из HTML-страницы с предупреждением пользователь может получить доступ к запрошенному веб-ресурсу. После перехода по этой ссылке Kaspersky Endpoint Security в течение часа не будет отображать предупреждения о недоверенном сертификате при переходе на другие веб-ресурсы в том же домене. Также Kaspersky Endpoint Security формирует событие об использовании защищенного соединения с недоверенным сертификатом.

  В некоторых случаях у Kaspersky Endpoint Security нет технической возможности показать HTML-страницу с предупреждением в браузере (см. рис. ниже). Например, если веб-ресурс использует устаревшую версию сетевого протокола и нестандартный порт. В этих случаях Kaspersky Endpoint Security заблокирует доступ к этому домену, а браузер покажет стандартное окно `ERR_CONNECTION_RESET`. Для доступа к веб-ресурсу вы можете добавить домен в исключения или использовать доверенный сертификат.

- Если *стороннее приложение или служба* устанавливает соединение с доменом с недоверенным сертификатом, Kaspersky Endpoint Security создаст собственный сертификат для проверки трафика. Новый сертификат будет иметь статус *Недоверенный*. Это нужно, чтобы предупредить стороннее приложение о недоверенном соединении, так как показать HTML-страницу в этом случае невозможно и соединение может быть установлено в фоновом режиме. Поэтому, если стороннее приложение имеет встроенные инструменты проверки сертификатов, соединение может быть разорвано. В этом случае, вам нужно обратиться к владельцу домена и настроить доверенное соединение. Если настроить доверенное соединение невозможно, вы можете добавить это стороннее приложение в список доверенных приложений. Также Kaspersky Endpoint Security формирует событие об использовании защищенного соединения с недоверенным сертификатом.

Как настроить проверку защищенных соединений с недоверенным сертификатом в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Настройки сети**.
4. В блоке **Проверка защищенных соединений** нажмите на кнопку **Дополнительные настройки**.
5. В открывшемся окне выберите режим работы приложения при переходе на домен с недоверенным сертификатом: **Разрешать** или **Блокировать**.
6. Сохраните внесенные изменения.

Как настроить проверку защищенных соединений с недоверенным сертификатом в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки** → **Настройки сети**.

5. В блоке **Проверка защищенных соединений** перейдите по ссылке **Настройки**.

6. В открывшемся окне выберите режим работы приложения при переходе на домен с недоверенным сертификатом: **Разрешать соединение** или **Блокировать соединение**.

7. Сохраните внесенные изменения.

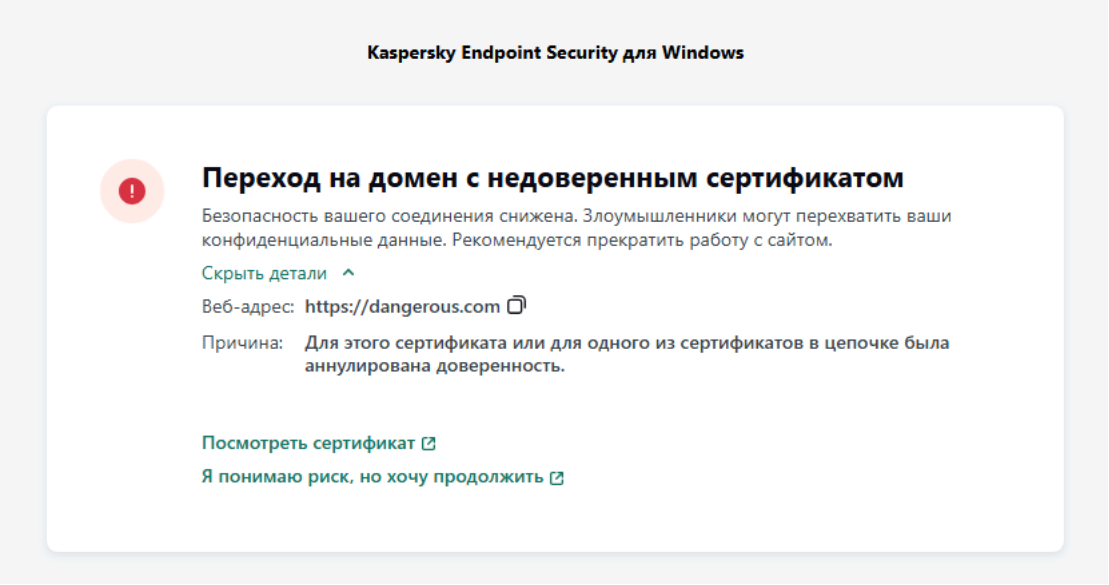
Как настроить проверку защищенных соединений с недоверенным сертификатом в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

3. В блоке **Проверка защищенных соединений** выберите режим работы приложения при переходе на домен с недоверенным сертификатом: **Разрешать** или **Блокировать**.

4. Сохраните внесенные изменения.



Предупреждение о переходе на домен с недоверенным сертификатом

Исключение защищенных соединений из проверки

Большинство веб-ресурсов используют защищенное соединение. Специалисты "Лаборатории Касперского" рекомендуют включить проверку защищенных соединений. Если проверка защищенных соединений мешает работе, вы можете добавить веб-сайт в исключения, – *доверенные адреса*. В этом случае Kaspersky Endpoint Security не будет проверять HTTPS-трафик доверенных веб-адресов при работе компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль.

Если доверенное приложение использует защищенное соединение, вы можете выключить проверку защищенных соединений для этого приложения. Например, вы можете выключить проверку защищенных соединений для приложений облачных хранилищ, так как эти приложения используют двухфакторную аутентификацию с собственным сертификатом.

Как исключить веб-адрес из проверки защищенных соединений в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Общие настройки** → **Настройки сети**.
5. В блоке **Проверка защищенных соединений** нажмите на кнопку **Настроить доверенные адреса**.
6. Нажмите на кнопку **Добавить**.
7. Введите имя домена или IP-адрес, если вы хотите, чтобы приложение Kaspersky Endpoint Security не проверяло защищенные соединения, устанавливаемые при переходе на эту веб-страницу.

   Kaspersky Endpoint Security поддерживает символ `*` для ввода маски в имени домена.

   > Kaspersky Endpoint Security не поддерживает символ `*` для IP-адресов. Вы можете выбрать диапазон IP-адресов с помощью маски подсети (например, 198.51.100.0/24).

   Примеры:

   - `domain.com` – запись включает в себя следующие адреса: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Запись исключает поддомены (например, `subdomain.domain.com`).
   - `subdomain.domain.com` – запись включает в себя следующие адреса: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Запись исключает домен `domain.com`.
   - `*.domain.com` – запись включает в себя следующие адреса: `https://movies.domain.com`, `https://images.domain.com/page123`. Запись исключает домен `domain.com`.
8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как исключить веб-адрес из проверки защищенных соединений в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки сети**.
5. В блоке **Проверка защищенных соединений** нажмите на кнопку **Доверенные домены**.
6. Нажмите на кнопку **Добавить**.
7. Введите имя домена или IP-адрес, если вы хотите, чтобы приложение Kaspersky Endpoint Security не проверяло защищенные соединения, устанавливаемые при переходе на эту веб-страницу.

Kaspersky Endpoint Security поддерживает символ `*` для ввода маски в имени домена.

> Kaspersky Endpoint Security не поддерживает символ `*` для IP-адресов. Вы можете выбрать диапазон IP-адресов с помощью маски подсети (например, 198.51.100.0/24).

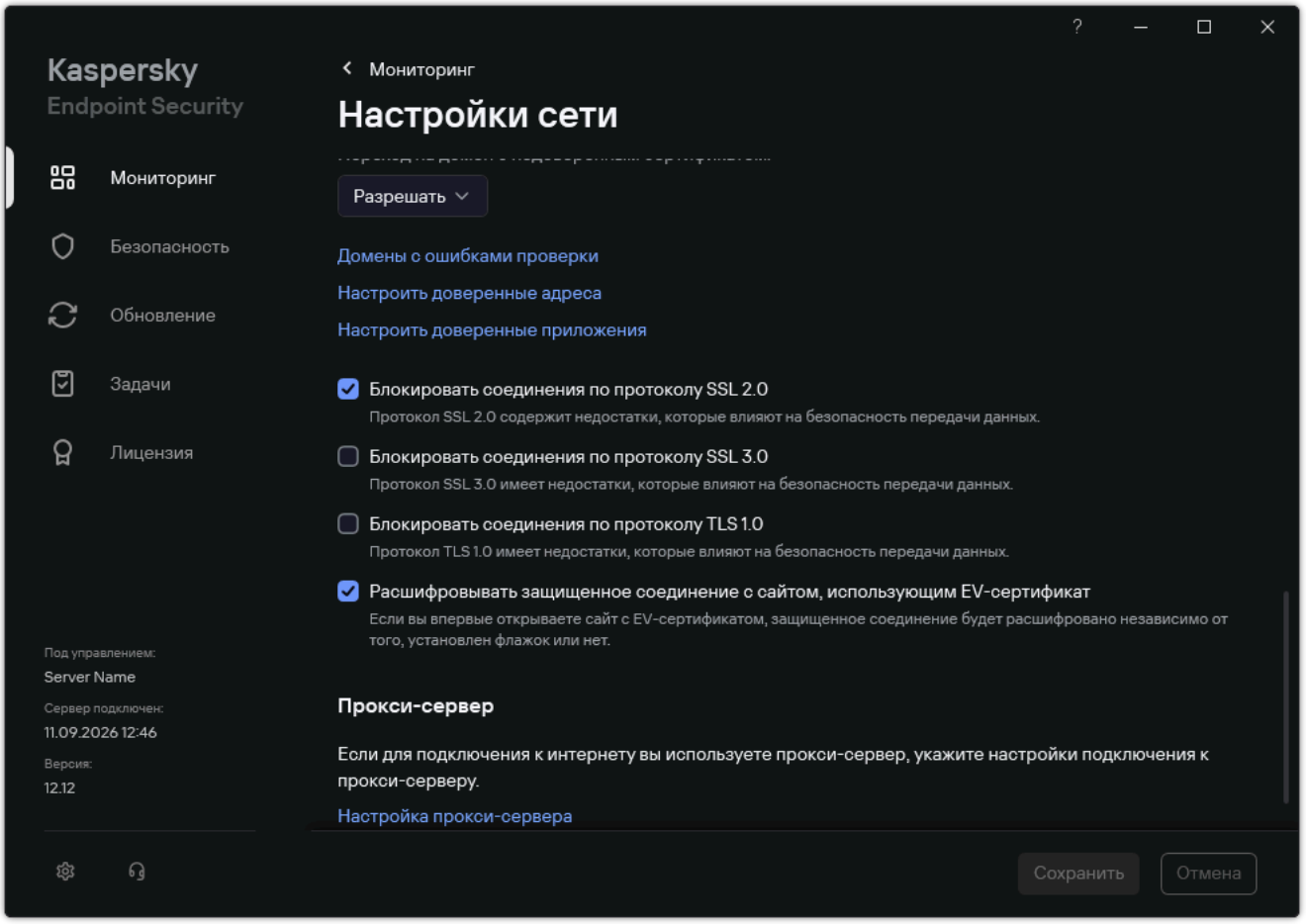
Примеры:

- `domain.com` – запись включает в себя следующие адреса: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Запись исключает поддомены (например, `subdomain.domain.com`).
- `subdomain.domain.com` – запись включает в себя следующие адреса: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Запись исключает домен `domain.com`.
- `*.domain.com` – запись включает в себя следующие адреса: `https://movies.domain.com`, `https://images.domain.com/page123`. Запись исключает домен `domain.com`.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как исключить веб-адрес из проверки защищенных соединений в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.



Параметры сети приложения

3. В блоке **Проверка защищенных соединений** нажмите на кнопку **Настроить доверенные адреса**.

4. Нажмите на кнопку **Добавить**.

5. Введите имя домена или IP-адрес, если вы хотите, чтобы приложение Kaspersky Endpoint Security не проверяло защищенные соединения, устанавливаемые при переходе на эту веб-страницу.

   Kaspersky Endpoint Security поддерживает символ `*` для ввода маски в имени домена.

   > Kaspersky Endpoint Security не поддерживает символ `*` для IP-адресов. Вы можете выбрать диапазон IP-адресов с помощью маски подсети (например, 198.51.100.0/24).

   Примеры:

   - `domain.com` – запись включает в себя следующие адреса: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Запись исключает поддомены (например, `subdomain.domain.com`).
   - `subdomain.domain.com` – запись включает в себя следующие адреса: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Запись исключает домен `domain.com`.
   - `*.domain.com` – запись включает в себя следующие адреса: `https://movies.domain.com`, `https://images.domain.com/page123`. Запись исключает домен `domain.com`.

6. Сохраните внесенные изменения.

По умолчанию Kaspersky Endpoint Security не проверяет защищенные соединения при возникновении ошибок и добавляет веб-сайт в специальный список – *домены с ошибками проверки*. Kaspersky Endpoint Security составляет список для каждого пользователя отдельно и не передает данные в Kaspersky Security Center. Вы можете включить блокирование соединения при возникновении ошибки. Вы можете просмотреть список доменов с ошибками проверки защищенных соединений только в локальном интерфейсе приложения.

Чтобы просмотреть список доменов с ошибками проверки, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

3. В блоке **Проверка защищенных соединений** нажмите на кнопку **Домены с ошибками проверки**.

   Откроется список доменов с ошибками проверки. Чтобы сбросить список вам нужно включить блокирование соединения при возникновении ошибки в политике, применить политику, вернуть параметр в исходное состояние и снова применить политику.

Специалисты "Лаборатории Касперского" составляют список доверенных веб-сайтов, которые Kaspersky Endpoint Security не проверяет независимо от параметров приложения, – *глобальные исключения*.

Чтобы просмотреть глобальные исключения из проверки защищенного трафика, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.
3. В блоке **Проверка защищенных соединений** нажмите на ссылку со списком доверенных веб-сайтов.

   Откроется список веб-сайтов, составленный специалистами "Лаборатории Касперского". Kaspersky Endpoint Security не проверяет защищенные соединения для сайтов из списка. Список может быть обновлен при обновлении баз и модулей Kaspersky Endpoint Security.

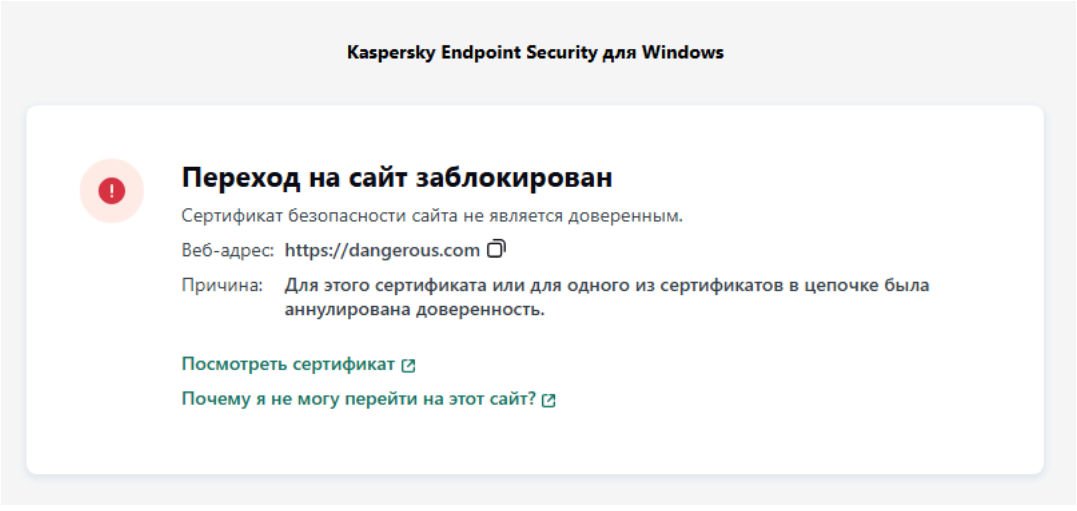
Блокировка доступа к доменам с недоверенными сертификатами

В некоторых случаях при блокировке доступа к домену с недоверенным сертификатом Kaspersky Endpoint Security отображает в браузере HTML-страницу с предупреждением, на которой отсутствует ссылка для перехода к запрошенному веб-ресурсу.

Это может произойти по следующим причинам:

- Администратор запретил переход на домены с недоверенными сертификатами.
- Домен имеет недоверенный или недействительный сертификат, и на веб-сервере используется механизм HTTP Strict Transport Security (HSTS). *HSTS* – это механизм обеспечения безопасности, который позволяет принудительно использовать защищенный протокол HTTPS при взаимодействии клиента с веб-сервером. В этом случае вы не сможете получить доступ к домену, даже если вы добавили его в список доверенных адресов. Механизм HSTS описан в спецификации RFC 6797.

  В некоторых случаях веб-сайт можно открыть напрямую через браузер, без использования приложения Kaspersky Endpoint Security. Браузеры не всегда обнаруживают отозванные сертификаты, в то время как приложение Kaspersky Endpoint Security выполняет онлайн-проверку отзыва сертификата при установлении соединения. Благодаря этому приложение может обнаружить проблему с сертификатом раньше, чем браузер, и отобразить соответствующее сообщение об ошибке.



Предупреждение о переходе на домен с недоверенным сертификатом

Удаление данных

Kaspersky Endpoint Security позволяет дистанционно удалять данные на компьютерах пользователей с помощью задачи.

Kaspersky Endpoint Security удаляет данные следующим образом:

- в тихом режиме;
- на жестких и съемных дисках;
- для всех учетных записей на компьютере.

Kaspersky Endpoint Security выполняет задачу *Удаление данных* при любом типе лицензирования, даже после истечения срока действия лицензии.

Режимы удаления данных

Задача позволяет удалять данные в следующих режимах:

- Немедленное удаление данных.

  В этом режиме вы можете, например, удалить устаревшие данные, чтобы освободить дисковое пространство.

- Отложенное удаление данных.

  Этот режим предназначен, например, для защиты данных на ноутбуке в случае его потери или кражи. Вы можете настроить автоматическое удаление данных, если ноутбук покинул пределы сети организации и давно не синхронизировался с Kaspersky Security Center.

Настроить расписание удаления данных в свойствах задачи невозможно. Вы можете только немедленно удалить данные после запуска задачи вручную или настроить отложенное удаление данных при отсутствии связи с Kaspersky Security Center.

Ограничения

Удаление данных имеет следующие ограничения:

- Управление задачей *Удаление данных* доступно только администратору Kaspersky Security Center. Настроить или запустить задачу в локальном интерфейсе Kaspersky Endpoint Security невозможно.
- Для файловой системы NTFS Kaspersky Endpoint Security удаляет имена только основных потоков данных. Удалить имена альтернативных потоков данных невозможно.
- При удалении файла символической ссылки Kaspersky Endpoint Security также удаляет файлы, пути к которым указаны в символической ссылке.

Создание задачи удаления данных

Чтобы удалить данные на компьютерах пользователей, выполните следующие действия:

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Удаление данных**.

   c. В поле **Название задачи** введите короткое описание, например, *Удаление данных (Анти-Вор)*.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

   Если в группу администрирования области действия задачи добавлены новые компьютеры, то задача немедленного удаления данных запускается на новых компьютерах только при условии, что между завершением выполнения задачи и добавлением новых компьютеров прошло менее 5 минут.

5. Завершите работу мастера.

   В списке задач отобразится новая задача.

6. Нажмите на задачу Kaspersky Endpoint Security **Удаление данных**.

   Откроется окно свойств задачи.

7. Выберите вкладку **Параметры приложения**.

8. Выберите метод удаления данных:

   - **Удалять средствами операционной системы**. Kaspersky Endpoint Security удаляет файлы средствами операционной системы без помещения файлов в корзину.

   - **Удалять без возможности восстановления**. Kaspersky Endpoint Security перезаписывает файлы случайными данными. Восстановить данные после удаления практически невозможно.

9. Если вы хотите использовать отложенное удаление данных, установите флажок **Автоматически удалять данные при отсутствии связи с Kaspersky Security Center более N дней**. Задайте количество дней.

   Задача в режиме отложенного удаления данных будет выполняться при каждом превышении срока отсутствия связи с Kaspersky Security Center.

   При настройке отложенного удаления данных учитывайте, что сотрудники могут иметь разный график работы. Также учитывайте график работы автономных пользователей. Подробнее о работе с автономными компьютерами и автономными пользователями см. в справке Kaspersky Security Center.

   Если компьютер выключен и срок отсутствия связи превышен, после включения компьютера Kaspersky Endpoint Security не удаляет данные немедленно. Приложение ожидает синхронизации с Kaspersky Security Center в течение одного часа. Это нужно, чтобы предотвратить несанкционированное удаление данных на компьютерах пользователей, которые, например, выключили компьютер перед уходом в отпуск.

   Если флажок снят, задача будет выполнена сразу после синхронизации с Kaspersky Security Center.

10. Создайте список объектов для удаления:

    - **Папки**. Kaspersky Endpoint Security удалит все файлы в папке, а также вложенные папки. Kaspersky Endpoint Security не поддерживает маски и переменные окружения при вводе пути к папке.

    - **Файлы по расширению**. Kaspersky Endpoint Security выполнит поиск файлов с указанными расширениями на всех дисках компьютера, в том числе съемных дисках. Для указания нескольких расширений используйте символы `;` или `,`.

    - **Стандартные области**. Kaspersky Endpoint Security удалит файлы из следующих областей:

      - **Документы**. Файлы в стандартной папке операционной системы *Документы*, а также вложенные папки.

      - **Файлы Cookies**. Файлы, в которых браузер сохраняет данные с посещенных пользователем веб-сайтов (например, данные для авторизации пользователя).

      - **Рабочий стол**. Файлы в стандартной папке операционной системы *Рабочий стол*, а также вложенные папки.

      - **Временные файлы Internet Explorer**. Временные файлы, связанные с работой браузера Internet Explorer: копии веб-страниц, изображений и медиафайлов.

      - **Временные файлы**. Временные файлы, связанные с работой установленных на компьютере приложений. Например, приложения Microsoft Office создают временные файлы с резервными копиями документов.

- **Файлы Outlook**. Файлы, связанные с работой почтового клиента Outlook: файлы данных (PST), автономные файлы данных (OST), файлы автономной адресной книги (OAB) и файлы персональной адресной книги (PAB).

- **Профиль пользователя**. Набор файлов и папок, в которых хранятся параметры операционной системы для учетной записи локального пользователя.

Вы можете создать список объектов для удаления на каждой из вкладок. Kaspersky Endpoint Security создаст общий консолидированный список и удалит файлы из этого списка при выполнении задачи.

Удалить файлы, необходимые для работы Kaspersky Endpoint Security, невозможно.

11. Сохраните внесенные изменения.

12. Установите флажок напротив задачи.

13. Нажмите на кнопку **Запустить**.

В результате на компьютерах пользователей будут удалены данные в соответствии с выбранным режимом: немедленно или при отсутствии связи. Если Kaspersky Endpoint Security не может удалить файл, например, пользователь использует файл в настоящий момент, приложение не пытается удалить его снова. Для завершения удаления данных повторите запуск задачи.

Контроль компьютера

Веб-Контроль

Веб-Контроль управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени. При попытке пользователя открыть веб-сайт, доступ к которому ограничен Веб-Контролем, Kaspersky Endpoint Security заблокирует доступ или покажет предупреждение (см. рис. ниже).

Для работы Веб-Контроля необходимо выполнить первоначальную настройку приложения:

- Для контроля HTTPS-трафика включите проверку защищенных соединений (по умолчанию проверка включена).
- Выберите порты, которые Kaspersky Endpoint Security будет контролировать (по умолчанию приложение контролирует все порты).
- Выберите приложения, трафик которых будет контролировать Kaspersky Endpoint Security. Основные браузеры уже добавлены в список, рекомендованный "Лабораторией Касперского". Если вашего браузера нет в списке, добавьте приложение вручную.
- Рекомендуется внедрить в трафик скрипт для взаимодействия с веб-страницами (по умолчанию внедрение скрипта выключено). Скрипт позволяет регистрировать события работы Веб-Контроля для журнала событий приложения, журнала событий ОС, отчетов.

Способы управления доступом к веб-сайтам

Веб-Контроль позволяет настраивать доступ к веб-сайтам следующими способами:

- **Категория веб-сайта**. Категоризацию веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз приложения). Вы можете ограничить доступ пользователей, например, к категории *Социальные сети* или другим категориям.
- **Тип данных**. Вы можете ограничить доступ пользователей к данным на веб-сайте и, например, скрыть графические изображения. Kaspersky Endpoint Security определяет тип данных по формату файла, а не по расширению.

  Kaspersky Endpoint Security не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, Kaspersky Endpoint Security определит тип данных *Архивы*, а не *Графические файлы*.

- **Отдельный адрес**. Вы можете ввести веб-адрес или использовать маски.

Вы можете использовать одновременно несколько способов регулирования доступа к веб-сайтам. Например, вы можете ограничить доступ к типу данных *Файлы офисных приложений* только для категории веб-сайтов *Веб-почта*.

Правила доступа к веб-сайтам

Веб-Контроль управляет доступом пользователей к веб-сайтам с помощью *правил доступа*. Вы можете настроить следующие дополнительные параметры правила доступа к веб-сайтам:

- Пользователи, на которых распространяется правило.

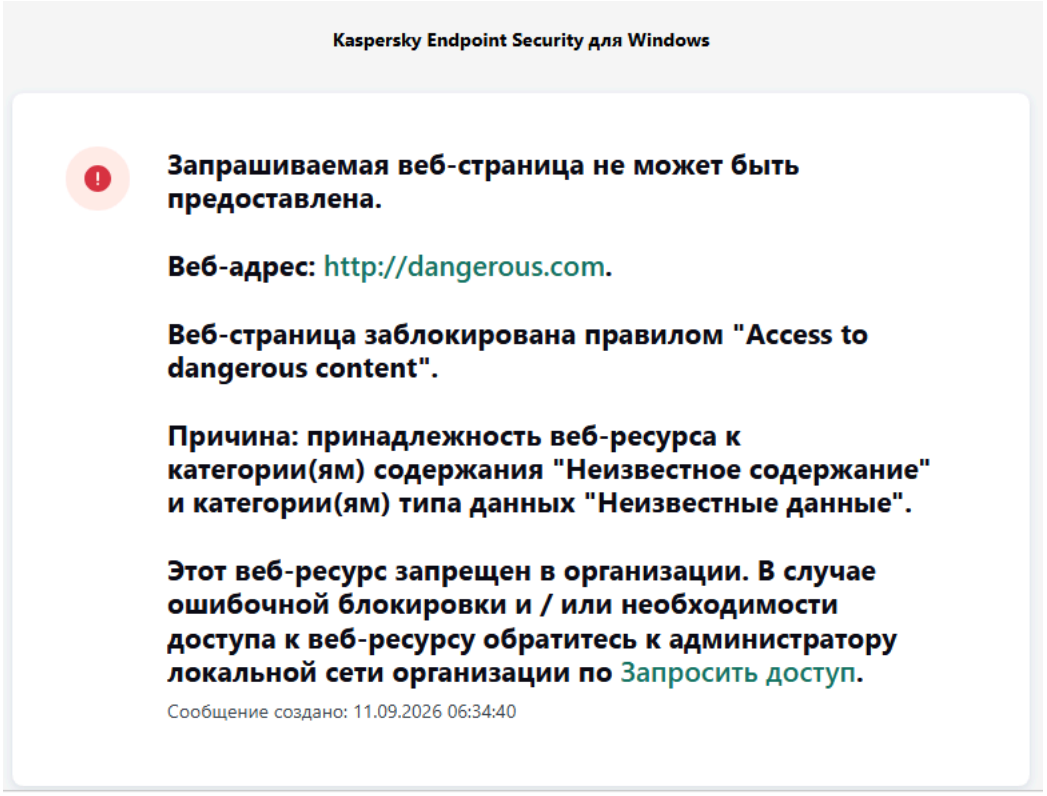
  Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

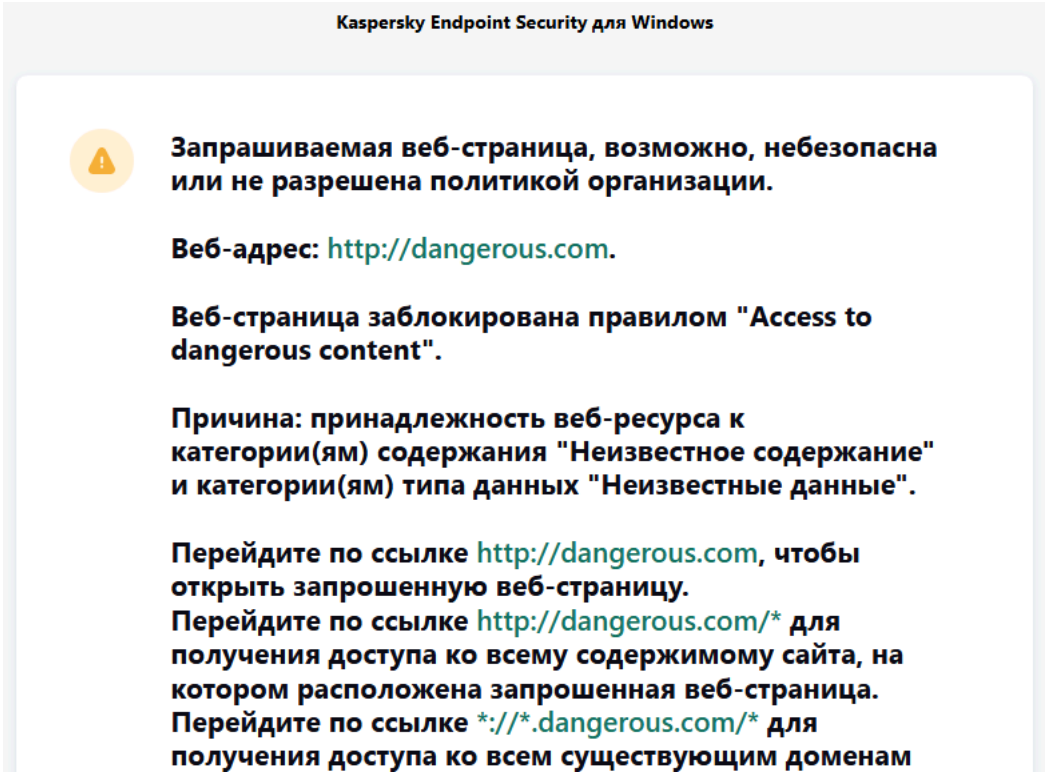
- Расписание работы правила.

  Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Приоритеты правил доступа

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом. Например, Kaspersky Endpoint Security может определить корпоративный портал как социальную сеть. Чтобы ограничить доступ к социальным сетям и предоставить доступ к корпоративному веб-порталу, создайте два правила: запрещающее правило для категории веб-сайтов *Социальные сети* и разрешающее правило для корпоративного веб-портала. Правило доступа к корпоративному веб-порталу должно иметь приоритет выше, чем правило доступа к социальным сетям.





Сообщения Веб-Контроля

Добавление правила доступа к веб-ресурсам

Правило доступа к веб-ресурсам – набор фильтров и действий, которое Kaspersky Endpoint Security выполняет при посещении пользователями веб-ресурсов. Правила доступа могут включать в себя расписание работы правила.

Не рекомендуется создавать более 1000 правил доступа к веб-ресурсам, поскольку это может привести к нестабильности системы.

Правило доступа к веб-ресурсам представляет собой набор фильтров и действие, которое Kaspersky Endpoint Security выполняет при посещении пользователями описанных в правиле веб-ресурсов в указанное в расписании работы правила время. Фильтры позволяют точно задать круг веб-ресурсов, доступ к которым контролирует компонент Веб-Контроль.

Доступны следующие фильтры:

- **Фильтр по содержанию**. Веб-Контроль разделяет веб-ресурсы по категориям содержания и категориям типа данных. Вы можете контролировать доступ пользователей к размещенным на веб-ресурсах данным, относящихся к определенными этими категориями типам данных. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории содержания и / или категории типа данных, Kaspersky Endpoint Security выполняет действие, указанное в правиле.

- **Фильтр по адресам веб-ресурсов**. Вы можете контролировать доступ пользователей ко всем адресам веб-ресурсов или к отдельным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

  Если задан и фильтр по содержанию, и фильтр по адресам веб-ресурсов, и заданные адреса веб-ресурсов и / или группы адресов веб-ресурсов принадлежат к выбранным категориям содержания или категориям типа данных, Kaspersky Endpoint Security контролирует доступ не ко всем веб-ресурсам выбранных категорий содержания и / или категорий типа данных, а только к заданным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

- **Фильтр по именам пользователей и групп пользователей**. Вы можете задавать пользователей и / или группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом.

- **Расписание работы правила**. Вы можете задавать расписание работы правила. Расписание работы правила определяет время, когда Kaspersky Endpoint Security контролирует доступ к веб-ресурсам, указанным в правиле.

После установки приложения Kaspersky Endpoint Security список правил компонента Веб-Контроль не пуст. Предустановлено *Правило по умолчанию*. Это правило в зависимости от выбранного действия разрешает или запрещает всем пользователям доступ ко всем веб-ресурсам, которые не попадают под действие других правил.

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом. Например, Kaspersky Endpoint Security может определить корпоративный портал как социальную сеть. Чтобы ограничить доступ к социальным сетям и предоставить доступ к корпоративному веб-порталу, создайте два правила: запрещающее правило для категории веб-сайтов *Социальные сети* и разрешающее правило для корпоративного веб-портала. Правило доступа к корпоративному веб-порталу должно иметь приоритет выше, чем правило доступа к социальным сетям.

Как добавить правило доступа к веб-ресурсам в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Контроль безопасности** → **Веб-Контроль**.

4. Установите флажок **Веб-Контроль**.

5. В блоке **Настройки Веб-Контроля** нажмите на кнопку **Добавить**.

   Откроется окно **Правило доступа к веб-ресурсам**.

6. Настройте правило доступа к веб-ресурсам (см. таблицу ниже).

7. Если вы хотите, чтобы Веб-Контроль разрывал подключение к запрещенному веб-ресурсу сразу после применения политики, установите флажок **Завершать активные пользовательские сеансы браузера после применения правила**.

   > Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения.

   Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.

8. Сохраните внесенные изменения.

Как добавить правило доступа к веб-ресурсам в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности** → **Веб-Контроль**.

5. Включите переключатель **Веб-Контроль ВКЛЮЧЕН**.

6. В блоке **Список правил** нажмите на кнопку **Добавить**.

7. Настройте правило доступа к веб-ресурсам (см. таблицу ниже).

8. Если вы хотите, чтобы Веб-Контроль разрывал подключение к запрещенному веб-ресурсу сразу после применения политики, установите флажок **Завершать активные пользовательские сеансы браузера после применения правила**.

   > Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения.

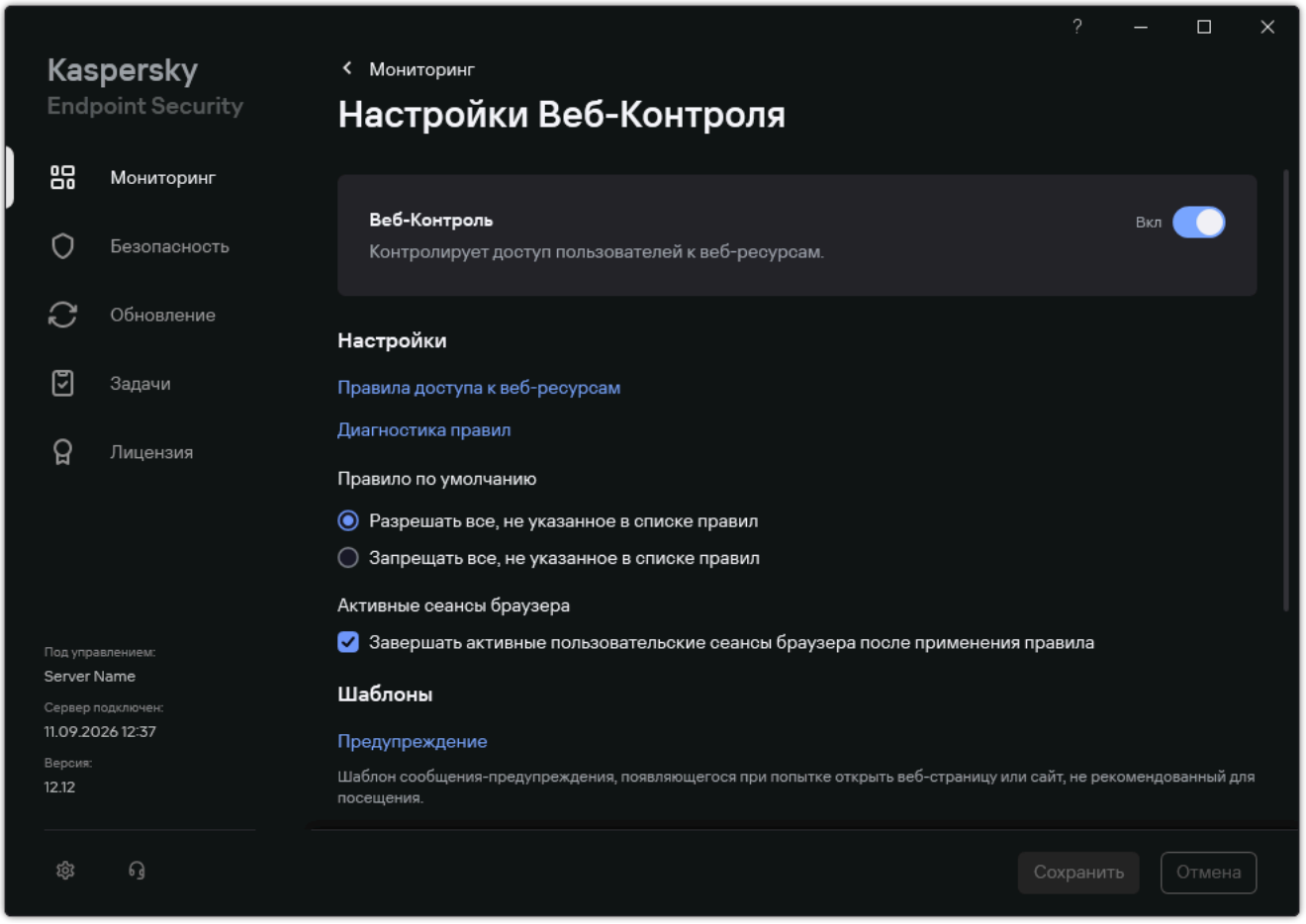
   Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.

9. Сохраните внесенные изменения.

Как добавить правило доступа к веб-ресурсам в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.



Параметры Веб-Контроля

3. Включите переключатель **Веб-Контроль**.

4. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.

5. В открывшемся окне нажмите на кнопку **Добавить**.

   Откроется окно **Правило доступа к веб-ресурсам**.

6. Настройте правило доступа к веб-ресурсам (см. таблицу ниже).

7. Если вы хотите, чтобы Веб-Контроль разрывал подключение к запрещенному веб-ресурсу сразу после применения политики, установите флажок **Завершать активные пользовательские сеансы браузера после применения правила**.

   > Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения.

   Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.

8. Сохраните внесенные изменения.

В результате новое правило Веб-Контроля будет добавлено в список. Если требуется, измените приоритет правила Веб-Контроля. Также вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя, не удаляя его из списка правил.

Параметры правила Веб-Контроля

Параметр	Описание
Название правила	Название правила Веб-Контроля.
Состояние	• **Активно**. • **Не активно**. Вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя.
Действие	• **Разрешать**. Веб-Контроль разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила. • **Запрещать**. Веб-Контроль запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила и выводит сообщение о запрете доступа. • **Предупреждать**. При попытке доступа к веб-ресурсам, удовлетворяющим правилу, Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
Содержимое фильтра	• **По категориям содержания**. Вы можете контролировать доступ пользователей к веб-ресурсам по категориям (например, категория *Социальные сети*). • **По типам данных**. Вы можете контролировать доступ пользователей к веб-ресурсам по размещенным данным, относящихся к определенным типам данных (например, *Графические файлы*).
Адреса	• **Ко всем адресам**. Веб-Контроль не фильтрует веб-ресурсы по адресам. • **К отдельным адресам**. Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Вы можете ввести веб-адрес или использовать маски. Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно. Если Проверка защищенных соединений отключена, для протокола HTTPS доступна фильтрация только по имени сервера.
Пользователи	• **Ко всем пользователям**. Веб-Контроль не фильтрует веб-ресурсы для отдельных пользователей. • **К отдельным пользователям и / или группам**. Веб-Контроль фильтрует веб-ресурсы только для отдельных пользователей. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.
Расписание работы правила	Расписание работы правила определяет время, когда Kaspersky Endpoint Security контролирует доступ к веб-ресурсам, указанным в правиле. Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Фильтр по адресам веб-ресурсов

Для контроля доступа к отдельным веб-ресурсам вам нужно создать правило Веб-Контроля, сформировать список веб-адресов и выбрать действие Веб-Контроля. При формировании списка веб-адресов вы можете ввести URL-адрес или использовать маски.

Правила могут включать в себя расписание работы правила и список пользователей, которым это правило назначено. Например, вы можете ограничить доступ к веб-сайтам только в рабочее время или разрешить посещение веб-сайтов только пользователям определенных групп.

Как включить фильтр по адресам веб-ресурсов в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Веб-Контроль**.
4. Установите флажок **Веб-Контроль**.
5. В блоке **Настройки Веб-Контроля** нажмите на кнопку **Добавить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
6. Настройте правило доступа к веб-ресурсам:
   a. В поле **Название** введите название правила.
   b. В раскрывающемся списке **Применять к адресам** выберите **К отдельным адресам**.
   c. Сформируйте список адресов веб-ресурсов. Вы можете ввести веб-адрес или использовать маски. Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла.

      Если Проверка защищенных соединений отключена, для протокола HTTPS доступна фильтрация только по имени сервера.

   d. В раскрывающемся списке **Применять к пользователям** выберите нужный фильтр для пользователей:

      - **Ко всем пользователям**. Веб-Контроль не фильтрует веб-ресурсы по адресам.
      - **К отдельным пользователям или группам**. Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Вы можете ввести веб-адрес или использовать маски. Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

e. В раскрывающемся списке **Действие** выберите нужный вариант:

- **Разрешать**. Веб-Контроль разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
- **Запрещать**. Веб-Контроль запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила и выводит сообщение о запрете доступа.
- **Предупреждать**. При попытке доступа к веб-ресурсам, удовлетворяющим правилу, Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

f. В раскрывающемся списке **Расписание работы правила** выберите расписание или сформируйте новое расписание.

7. Если вы хотите, чтобы Веб-Контроль разрывал подключение к запрещенному веб-ресурсу сразу после применения политики, установите флажок **Завершать активные пользовательские сеансы браузера после применения правила**.

> Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения.

Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.

8. Сохраните внесенные изменения.

Как включить фильтр по адресам веб-ресурсов в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Веб-Контроль**.
5. Включите переключатель **Веб-Контроль ВКЛЮЧЕН**.
6. В блоке **Список правил** нажмите на кнопку **Добавить**.
7. Настройте правило доступа к веб-ресурсам:

   a. В поле **Имя правила** введите название правила.

   b. Установите статус правила доступа к веб-ресурсам **Включен**.

   Вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя, не удаляя из списка правил.

c. В блоке **Действие** выберите нужный вариант:

- **Разрешать**. Веб-Контроль разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
- **Блокировать**. Веб-Контроль запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила и выводит сообщение о запрете доступа.
- **Информировать**. При попытке доступа к веб-ресурсам, удовлетворяющим правилу, Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

d. В блоке **Область применения** выберите **Отдельные веб-сайты**.

e. Настройте фильтр по содержанию:

- **Отдельный адрес**. Сформируйте список адресов веб-ресурсов. Вы можете ввести веб-адрес или использовать маски. Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла.

  > Если Проверка защищенных соединений отключена, для протокола HTTPS доступна фильтрация только по имени сервера.

- **Тип данных**. Вы можете контролировать доступ пользователей к веб-ресурсам по размещенным данным, относящихся к определенным типам данных (например, *Графические файлы*).

f. В блоке **Пользователь или группа** выберите пользователей, к которым Веб-Контроль будет применять правило.

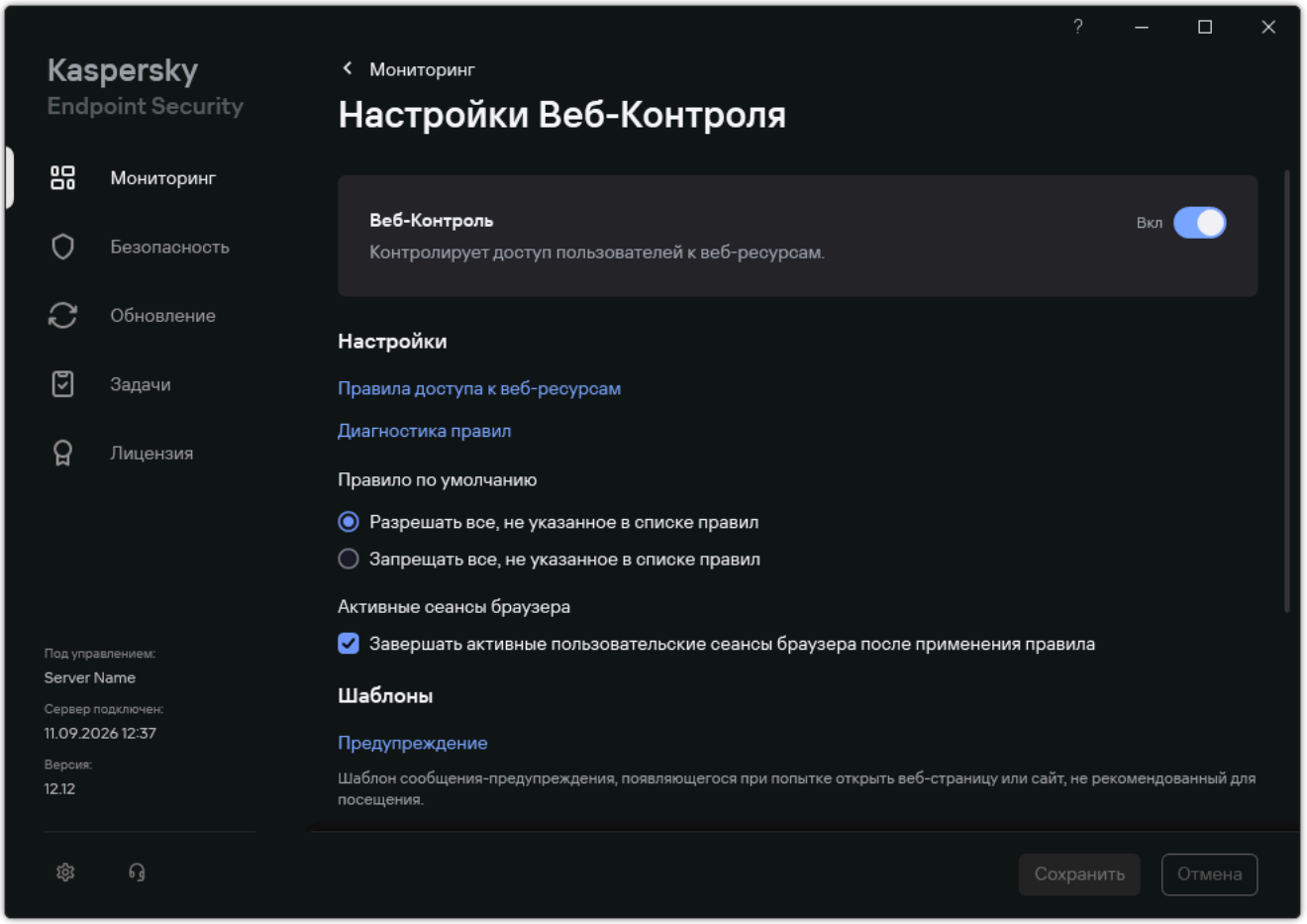
Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Вы можете ввести веб-адрес или использовать маски. Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

g. В блоке **Расписание доступа** выберите расписание или сформируйте новое расписание.

8. Сохраните внесенные изменения.

Как включить фильтр по адресам веб-ресурсов в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.



Параметры Веб-Контроля

3. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.
4. В открывшемся окне нажмите на кнопку **Добавить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
5. В поле **Название правила** введите название правила.
6. Установите статус правила доступа к веб-ресурсам **Активно**.

   Вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя.
7. В блоке **Действие** выберите нужный вариант:

   - **Разрешать**. Веб-Контроль разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
   - **Запрещать**. Веб-Контроль запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила и выводит сообщение о запрете доступа.
   - **Предупреждать**. При попытке доступа к веб-ресурсам, удовлетворяющим правилу, Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
8. В блоке **Адреса** выберите **К отдельным адресам**.

Сформируйте список адресов веб-ресурсов. Вы можете ввести веб-адрес или использовать маски. Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла.

> Если Проверка защищенных соединений отключена, для протокола HTTPS доступна фильтрация только по имени сервера.

9. В блоке **Пользователи** выберите нужный фильтр для пользователей:

   - **Ко всем пользователям**. Веб-Контроль не фильтрует веб-ресурсы для отдельных пользователей.
   - **К отдельным пользователям и / или группам**. Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Вы можете ввести веб-адрес или использовать маски. Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

10. В раскрывающемся списке **Расписание работы правила** выберите расписание или сформируйте новое расписание.

11. Если вы хотите, чтобы Веб-Контроль разрывал подключение к запрещенному веб-ресурсу сразу после применения политики, установите флажок **Завершать активные пользовательские сеансы браузера после применения правила**.

    > Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения.

    Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.

12. Сохраните внесенные изменения.

В результате новое правило Веб-Контроля будет добавлено в список. Если требуется, измените приоритет правила Веб-Контроля. Также вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя, не удаляя его из списка правил.

Фильтр по содержанию веб-ресурсов

Для контроля доступа по содержанию веб-ресурсов в Веб-Контроле предусмотрены следующие фильтры: фильтр по категориям и фильтр по типу данных.

Категоризацию веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз приложения). Вы можете ограничить доступ пользователей, например, к категории *Социальные сети* или другим категориям.

Вы можете ограничить доступ пользователей по типу данных и, например, скрыть графические изображения. Kaspersky Endpoint Security определяет тип данных по формату файла, а не по расширению. Веб-Контроль определяет следующие типы данных:

- Видео;
- Звуковые данные;

- Файлы офисных приложений;
- Исполняемые файлы;
- Архивы;
- Графические файлы;
- Скрипты.

Kaspersky Endpoint Security не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, Kaspersky Endpoint Security определит тип данных *Архивы*, а не *Графические файлы*.

Правила могут включать в себя расписание работы правила и список пользователей, которым это правило назначено. Например, вы можете ограничить доступ к веб-сайтам только в рабочее время или разрешить посещение веб-сайтов только пользователям определенных групп.

Как включить фильтр по содержанию веб-ресурсов в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Веб-Контроль**.
4. Установите флажок **Веб-Контроль**.
5. В блоке **Настройки Веб-Контроля** нажмите на кнопку **Добавить**.
   Откроется окно **Правило доступа к веб-ресурсам**.
6. Настройте правило доступа к веб-ресурсам:
   a. В поле **Название** введите название правила.
   b. В раскрывающемся списке **Фильтровать содержание** выберите нужный фильтр по содержанию:
      - **По категориям содержания**. Вы можете контролировать доступ пользователей к веб-ресурсам по категориям (например, категория *Социальные сети*).
      - **По типам данных**. Вы можете контролировать доступ пользователей к веб-ресурсам по размещенным данным, относящихся к определенным типам данных (например, *Графические файлы*).
      - **По категориям содержания и типам данных**. Фильтры по категориям содержания и типам данных включены.

   После выбора фильтров настройте их параметры.

c. В раскрывающемся списке **Применять к пользователям** выберите нужный фильтр для пользователей:

- **Ко всем пользователям**. Веб-Контроль не фильтрует веб-ресурсы по адресам.
- **К отдельным пользователям или группам**. Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Вы можете ввести веб-адрес или использовать маски. Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

d. В раскрывающемся списке **Действие** выберите нужный вариант:

- **Разрешать**. Веб-Контроль разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
- **Запрещать**. Веб-Контроль запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила и выводит сообщение о запрете доступа.
- **Предупреждать**. При попытке доступа к веб-ресурсам, удовлетворяющим правилу, Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

e. В раскрывающемся списке **Расписание работы правила** выберите расписание или сформируйте новое расписание.

7. Если вы хотите, чтобы Веб-Контроль разрывал подключение к запрещенному веб-ресурсу сразу после применения политики, установите флажок **Завершать активные пользовательские сеансы браузера после применения правила**.

   Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения.

   Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.

8. Сохраните внесенные изменения.

Как включить фильтр по содержанию веб-ресурсов в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Веб-Контроль**.
5. Включите переключатель **Веб-Контроль ВКЛЮЧЕН**.
6. В блоке **Список правил** нажмите на кнопку **Добавить**.

7. Настройте правило доступа к веб-ресурсам:

   a. В поле **Имя правила** введите название правила.

   b. Установите статус правила доступа к веб-ресурсам **Включен**.

      Вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя.

   c. В блоке **Действие** выберите нужный вариант:

      - **Разрешать**. Веб-Контроль разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
      - **Блокировать**. Веб-Контроль запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила и выводит сообщение о запрете доступа.
      - **Информировать**. При попытке доступа к веб-ресурсам, удовлетворяющим правилу, Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

   d. В блоке **Область применения** выберите **Категория содержания**.

   e. Настройте фильтр по содержанию:

      - **Категория содержания**. Вы можете контролировать доступ пользователей к веб-ресурсам по категориям (например, категория *Социальные сети*).
      - **Тип данных**. Вы можете контролировать доступ пользователей к веб-ресурсам по размещенным данным, относящихся к определенным типам данных (например, *Графические файлы*).

   f. В блоке **Пользователь или группа** выберите пользователей, к которым Веб-Контроль будет применять правило.

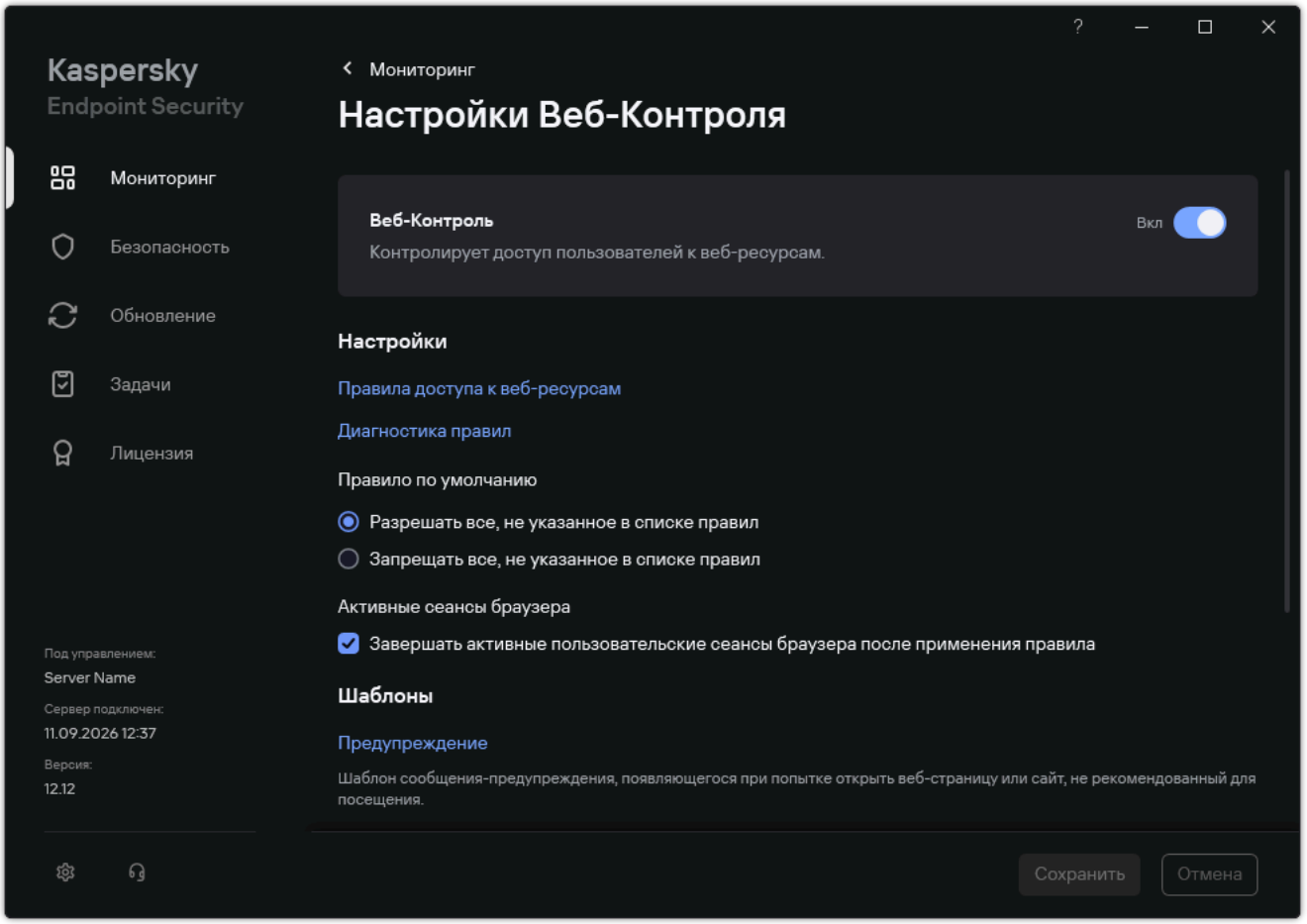
      Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Вы можете ввести веб-адрес или использовать маски. Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   g. В блоке **Расписание доступа** выберите расписание или сформируйте новое расписание.

8. Сохраните внесенные изменения.

Как включить фильтр по содержанию веб-ресурсов в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.



Параметры Веб-Контроля

3. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.
4. В открывшемся окне нажмите на кнопку **Добавить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
5. В поле **Название правила** введите название правила.
6. Установите статус правила доступа к веб-ресурсам **Активно**.

   Вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя.
7. В блоке **Действие** выберите нужный вариант:

   - **Разрешать**. Веб-Контроль разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
   - **Запрещать**. Веб-Контроль запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила и выводит сообщение о запрете доступа.
   - **Предупреждать**. При попытке доступа к веб-ресурсам, удовлетворяющим правилу, Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

8. В блоке **Содержимое фильтра** выберите нужный фильтр по содержанию:

   - **По категориям содержания**. Вы можете контролировать доступ пользователей к веб-ресурсам по категориям (например, категория *Социальные сети*).
   - **По типам данных**. Вы можете контролировать доступ пользователей к веб-ресурсам по размещенным данным, относящихся к определенным типам данных (например, *Графические файлы*).

   Для настройки фильтра по содержанию выполните следующие действия:

   a. Нажмите на ссылку **Настроить**.

   b. Установите флажки напротив названий желаемых категорий содержания и / или типов данных.

   Установка флажка напротив названия категории содержания и / или типа данных означает, что Kaspersky Endpoint Security, в соответствии с правилом, контролирует доступ к веб-ресурсам, принадлежащим к выбранным категориям содержания и / или типам данных.

   c. Вернитесь в окно настройки правила доступа к веб-ресурсам.

9. В блоке **Пользователи** выберите нужный фильтр для пользователей:

   - **Ко всем пользователям**. Веб-Контроль не фильтрует веб-ресурсы по адресам.
   - **К отдельным пользователям и / или группам**. Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Вы можете ввести веб-адрес или использовать маски. Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно. Для создания списка пользователей, к которым вы хотите применить правило, выполните следующие действия:

     a. Нажмите на кнопку **Добавить**.

     b. В открывшемся окне выберите пользователей или группы пользователей, к которым вы хотите применить правило доступа к веб-ресурсам.

     c. Вернитесь в окно настройки правила доступа к веб-ресурсам.

10. Выберите из раскрывающегося списка **Расписание работы правила** название нужного расписания или сформируйте новое расписание на основе выбранного расписания работы правила. Для этого выполните следующие действия:

    a. Нажмите на кнопку **Изменить или добавить новое**.

    b. В открывшемся окне нажмите на кнопку **Добавить**.

    c. В открывшемся окне введите название расписания работы правила.

    d. Настройте расписание доступа к веб-ресурсам для пользователей.

    e. Вернитесь в окно настройки правила доступа к веб-ресурсам.

11. Если вы хотите, чтобы Веб-Контроль разрывал подключение к запрещенному веб-ресурсу сразу после применения политики, установите флажок **Завершать активные пользовательские сеансы браузера после применения правила**.

Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения.

Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.

12. Сохраните внесенные изменения.

В результате новое правило Веб-Контроля будет добавлено в список. Если требуется, измените приоритет правила Веб-Контроля. Также вы можете в любое время выключить правило доступа к веб-ресурсам с помощью переключателя, не удаляя его из списка правил.

Проверка работы правил доступа к веб-ресурсам

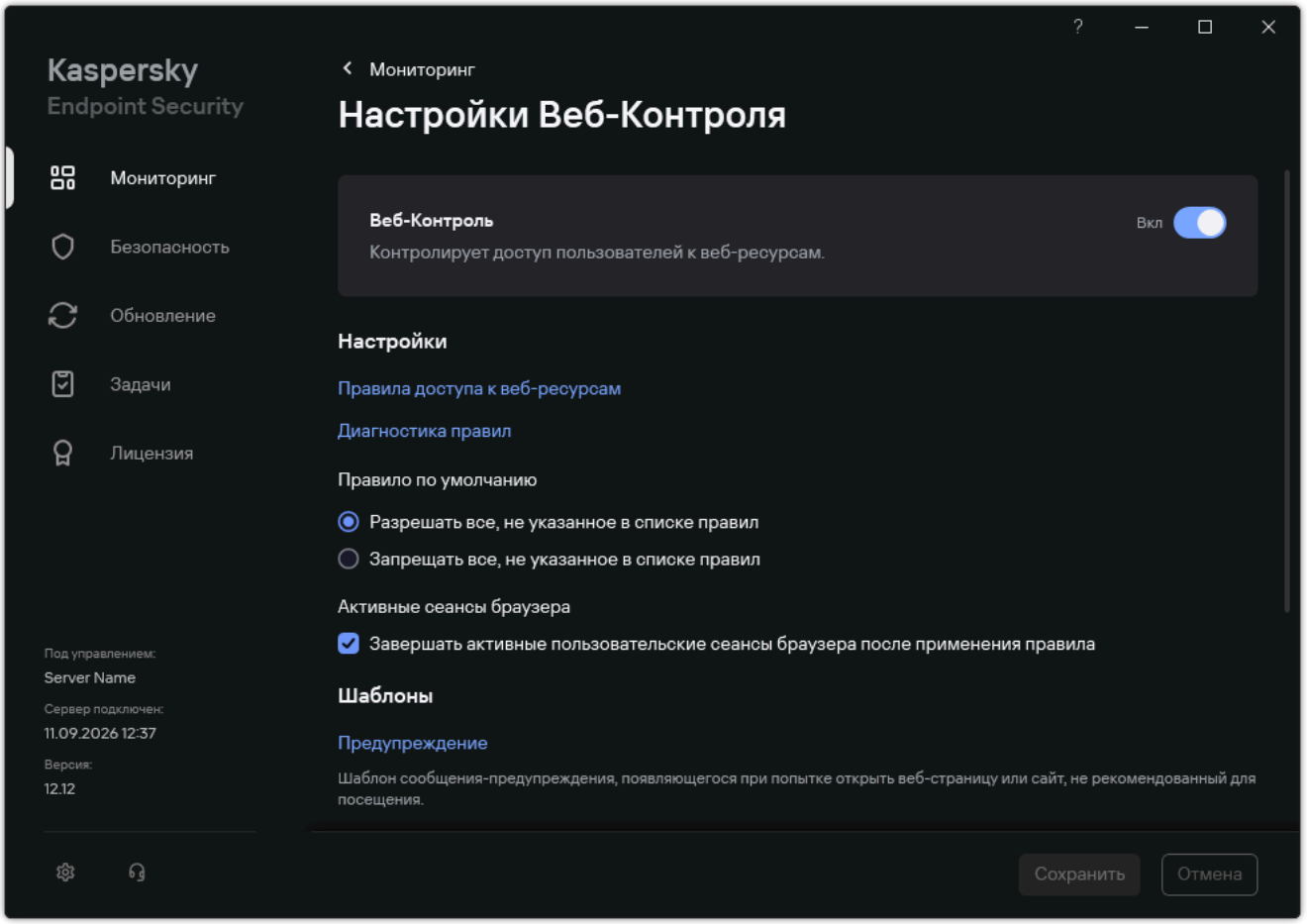
При настройке Веб-Контроля вы можете случайно заблокировать доступ к веб-ресурсам, необходимым пользователям для работы. Для определения правила Веб-Контроля, которое блокирует доступ к веб-ресурсам, предназначен инструмент *Диагностика правил Веб-Контроля*. Диагностика правил Веб-Контроля доступна только в интерфейсе Kaspersky Endpoint Security. В консоли Kaspersky Security Center определить правило Веб-Контроля, которое включает в себя веб-ресурс, невозможно.

Если блокировка доступа к веб-ресурсу, по мнению пользователя, была ошибочна, по ссылке из сообщения о блокировке веб-ресурса пользователь может отправить уже сформированное сообщение администратору локальной сети организации.

Чтобы проверить работу правил доступа к веб-ресурсам, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.



Параметры Веб-Контроля

3. В блоке **Настройки** нажмите на ссылку **Диагностика правил**.

   Откроется окно **Диагностика правил**.

4. Установите флажок **Укажите адрес**, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к определенному веб-ресурсу. В поле ниже введите адрес веб-ресурса.

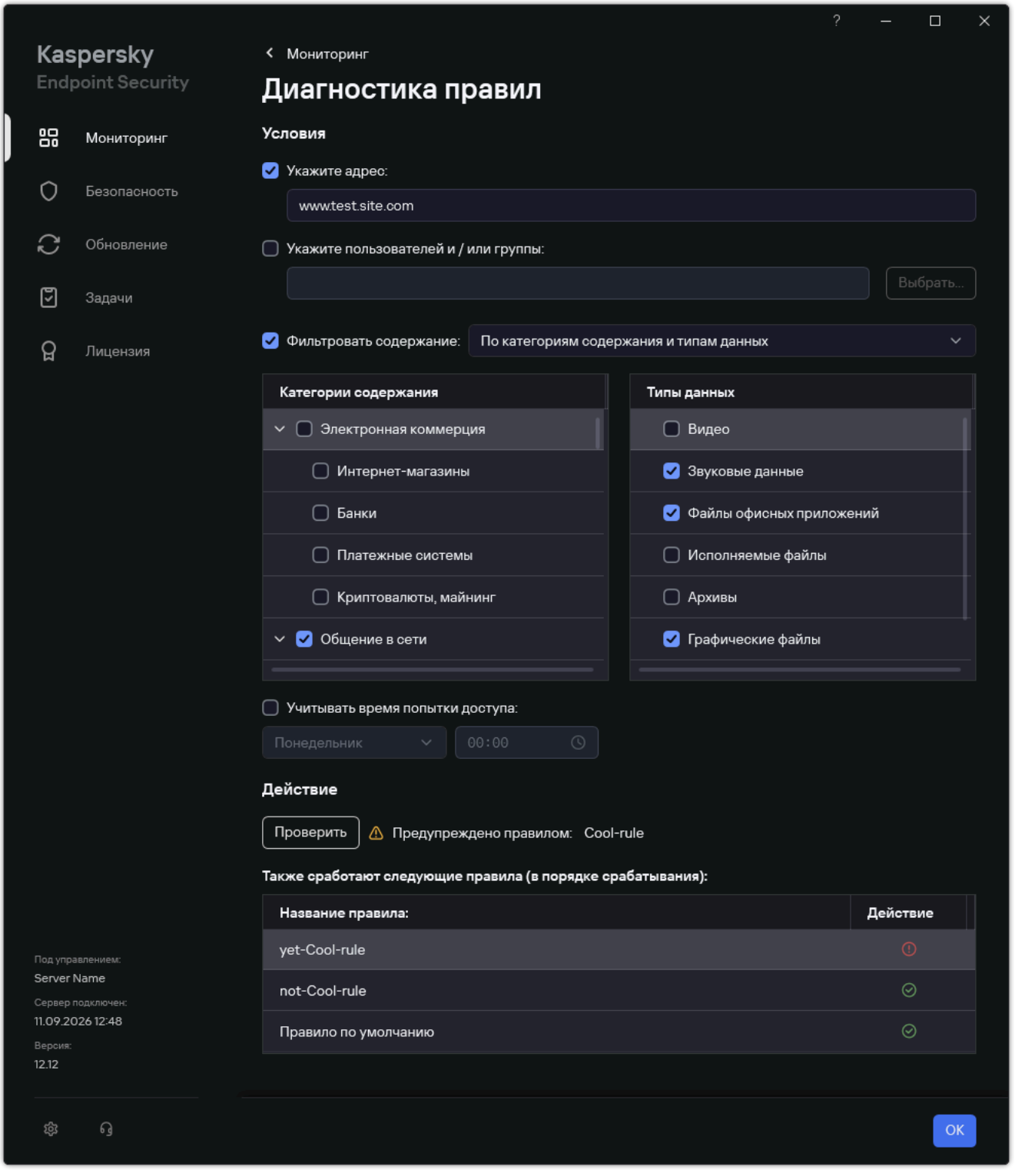
5. Задайте список пользователей и / или групп пользователей, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к веб-ресурсам для определенных пользователей и / или групп пользователей.

6. Установите флажок **Фильтровать содержание** и в раскрывающемся списке выберите нужный элемент (**По категориям содержания**, **По типам данных** или **По категориям содержания и типам данных**), если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к веб-ресурсам определенных категорий содержания и / или категорий типа данных.

7. Установите флажок **Учитывать время попытки доступа**, если вы хотите проверить работу правил с учетом дня недели и времени совершения попытки доступа к веб-ресурсам, указанным в условиях диагностики правил. Далее укажите день недели и время.

8. Нажмите на кнопку **Проверить**.

В результате проверки выводится сообщение о действии Kaspersky Endpoint Security в соответствии с первым сработавшим правилом при попытке доступа к заданному веб-ресурсу (разрешение, запрет, предупреждение). Первым срабатывает правило, которое находится в списке правил Веб-Контроля выше других правил, удовлетворяющих условиям диагностики. Сообщение выводится справа от кнопки **Проверить**. В таблице ниже выводится список остальных сработавших правил с указанием действия, которое выполняет Kaspersky Endpoint Security. Правила выводятся в порядке убывания приоритета.



Результат проверки доступа к веб-ресурсам

Экспорт и импорт правил Веб-Контроля

Вы можете экспортировать список правил Веб-Контроля в файл в формате XML или JSON. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных адресов. Вы можете использовать функцию экспорта / импорта для резервного копирования списка правил Веб-Контроля или для миграции списка на другой сервер.

Как экспортировать / импортировать список правил Веб-Контроля в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Веб-Контроль**.
4. Для экспорта списка правил Веб-Контроля выполните следующие действия:
   a. Выберите правила, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

      Если вы не выбрали ни одного правила, Kaspersky Endpoint Security экспортирует все правила.

   b. Нажмите на ссылку **Экспортировать**.
   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список правил, а также выберите папку, в которой вы хотите сохранить этот файл.
   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл.
5. Для импорта списка правил Веб-Контроля выполните следующие действия:
   a. Нажмите на ссылку **Импортировать**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

   b. Откройте файл.

      Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
6. Сохраните внесенные изменения.

Как экспортировать / импортировать список правил Веб-Контроля в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Веб-Контроль**.

5. Для экспорта списка правил в блоке **Список правил** выполните следующие действия:

   a. Выберите правила, которые вы хотите экспортировать.

   b. Нажмите на кнопку → **Экспортировать**.

      Kaspersky Endpoint Security экспортирует список правил в JSON-файл в папку для загрузки по умолчанию.

6. Для импорта списка правил в блоке **Список правил** выполните следующие действия:

   a. Нажмите на кнопку → **Импортировать**.

      В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список правил.

   b. Откройте файл.

      Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.

7. Сохраните внесенные изменения.

Экспорт и импорт адресов веб-ресурсов правила Веб-Контроля

Если в правиле доступа к веб-ресурсам вы сформировали список адресов веб-ресурсов, вы можете экспортировать его в файл:

- Файл в формате TXT в Консоли администрирования (MMC).
- Файл в формате JSON в Web Console.
- Файл в формате CSV в интерфейсе приложения.

В дальнейшем вы можете импортировать список из этого файла, чтобы при настройке правила не создавать список адресов веб-ресурсов вручную. Возможность экспорта и импорта списка адресов веб-ресурсов может понадобиться, например, если вы создаете правила со сходными параметрами.

Вы также можете выполнить экспорт / импорт всех правил Веб-Контроля, а не только адресов веб-ресурсов отдельного правила.

Как экспортировать / импортировать адреса веб-ресурсов правила Веб-Контроля в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Контроль безопасности** → **Веб-Контроль**.

5. В блоке **Настройки Веб-Контроля** выберите правило, список адресов веб-ресурсов которого вы хотите экспортировать или импортировать.

   Откроются свойства правила Веб-Контроля.

6. Для экспорта списка веб-ресурсов в списке адресов выполните следующие действия:

   a. Выберите адреса, которые вы хотите экспортировать.

      Если вы не выбрали ни одного адреса, Kaspersky Endpoint Security экспортирует все адреса.

   b. Нажмите на кнопку .

   c. В открывшемся окне введите имя файла формата TXT, в который вы хотите экспортировать список адресов веб-ресурсов, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список адресов веб-ресурсов в TXT-файл.

7. Для импорта списка веб-ресурсов в списке адресов выполните следующие действия:

   a. Нажмите на кнопку .

      В открывшемся окне выберите TXT-файл, из которого вы хотите импортировать список веб-ресурсов.

   b. Откройте файл.

      Если на компьютере уже есть список адресов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из TXT-файла.

8. Для применения политики на компьютерах закройте замки , сохраните внесенные изменения.

Как экспортировать / импортировать адреса веб-ресурсов правила Веб-Контроля в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности** → **Веб-Контроль**.

5. В блоке **Список правил** выберите правило, список адресов веб-ресурсов которого вы хотите экспортировать или импортировать.

   Откроются свойства правила Веб-Контроля.

6. В блоке **Область применения** → **Отдельные веб-сайты** нажмите на кнопку **Изменить**.

7. Для экспорта списка веб-ресурсов в списке адресов выполните следующие действия:

   a. Выберите адреса, которые вы хотите экспортировать.

   b. Нажмите на кнопку → **Экспортировать**.

      Kaspersky Endpoint Security экспортирует список адресов веб-ресурсов в JSON-файл в папку для загрузки по умолчанию.

8. Для импорта списка веб-ресурсов в списке адресов выполните следующие действия:

   a. Нажмите на кнопку → **Импортировать**.

      В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список адресов веб-ресурсов.

   b. Откройте файл.

      Если на компьютере уже есть список адресов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.

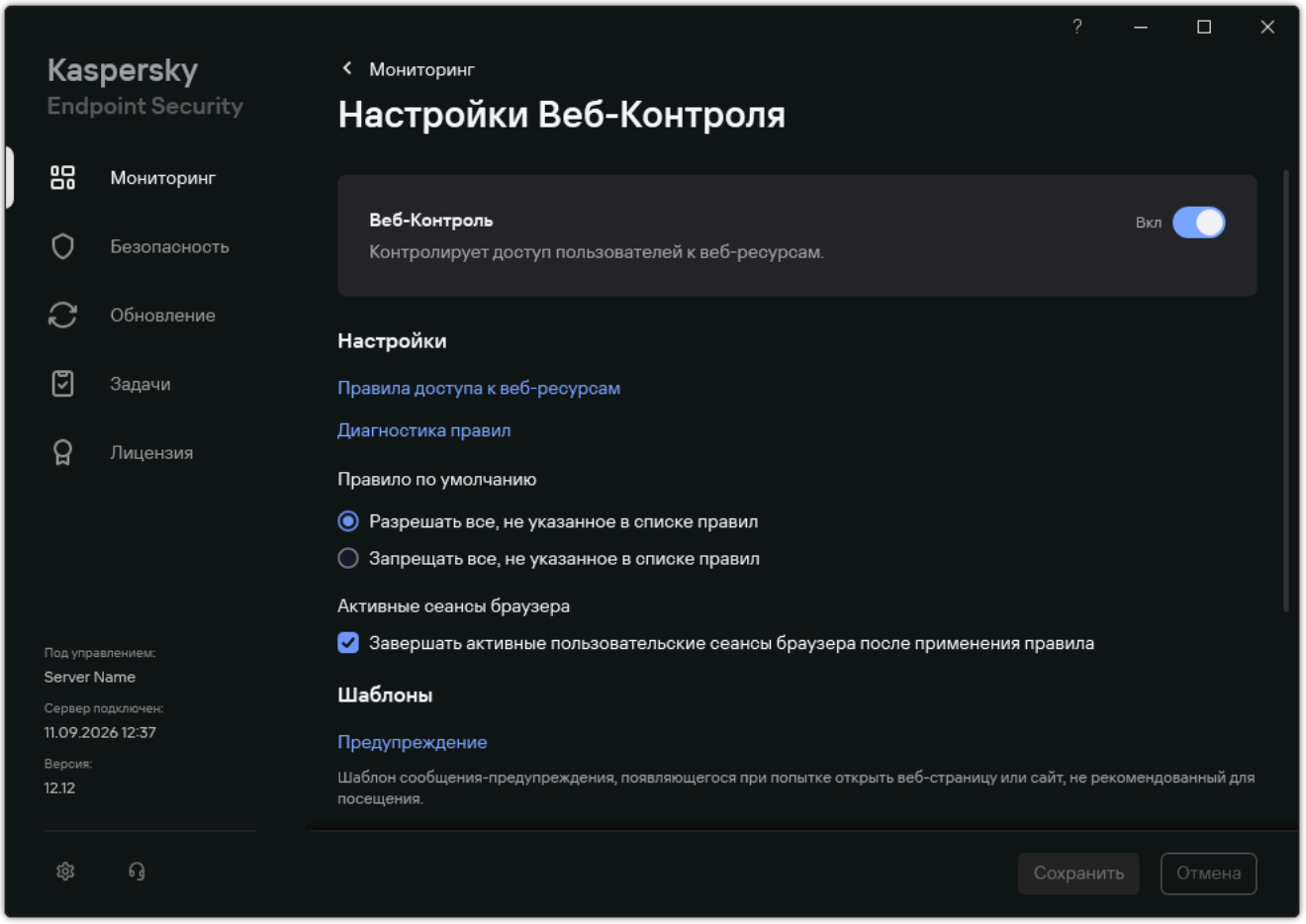
   Таким же образом вы можете экспортировать и импортировать группы веб-сайтов.

9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как экспортировать / импортировать адреса веб-ресурсов правила Веб-Контроля в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.



Параметры Веб-Контроля

3. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.

4. Выберите правило, список адресов веб-ресурсов которого вы хотите экспортировать или импортировать.

5. Для экспорта списка доверенных веб-ресурсов в блоке **Адреса** выполните следующие действия:

   a. Выберите адреса, которые вы хотите экспортировать.

      Если вы не выбрали ни одного адреса, Kaspersky Endpoint Security экспортирует все адреса.

   b. Нажмите на кнопку **Экспорт**.

   c. В открывшемся окне введите имя файла формата CSV, в который вы хотите экспортировать список адресов веб-ресурсов, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список адресов веб-ресурсов в CSV-файл.

6. Для импорта списка веб-ресурсов в блоке **Адреса** выполните следующие действия:

   a. Нажмите на кнопку **Импорт**.

      В открывшемся окне выберите CSV-файл, из которого вы хотите импортировать список веб-ресурсов.

   b. Откройте файл.

      Если на компьютере уже есть список адресов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из CSV-файла.

7. Сохраните внесенные изменения.

Мониторинг активности пользователей в интернете

Kaspersky Endpoint Security позволяет записывать данные о посещении пользователями всех веб-сайтов, в том числе и разрешенных. Таким образом, вы можете получить полную историю просмотров в браузере. Kaspersky Endpoint Security отправляет события активности пользователя в Kaspersky Security Center, локальный журнал Kaspersky Endpoint Security, журнал событий Windows. Для получения событий в Kaspersky Security Center нужно настроить параметры событий в политике в Консоли администрирования или Web Console. Также вы можете настроить отправку событий Веб-Контроля по электронной почте и отображение уведомлений на экране компьютера пользователя.

Браузеры, которые поддерживают функцию мониторинга: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Яндекс.Браузер, Mozilla Firefox. Мониторинг активности пользователей не работает в других браузерах.

Kaspersky Endpoint Security создает следующие события активности пользователя в интернете:

- блокировка веб-сайта (статус *Критическое*);
- посещение нерекомендованного веб-сайта (статус *Предупреждение*);
- посещение разрешенного веб-сайта (статус *Информационное сообщение*).

Для мониторинга активности необходимо выполнить следующие действия:

- Внедрите в трафик скрипт взаимодействия с веб-страницами (см. инструкцию ниже). Скрипт позволяет регистрировать события работы Веб-Контроля.
- Для контроля HTTPS-трафика нужно включить проверку защищенных соединений.

Внедрение скрипта взаимодействия с веб-страницами

Как внедрить в трафик скрипт взаимодействия с веб-страницами в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Настройки сети**.
4. В блоке **Проверка защищенных соединений** установите флажок **Внедрять в трафик скрипт взаимодействия с веб-страницами**.
5. Сохраните внесенные изменения.

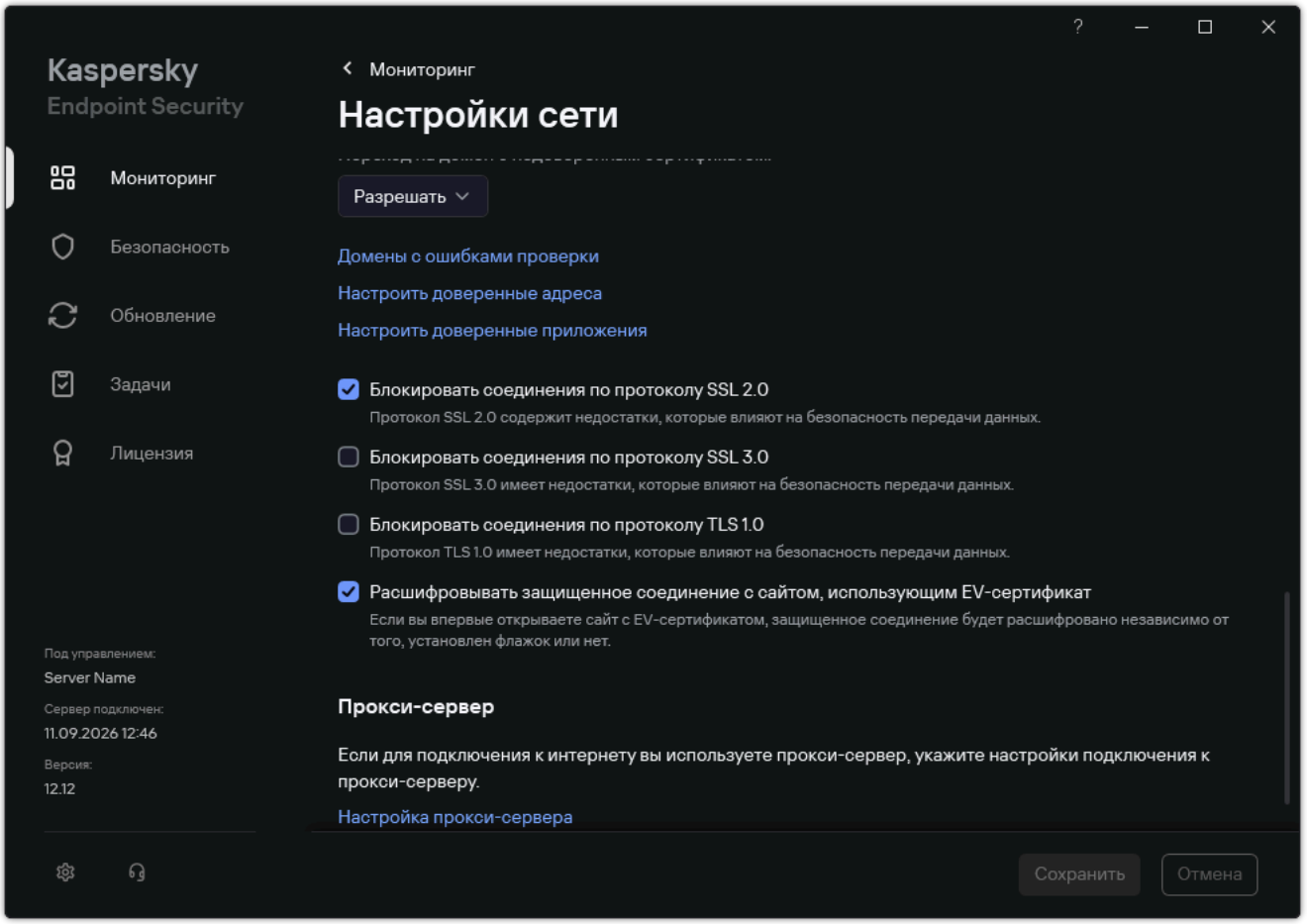
Как внедрить в трафик скрипт взаимодействия с веб-страницами в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. В окне политики выберите **Общие настройки** → **Настройки сети**.
5. В блоке **Проверка защищенных соединений** перейдите по ссылке **Настройки**.
6. В открывшемся окне установите флажок **Внедрять в трафик скрипт взаимодействия с веб-страницами**.
7. Сохраните внесенные изменения.

Как внедрить в трафик скрипт взаимодействия с веб-страницами в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.



Параметры сети приложения

3. В блоке **Обработка трафика** установите флажок **Внедрять в трафик скрипт взаимодействия с веб-страницами**.
4. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security внедрит в трафик скрипт взаимодействия с веб-страницами. Скрипт позволяет регистрировать события работы Веб-Контроля для журнала событий приложения, журнала событий ОС, отчетов. В своей работе скрипт постоянно обращается к серверам `*.scr.kaspersky-labs.com` для передачи статистики проверенных веб-страниц и выполненных действий (доступ разрешен или заблокирован).

Настройка записи событий Веб-Контроля

Чтобы настроить запись событий Веб-Контроля на компьютере пользователя, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки интерфейса**.
3. В блоке **Уведомления** нажмите на кнопку **Настроить уведомления**.

4. В открывшемся окне выберите раздел **Веб-Контроль**.

   Откроется таблица событий Веб-Контроля и способов уведомлений.

5. Настройте для каждого события способ уведомления: **Сохранять в локальном отчете** и **Сохранять в журнале событий Windows**.

   Для записи событий посещения разрешенных веб-сайтов нужно дополнительно настроить Веб-Контроль (см. инструкцию ниже).

   Также в таблице событий вы можете включить уведомление на экране и уведомление по электронной почте. Для отправки уведомлений по почте нужно настроить параметры SMTP-сервера. Подробнее об отправке уведомлений по почте см. в справке Kaspersky Security Center.

6. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security начинает записывать события активности пользователя в интернете.

Веб-Контроль отправляет события активности пользователя в Kaspersky Security Center следующим образом:

- Если вы используете Kaspersky Security Center, Веб-Контроль отправляет события по всем объектам, из которых состоит веб-страница. Поэтому при блокировании одной веб-страницы может быть создано несколько событий. Например, при блокировании веб-страницы http://www.example.com Kaspersky Endpoint Security может отправить события по следующим объектам: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js и так далее.

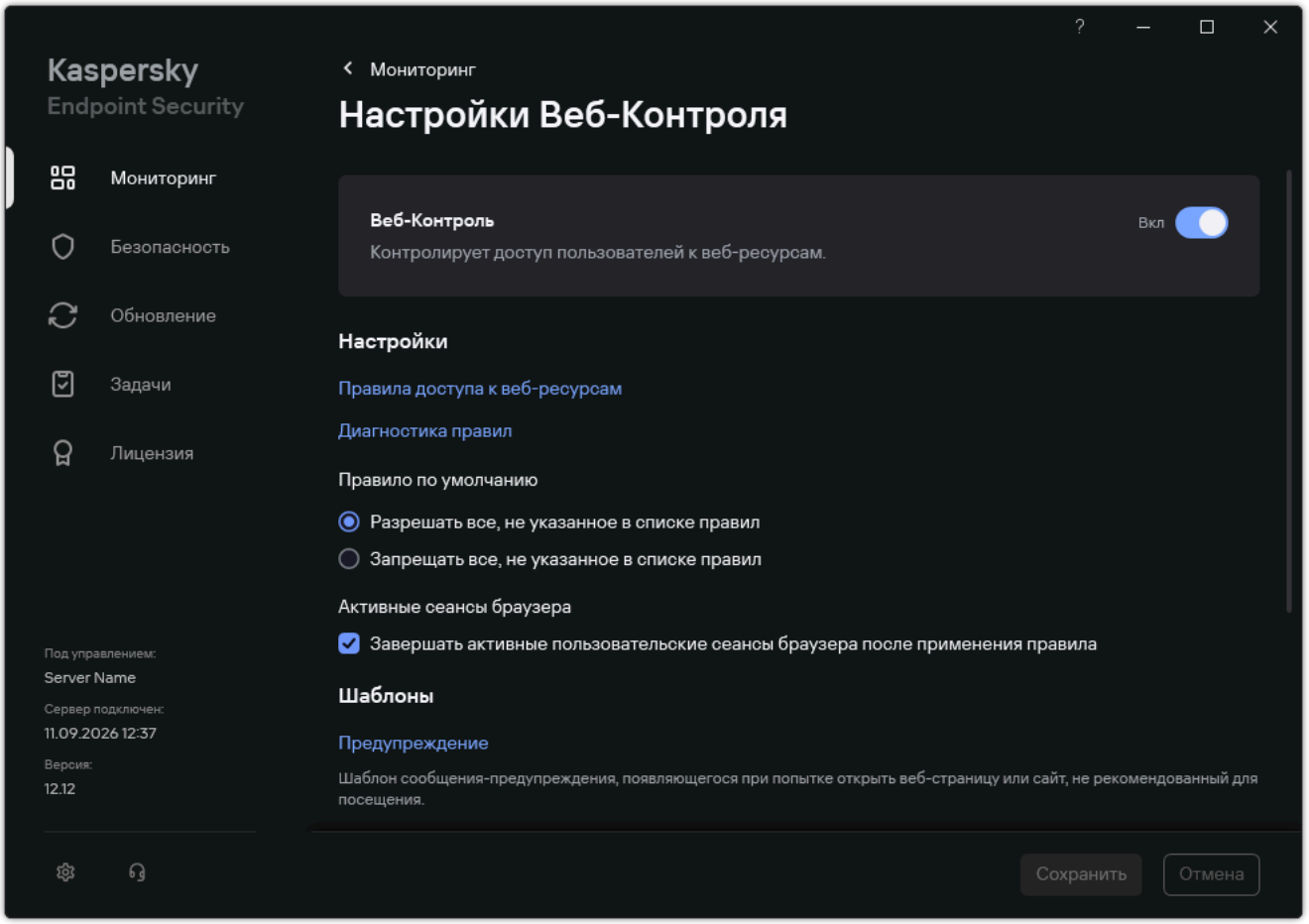
- Если вы используете Kaspersky Security Center Cloud Console, Веб-Контроль группирует события и отправляет только протокол и домен веб-сайта. Например, если пользователь посетил нерекомендованные веб-страницы http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, то Kaspersky Endpoint Security отправит только одно событие с объектом http://www.example.com.

Запись событий посещения разрешенных веб-сайтов

Чтобы включить запись событий посещения разрешенных веб-сайтов, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

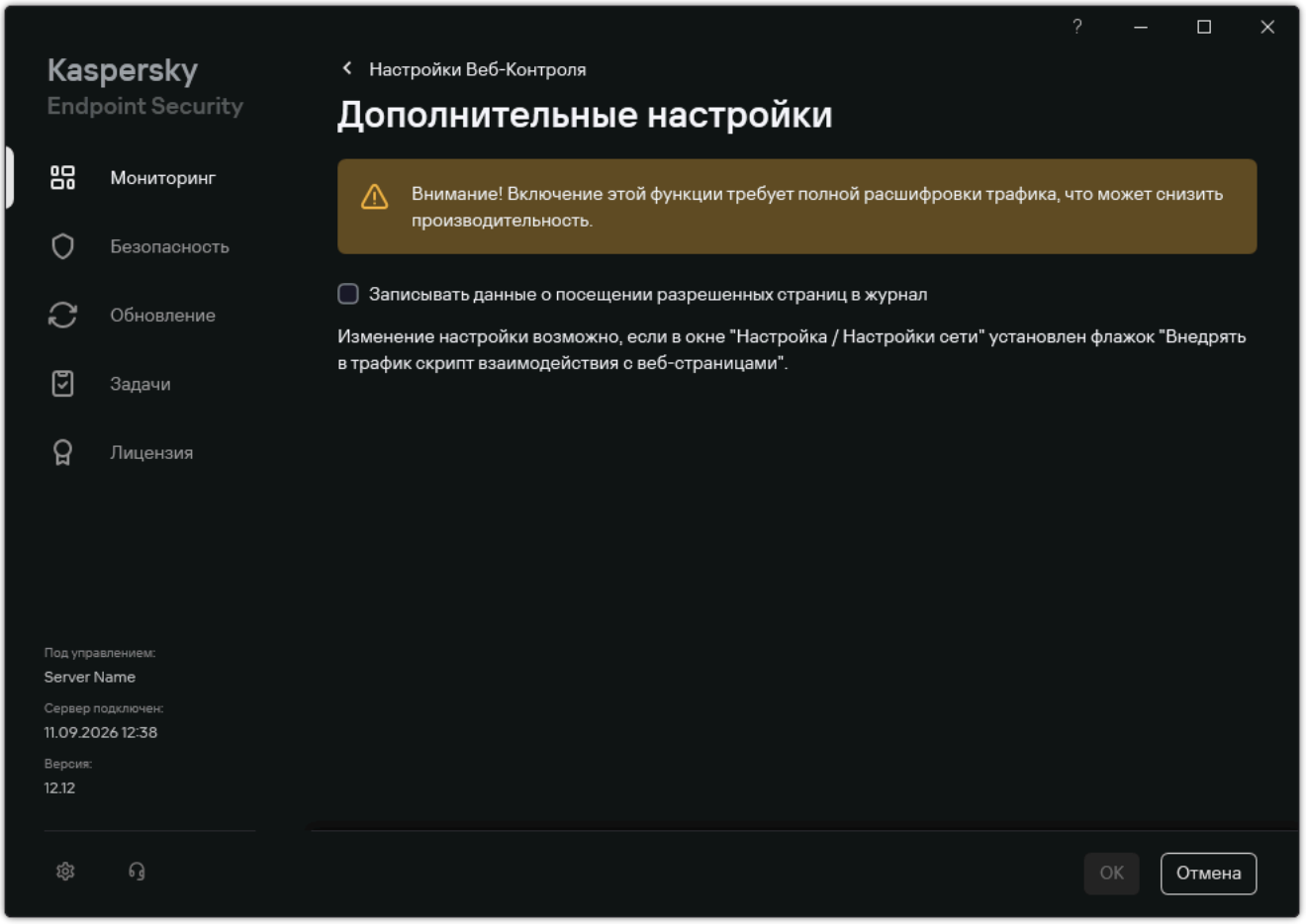
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.



Параметры Веб-Контроля

3. В блоке **Дополнительно** нажмите на кнопку **Дополнительные настройки**.

4. В открывшемся окне установите флажок **Записывать данные о посещении разрешенных страниц в журнал**.



Дополнительные параметры Веб-Контроля

5. Сохраните внесенные изменения.

В результате вам будет доступна полная история просмотров в браузере.

Изменение шаблонов сообщений Веб-Контроля

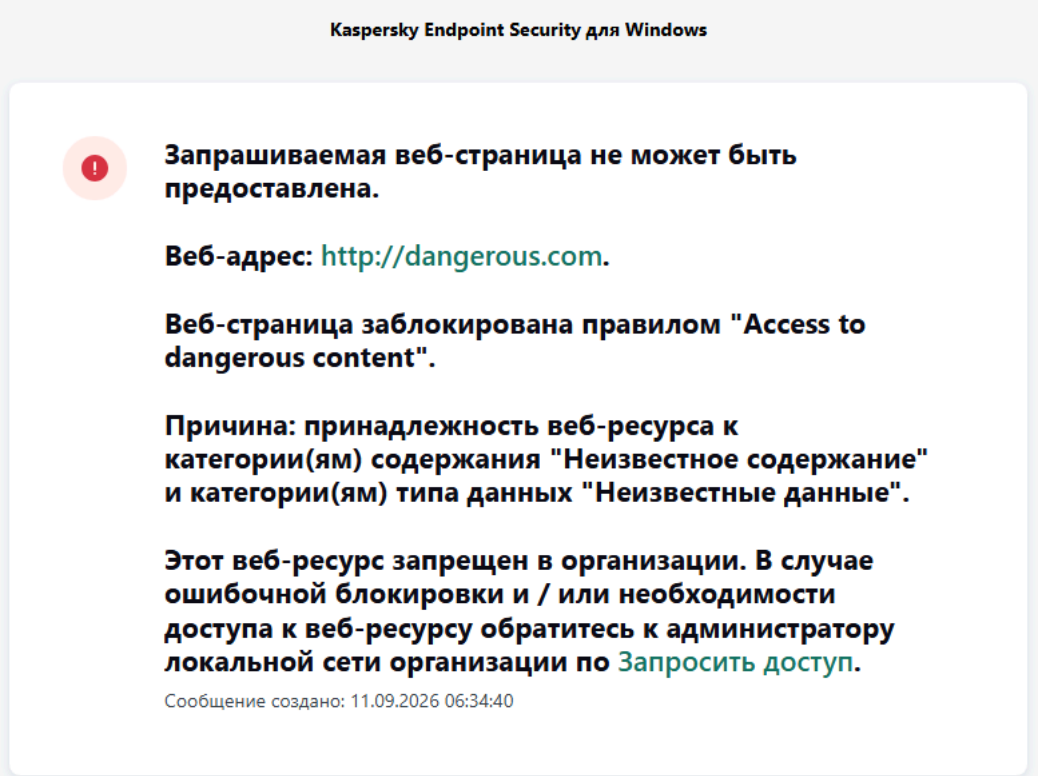
В зависимости от действия, заданного в свойствах правил Веб-Контроля, при попытке пользователей получить доступ к веб-ресурсам Kaspersky Endpoint Security выводит сообщение (подменяет ответ HTTP-сервера HTML-страницей с сообщением) одного из следующих типов:

- Сообщение-предупреждение. Такое сообщение предупреждает пользователя о том, что посещение веб-ресурса не рекомендуется и / или не соответствует корпоративной политике безопасности. Kaspersky Endpoint Security выводит сообщение-предупреждение, если в параметрах правила, описывающего этот веб-ресурс, выбрано действие **Предупреждать**.

  Если, по мнению пользователя, предупреждение ошибочно, по ссылке из предупреждения пользователь может отправить уже сформированное сообщение администратору локальной сети организации.

- Сообщение о блокировке веб-ресурса. Kaspersky Endpoint Security выводит сообщение о блокировке веб-ресурса (см. рис. ниже), если в параметрах правила, которое описывает этот веб-ресурс, выбрано действие **Запрещать**.

Если блокировка доступа к веб-ресурсу, по мнению пользователя, была ошибочна, по ссылке из сообщения о блокировке веб-ресурса пользователь может отправить уже сформированное сообщение администратору локальной сети организации.



Сообщение о блокировке веб-ресурса

Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и сообщения для отправки администратору локальной сети организации предусмотрены шаблоны. Для работы с шаблонами сообщений предусмотрены специальные переменные (например, %USER_NAME%). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров. При формировании сообщения Kaspersky Endpoint Security определяет значение переменной из настроек операционной системы и подставляет это значение в сообщение, соответствующие конкретному компьютеру, пользователю и событию.

Как изменить шаблон сообщений Веб-Контроля в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Веб-Контроль**.
4. В блоке **Настройки шаблонов сообщений** нажмите на кнопку **Шаблоны**.

5. Настройте шаблоны сообщений Веб-Контроля:

   - **Предупреждение**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу.

   - **Сообщение о блокировке**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу.

   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете доступа к веб-странице**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

   Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Переменная** и выберите нужную переменную из списка доступных.

   Также вы можете восстановить текст шаблона по умолчанию с помощью кнопки **По умолчанию**.

6. Сохраните внесенные изменения.

Как изменить шаблон сообщений Веб-Контроля в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности → Веб-Контроль**.

5. В блоке **Шаблоны сообщений** перейдите по ссылке **Сообщение о блокировке сайта** и настройте шаблоны сообщений Веб-Контроля:

   - **Предупреждение**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу.

   - **Сообщение о блокировке**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу.

   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете доступа к веб-странице**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

   Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Добавить переменную** и выберите нужную переменную из списка доступных.

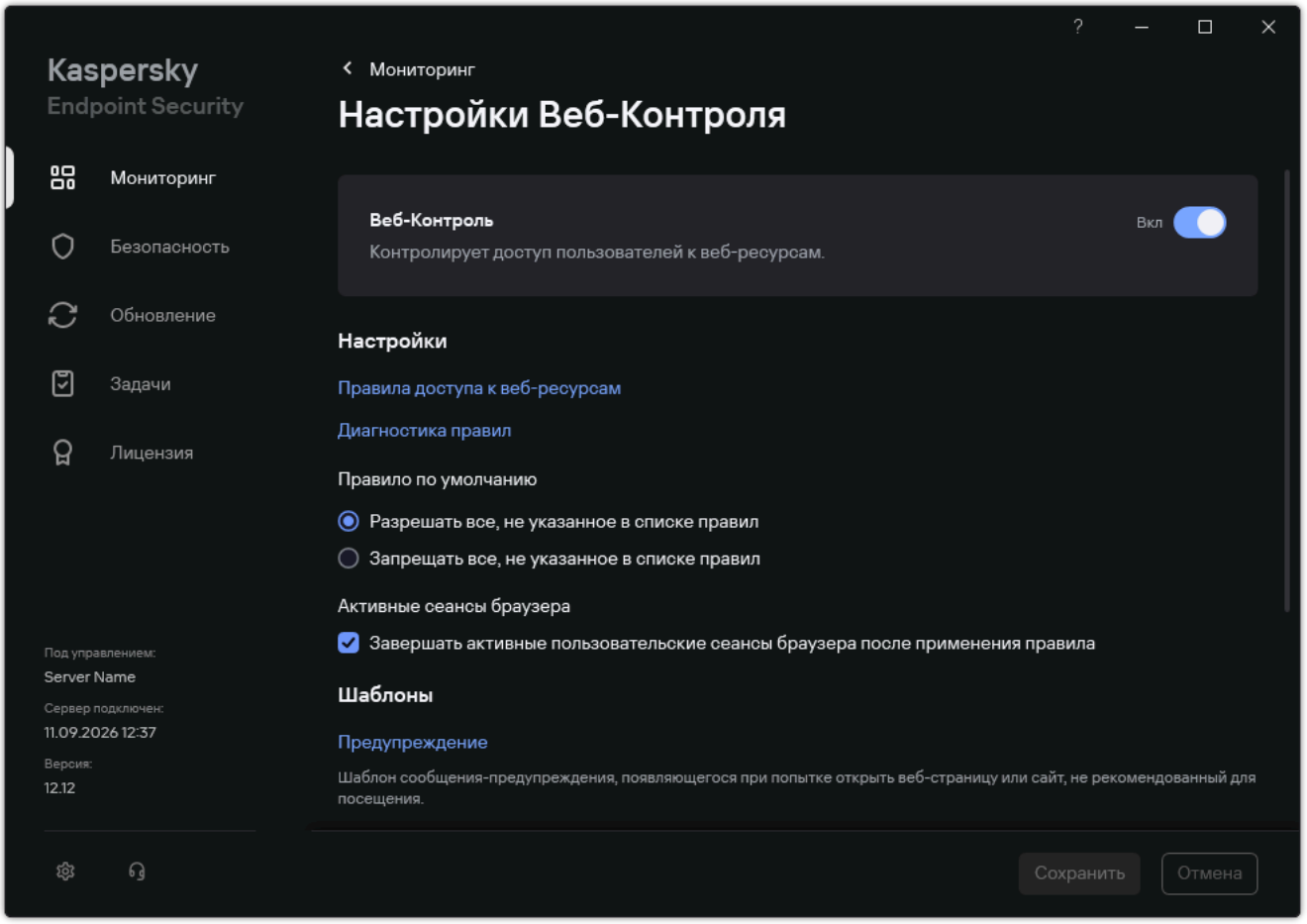
Также вы можете восстановить текст шаблона по умолчанию с помощью кнопки **Восстановить по умолчанию**.

6. Сохраните внесенные изменения.

Как изменить шаблон сообщений Веб-Контроля в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Веб-Контроль**.



Параметры Веб-Контроля

3. В блоке **Шаблоны** настройте шаблоны сообщений Веб-Контроля:

- **Предупреждение**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу.

- **Сообщение о блокировке**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу.

- **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете доступа к веб-странице**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Добавить переменную** и выберите нужную переменную из списка доступных.

Также вы можете восстановить текст шаблона по умолчанию с помощью кнопки **Сбросить**.

4. Сохраните внесенные изменения.

Правила формирования масок адресов веб-ресурсов

Использование *маски адреса веб-ресурса* (далее также "маски адреса") может быть удобно в случаях, когда в процессе создания правила доступа к веб-ресурсам требуется ввести множество схожих адресов веб-ресурсов. Одна грамотно сформированная маска адреса может заменить множество адресов веб-ресурсов.

При формировании маски адреса следует использовать следующие правила:

1. Символ `*` заменяет любую последовательность из нуля или более символов.

   Например, при вводе маски адреса `*abc*` правило доступа к веб-ресурсам применяется ко всем адресам, содержащим последовательность `abc`. Пример: `http://www.example.com/page_0-9abcdef.html`.

2. Последовательность символов `*.` позволяет выбрать все домены адреса – *маска домена*. Маска домена `*.` трактуется как любое имя домена, имя поддомена или пустая строка.

   Пример: под действие маски `*.example.com` попадают следующие адреса:

   - `http://pictures.example.com` – маска домена `*.` применена для `pictures.`.
   - `http://user.pictures.example.com` – маска домена `*.` применена для `pictures.` и `user.`.
   - `http://example.com` – маска домена `*.` трактуется как пустая строка.

3. Последовательность символов `www.` в начале маски адреса трактуется как последовательность `*.`.

   Пример: маска адреса `www.example.com` трактуется как `*.example.com`. Под действие маски попадают адреса `www2.example.com` и `www.pictures.example.com`.

4. Если маска адреса начинается не с символа `*`, то содержание маски адреса эквивалентно тому же содержанию с префиксом `*.`.

5. Если маска адреса заканчивается символом, отличным от `/` или `*`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

   Пример: под действие маски адреса `http://www.example.com` попадают адреса вида `http://www.example.com/abc`, где `a`, `b`, `c` – любые символы.

6. Если маска адреса заканчивается символом `/`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

7. Последовательность символов `/*` в конце маски адреса трактуется как `/*` или пустая строка.

8. Проверка адресов веб-ресурсов по маске адреса осуществляется с учетом схемы (http или https):

   - Если сетевой протокол в маске адреса отсутствует, то под действие маски адреса попадает адрес с любым сетевым протоколом.

     Пример: под действие маски адреса `example.com` попадают адреса `http://example.com` и `https://example.com`.

   - Если сетевой протокол в маске адреса присутствует, то под действие маски адреса попадают только адреса с таким же сетевым протоколом, как у маски адреса.

     Пример: под действие маски адреса `http://*.example.com` попадает адрес `http://www.example.com` и не попадает адрес `https://www.example.com`.

9. Маска адреса, заключенная в двойные кавычки, трактуется без учета каких-либо дополнительных подстановок, за исключением символа `*`, если он изначально включен в состав маски адреса. Для масок адреса, заключенных в двойные кавычки, не выполняются правила 5 и 7 (см. примеры 14 – 18 в таблице ниже).

10. При сравнении с маской адреса веб-ресурса не учитываются имя пользователя и пароль, порт соединения и регистр символов.

Примеры применения правил формирования масок адресов

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
1	*.example.com	http://www.123example.com	Нет	См. правило 1.
2	*.example.com	http://www.123.example.com	Да	См. правило 2.
3	*example.com	http://www.123example.com	Да	См. правило 1.
4	*example.com	http://www.123.example.com	Да	См. правило 1.
5	http://www.*.example.com	http://www.123example.com	Нет	См. правило 1.
6	www.example.com	http://www.example.com	Да	См. правила 3, 2, 1.
7	www.example.com	https://www.example.com	Да	См. правила 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Да	См. правила 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Да	См. правила 3, 5, 1.
10	example.com	http://www.example.com	Да	См. правила 3, 1.
11	http://example.com/	http://example.com/abc	Да	См. правила 6.
12	http://example.com/*	http://example.com	Да	См. правило 7.
13	http://example.com	https://example.com	Нет	См. правило 8.
14	"example.com"	http://www.example.com	Нет	См. правило 9.
15	"http://www.example.com"	http://www.example.com/abc	Нет	См. правило 9.
16	"*.example.com"	http://www.example.com	Да	См. правила 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Да	См. правила 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Да	См. правила 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Нет	Маска адреса содержит больше информации, чем адрес веб-ресурса.

Веб-Контроль для виртуальных машин

Веб-Контроль контролирует трафик не только на компьютере, но и на виртуальной машине, которая развернута на этом компьютере локально. При этом вам не нужно устанавливать приложение Kaspersky Endpoint Security на локальную виртуальную машину. Таким образом, если пользователь пытается открыть веб-сайт, который запрещен правилом Веб-Контроля, в браузере на *виртуальной машине*, приложение, установленное на *компьютере*, заблокирует доступ к этому веб-сайту.

Работа Веб-Контроля на разных виртуальных машинах отличается.

Oracle VM VirtualBox

Kaspersky Endpoint Security поддерживает правила Веб-Контроля на виртуальных машинах Oracle VM VirtualBox без ограничений. Приложение может контролировать весь трафик виртуальной машины. Если в правилах Веб-Контроля настроен фильтр по учетным записям пользователей, приложение работает корректно, так как все процессы виртуальной машины запущены от имени локального пользователя.

VMware Workstation

Kaspersky Endpoint Security поддерживает правила Веб-Контроля на виртуальных машинах VMware Workstation с ограничениями. Приложение не поддерживает правила, в которых настроен фильтр по учетным записям пользователей. Процессы виртуальной машины запущены под системной учетной записью (SYSTEM). Таким образом, идентифицировать пользователя, который пытается открыть веб-сайт на виртуальной машине, невозможно.

Microsoft Hyper-V

Kaspersky Endpoint Security не поддерживает правила Веб-Контроля на виртуальных машинах Microsoft Hyper-V.

Переменные в шаблонах сообщений Веб-Контроля

В шаблонах сообщений пользователю или администратору вы можете использовать следующие переменные:

- **Имя пользователя** – `%USER_NAME%`.

  Имя текущей учетной записи компьютера, на котором появилось сообщение, в формате `<device name>\<user alias>` (например, `DESKTOP-123\John.Smith`).

- **Адрес веб-ресурса** – `%CANONIC_REQUEST_URL%`.

  Адрес заблокированного веб-ресурса.

- **Название правила** – %RULE%.

  Название правила, в соответствии с которым заблокирован веб-ресурс.

- **Адрес для отправки сообщения** – %COMPLAIN_EMAIL%.

  Адрес электронной почты для отправки отзыва о блокировании веб-ресурса. При нажатии на адрес электронной почты приложение открывает окно, в котором пользователь может написать сообщение администратору.

- **Название категории содержания** – %CONTENT_CATEGORY_LIST%.

  Категория веб-сайта, в которую включен заблокированный веб-ресурс (например, *Платежные системы*).

- **Название категории типа данных** – %TYPE_CATEGORY_LIST%.

  Категория типа данных, размещенных на заблокированном веб-ресурсе (например, *Графические файлы*).

- **Ссылка на запрошенный веб-ресурс** – %CONTINUE_PAGE%.

  Ссылка на запрошенную веб-страницу (например, `http://www.example.com/pagename.html`).

- **Ссылка на сайт** – %CONTINUE_SITE%.

  Ссылка на веб-сайт, на котором расположена запрошенная веб-страница (например, `http://www.example.com/`).

- **Ссылка для доступа к доменам** – %CONTINUE_DOMAIN%.

  Ссылка, переход по которой открывает доступ ко всем существующим веб-страницам доменного имени. Например, если адрес заблокированной веб-страницы `http://www.example.com`, то переменная %CONTINUE_DOMAIN% заменяется ссылкой `http://*.example.com`. Переход по этой ссылке открывает доступ ко всем веб-адресам основного доменного имени `http://www.example.com/`, включая его поддомены, например, `http://start.example.com/*` или `http://domain.domain.example.com/*`, где символ * обозначает любую последовательность символов (в том числе пустую).

Контроль устройств

Контроль устройств управляет доступом пользователей к установленным или подключенным к компьютеру устройствам (например, жестким дискам, камере или модулю Wi-Fi). Это позволяет защитить компьютер от заражения при подключении этих устройств и предотвратить потерю или утечку данных.

Если Контроль устройств включен, приложение передает в Kaspersky Security Center информацию о подключенных устройствах. Вы можете просмотреть список подключенных устройств в Kaspersky Security Center в папке **Дополнительно → Хранилища → Оборудование**.

Уровни доступа к устройствам

Контроль устройств управляет доступом на следующих уровнях:

- **Тип устройства**. Например, принтеры, съемные диски, CD/DVD-приводы.

Вы можете настроить доступ устройств следующим образом:

- Разрешать – .
- Запрещать – .
- По правилам (только принтеры и портативные устройства) – .
- Зависит от шины подключения (кроме Wi-Fi) – .
- Запрещать с исключениями (только Wi-Fi) – .

- **Шина подключения**. *Шина подключения* – интерфейс, с помощью которого устройства подключаются к компьютеру (например, USB, FireWire). Если для типа устройств выбран режим **Зависит от шины подключения**, приложение разрешает или запрещает доступ к устройству в зависимости от интерфейса подключения (например, через USB).

  Вы можете настроить доступ устройств следующим образом:

  - Разрешать – .
  - Запрещать – .

- **Доверенные устройства**. *Доверенные устройства* – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

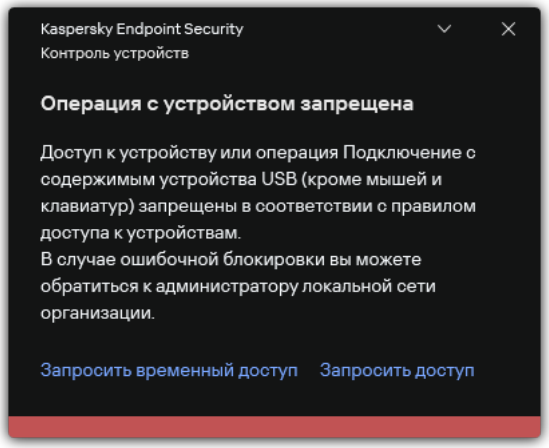
  Вы можете добавить доверенные устройства по следующим данным:

  - **Устройства по идентификатору**. Каждое устройство имеет уникальный идентификатор (англ. Hardware ID, HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы. Пример идентификатора устройства: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств.
  - **Устройства по модели**. Каждое устройство имеет идентификатор производителя (англ. Vendor ID, VID) и идентификатор продукта (англ. Product ID, PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы. Шаблон для ввода VID и PID: `VID_1234&PID_5678`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.
  - **Устройства по маске идентификатора**. Если вы используете несколько устройств с похожими идентификаторами, вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security не поддерживает символ `?` при вводе маски. Например, `WDC_C*`.
  - **Устройства по маске модели**. Если вы используете несколько устройств с похожими VID или PID (например, устройства одного производителя), вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security не поддерживает символ `?` при вводе маски. Например, `VID_05AC&PID_*`.

Контроль устройств регулирует доступ пользователей к устройствам с помощью *правил доступа*. Также Контроль устройств позволяет сохранять события подключения / отключения устройств. Для сохранения событий вам нужно настроить отправку событий в политике.

Если доступ к устройству зависит от шины подключения (статус), Kaspersky Endpoint Security не сохраняет события подключения / отключения устройства. Чтобы приложение Kaspersky Endpoint Security сохраняло события подключения / отключения устройства, разрешите доступ к соответствующему типу устройств (статус) или добавьте устройство в список доверенных.

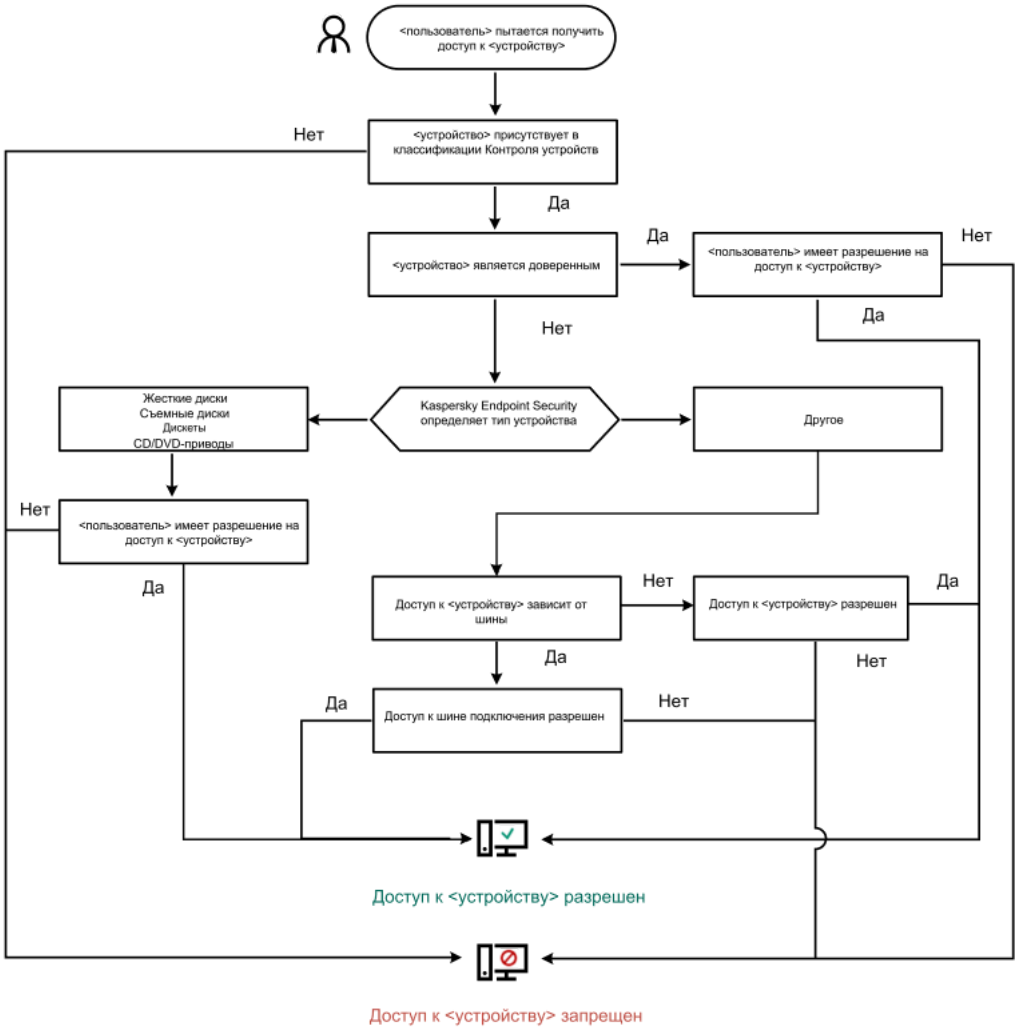
При подключении к компьютеру устройства, доступ к которому запрещен Контролем устройств, Kaspersky Endpoint Security заблокирует доступ и покажет уведомление (см. рис. ниже).



Уведомление Контроля устройств

Алгоритм работы Контроля устройств

Kaspersky Endpoint Security принимает решение о доступе к устройству после того, как пользователь подключил это устройство к компьютеру (см. рис. ниже).



Алгоритм работы Контроля устройств

Если устройство подключено и доступ разрешен, вы можете изменить правило доступа и запретить доступ. В этом случае при очередном обращении к устройству (просмотр дерева папок, чтение, запись) Kaspersky Endpoint Security блокирует доступ. Блокирование устройства без файловой системы произойдет только при последующем подключении устройства.

Если пользователю компьютера с установленным приложением Kaspersky Endpoint Security требуется запросить доступ к устройству, которое, по его мнению, было заблокировано ошибочно, передайте ему инструкцию по запросу доступа.

О правилах доступа

Правило доступа к устройствам – набор параметров, которые определяют доступ пользователей к установленным или подключенным к компьютеру устройствам: доступ к устройству, расписание доступа, разрешение на чтение или запись. Невозможно добавить устройство, которое выходит за рамки классификации Контроля устройств. Доступ к этим устройствам разрешен для всех пользователей.

Правила доступа к устройствам

Набор параметров правила доступа отличается в зависимости от типа устройств (см. таблицу ниже).

Параметры правила доступа

Устройства	Управление доступом	Расписание доступа к устройству	Назначение пользователей / группы пользователей	Приоритет	Разрешение на чтение / запись
Жесткие диски	✓	✓	✓	✓	✓
Съемные диски (включая USB-флешки)	✓	✓	✓	✓	✓
Дискеты	✓	✓	✓	✓	✓
CD/DVD-приводы	✓	✓	✓	✓	✓
Портативные устройства (MTP)	✓	✓	✓	✓	✓
Локальные принтеры	✓	–	✓	✓	–
Сетевые принтеры	✓	–	✓	✓	–
Модемы	✓	–	–	–	–
Стримеры	✓	–	–	–	–
Многофункциональные устройства	✓	–	–	–	–
Устройства чтения смарт-карт	✓	–	–	–	–
Windows CE USB ActiveSync устройства	✓	–	–	–	–
Внешние сетевые адаптеры	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Камеры и сканеры	✓	–	–	–	–

Правило доступа к сетям Wi-Fi

Правило доступа к сетям Wi-Fi определяет разрешение (статус ✓) или запрет (статус ⊘) на использование сетей Wi-Fi. Вы можете добавить в правило *доверенную сеть Wi-Fi* (статус ✓). Использование доверенной сети Wi-Fi разрешено без ограничений. По умолчанию правило доступа к сетям Wi-Fi разрешает доступ к любым сетям Wi-Fi.

Правила доступа к шинам подключения

Если для правила доступа по типу устройств выбрано значение **Зависит от шины подключения**, то приложение разрешает или запрещает доступ к устройству в зависимости интерфейса подключения. Для всех шин подключения из классификации компонента Контроль устройств по умолчанию созданы правила, разрешающие доступ к шинам.

Правила доступа к шинам определяют только разрешение (статус ✓) или запрет (статус ⊘) на подключение устройств. Приоритет правил доступа по типу устройств выше, чем приоритет правил доступа к шине.

Клавиатуры и мыши невозможно заблокировать средствами Контроля устройств. Если вы запретили доступ к шине подключения USB, пользователь продолжит работу с клавиатурой и мышью, подключенными через USB. Для предотвращения подключения к компьютеру зараженных USB-устройств, имитирующих клавиатуры, предназначен компонент Защита от атак BadUSB.

Получение данных об установленных устройствах

Kaspersky Security Center получает данные об установленных устройствах от следующих поставщиков: Агент администрирования и Kaspersky Endpoint Security. Данные об установленных устройствах нужны для управления доступом и формировании списка доверенных устройств.

Данные об аппаратном обеспечении компьютеров

Если Агент администрирования установлен на устройстве с операционной системой Windows, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства:

- оперативная память;
- запоминающие устройства (включая жесткие диски);
- материнская плата;
- процессор;
- сетевой адаптер;
- мониторы;
- видеоадаптер;
- звуковая плата.

Агент администрирования предоставляет эту информацию при каждой синхронизации с Kaspersky Security Center. Вы можете посмотреть аппаратное обеспечение компьютеров в свойствах компьютера (**Реестр оборудования**).

Данные об оборудовании

Kaspersky Endpoint Security предоставляет данные об установленном оборудовании: принтеры, съемные диски, портативные устройства (MTP) и так далее. Для получения данных об оборудовании нужно применить активную политику, в которой включена передача данных об установленных устройствах (по умолчанию передача данных включена).

Как включить передачу данных об установленных устройствах в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Общие настройки** → **Отчеты и хранилище**.
5. В блоке **Передача данных на Сервер администрирования** нажмите на кнопку **Настройка**.
6. Установите флажок **Установленные устройства**.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить передачу данных об установленных устройствах в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Интеграция с KSC**.
5. В блоке **Передача данных на Сервер администрирования** нажмите на кнопку **Дополнительные настройки**.
6. Установите флажок **Об установленных устройствах**.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

В результате вы можете просматривать список установленных устройств в консоли Kaspersky Security Center (**Хранилища** → **Оборудование**).

Контроль доступа к устройствам по типу

Контроль устройств позволяет управлять доступом к устройствам по типу. Тип устройства определяет операционная система при подключении устройства. Вы можете узнать тип устройства с помощью встроенного в операционную систему инструмента Менеджер устройств. Для управления доступом к устройствам вам нужно настроить правила. *Правило доступа к устройствам* – набор параметров, которые определяют доступ пользователей к установленным или подключенным к компьютеру устройствам: доступ к устройству, расписание доступа, разрешение на чтение или запись. Невозможно добавить устройство, которое выходит за рамки классификации Контроля устройств. Доступ к этим устройствам разрешен для всех пользователей.

По умолчанию Контроль устройств разрешает доступ ко всем устройствам для всех пользователей.

Вы можете настроить доступ к устройствам следующим образом:

- **Разрешать**.

  Kaspersky Endpoint Security предоставляет полный доступ к устройствам для всех пользователей.

- **Запрещать**.

  Kaspersky Endpoint Security блокирует подключение устройств. Приложение разрешает подключение только доверенных устройств.

- **Зависит от шины подключения**.

  Kaspersky Endpoint Security определяет интерфейс подключения устройства и ограничивает доступ к устройствам в соответствии со статусом подключения к шине. Также приложение разрешает подключение доверенных устройств.

- **По правилам**.

  Для некоторых типов устройств вы можете выбрать пользователей или группу пользователей, которым будет разрешено использование устройств, задать расписание для доступа к устройствам и настроить разрешения на чтение и запись. Также приложение разрешает подключение доверенных устройств.

Будьте осторожны при настройке доступа к типу устройств **Жесткие диски**. Если вы запретите доступ к системному диску, приложение может вызвать сбой при загрузке операционной системы (BSOD).

Если устройство выходит за рамки классификации Контроля устройств, ограничить доступ к таким устройствам невозможно.

Как контролировать доступ к устройствам по типу в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Контроль безопасности** → **Контроль устройств**.
5. В блоке **Настройки Контроля устройств** выберите вкладку **Типы устройств**.

   На вкладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации Контроля устройств.
6. Настройте правила доступ к устройствам:

   a. Выберите режим доступа: **Разрешать**, **Запрещать**, **Зависит от шины подключения**, **По правилам**.

      Чтобы выбрать режим доступа **По правилам** вам нужно открыть свойства правила доступа двойным щелчком мыши.

   b. Если вы выбрали режим доступа **Зависит от шины подключения**, вам нужно перейти на вкладку **Шины подключения** и настроить правила доступа для интерфейсов подключения.

   c. Для запоминающих устройств (например, съемных дисков) вы можете настроить права доступа для отдельных пользователей. Также вы можете задать расписание для доступа к устройствам и настроить разрешения на чтение и запись.

      Вы можете добавить устройства в список доверенных. *Доверенные устройства* – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

   d. Если требуется, настройте правила печати.

e. Если требуется, настройте правила доступа к Bluetooth-устройствам.

f. Если требуется, настройте правила подключения компьютера к Wi-Fi.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как контролировать доступ к устройствам по типу в Web Console и Cloud Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности** → **Контроль устройств**.

5. В блоке **Правила доступа к устройствам** выберите вкладку **Устройства и сети Wi-Fi**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. Настройте правила доступ к устройствам:

   a. Выберите режим доступа: **Разрешать**, **Запрещать**, **Зависит от шины**, **Пользовательское**.

      Если режим доступа недоступен в раскрывающемся меню, вам нужно открыть свойства правила доступа щелчком мыши по типу устройств.

   b. Если вы выбрали режим доступа **Зависит от шины**, вам нужно перейти на вкладку **Шины подключения** и настроить правила доступа для интерфейсов подключения.

   c. Для запоминающих устройств (например, съемных дисков) вы можете настроить права доступа для отдельных пользователей. Также вы можете задать расписание для доступа к устройствам и настроить разрешения на чтение и запись.

      Вы можете добавить устройства в список доверенных. *Доверенные устройства* – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

   d. Если требуется, настройте правила печати.

   e. Если требуется, настройте правила доступа к Bluetooth-устройствам.

   f. Если требуется, настройте правила подключения компьютера к Wi-Fi.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как контролировать доступ к устройствам в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Контроль безопасности** → **Контроль устройств**.

3. В блоке **Настройка доступа** перейдите по ссылке **Устройства и сети Wi-Fi**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

4. Настройте правила доступ к устройствам:

   a. Выберите режим доступа: **Разрешать**, **Запрещать**, **Зависит от шины подключения**, **По правилам**.

      Если режим доступа недоступен в раскрывающемся меню, вам нужно открыть свойства правила доступа щелчком мыши по типу устройств.

   b. Если вы выбрали режим доступа **Зависит от шины подключения**, вам нужно перейти на вкладку **Шины подключения** и настроить правила доступа для интерфейсов подключения.

   c. Для запоминающих устройств (например, съемных дисков) вы можете настроить права доступа для отдельных пользователей. Также вы можете задать расписание для доступа к устройствам и настроить разрешения на чтение и запись.

      Вы можете добавить устройства в список доверенных. *Доверенные устройства* – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

   d. Если требуется, настройте правила печати.

   e. Если требуется, настройте правила доступа к Bluetooth-устройствам.

   f. Если требуется, настройте правила подключения компьютера к Wi-Fi.

5. Сохраните внесенные изменения.

В результате при попытке пользователя получить доступ к устройству приложение заблокирует доступ в соответствии с правилами. Также Kaspersky Endpoint Security зарегистрирует соответствующее событие. Если вы хотите предоставить доступ к отдельным устройствам, вы можете добавить эти устройства в список доверенных.

Контроль доступа к устройствам по шине подключения

Чтобы изменить правило доступа к шине подключения, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.

3. В блоке **Настройка доступа** нажмите на кнопку **Шины подключения**.

   В открывшемся окне находятся правила доступа для всех шин подключения, которые есть в классификации компонента Контроль устройств.

4. Выберите правило доступа, которое хотите изменить.

5. В графе **Доступ** выберите доступ к шине подключения: **Разрешать** или **Запрещать**.

   Если вы изменили доступ к шине подключения **Последовательный порт** (COM) или **Параллельный порт** (LPT), для активации правила доступа вам нужно перезагрузить компьютер.

6. Сохраните внесенные изменения.

Разграничение прав доступа пользователей к устройствам

Вы можете настроить права доступа пользователей по типу устройств или к доверенным устройствам.

Разграничение прав доступа пользователей по типу устройств

Контроль устройств позволяет настроить права доступа пользователей к данным на *запоминающих устройствах*. Для этих устройств вы можете настроить разрешения на запись и чтение. Контроль устройств поддерживает следующие типы *запоминающих устройств*:

- Жесткие диски.
- Съемные диски (включая USB-флешки).
- Дискеты.
- CD/DVD-приводы.
- Портативные устройства (MTP). К портативным устройствам (MTP) относятся, например, мобильные устройства, фотокамеры, медиаплееры и другие.

Таким образом, вы можете, например, разрешить использование съемных дисков только группе администраторов. Для других типов устройств вы можете или запретить, или разрешить доступ для всех пользователей. Также вы можете настроить права доступа пользователей при работе с принтерами.

Как настроить права доступа пользователей к данным на запоминающих устройствах в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Контроль безопасности** → **Контроль устройств**.
5. В блоке **Настройки Контроля устройств** выберите вкладку **Типы устройств**.

   На вкладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации Контроля устройств.
6. Для настройки правил доступа к запоминающим устройствам откройте список правил двойным щелчком мыши.
7. Настройте правило доступа к запоминающим устройствам:

   a. В блоке **Правила доступа** нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила доступа к запоминающим устройствам.

b. В поле **Приоритет правила** задайте приоритет *записи правила*. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтения / запись) и приоритет.

Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Endpoint Security позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Endpoint Security регулирует доступ по записи запрещающей доступ к устройству.

c. В блоке **Правило для пользователей и групп** выберите пользователей или группы пользователей. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

d. Нажмите на кнопку **OK**.

8. В блоке **Расписания для выбранного правила доступа** настройте расписание доступа к запоминающим устройствам для пользователей.

Например, вы можете разрешить пользователям работать с запоминающими устройствами только в рабочее время.

9. Настройте разрешения пользователей для доступа к запоминающим устройствам в файловом менеджере (**Чтение** / **Запись**).

10. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить права доступа пользователей к данным на запоминающих устройствах в Web Console и Cloud Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности** → **Контроль устройств**.

5. В блоке **Правила доступа к устройствам** в таблице правил доступа откройте свойства правил доступа к запоминающим устройствам.

6. В блоке **Правила доступа к устройствам** выберите вариант **Пользовательское**.

7. Настройте правило доступа к запоминающим устройствам:

a. В блоке **Пользователи и их права** нажмите на кнопку **Добавить**.

Откроется окно добавления нового правила доступа к запоминающим устройствам.

b. В поле **Приоритет** задайте приоритет *записи правила*. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтение / запись) и приоритет.

Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Endpoint Security позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Endpoint Security регулирует доступ по записи запрещающей доступ к устройству.

c. В блоке **Пользователь или группа** выберите пользователей или группы пользователей. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

d. В блоке **Расписание доступа** настройте расписание доступа к запоминающим устройствам для пользователей.

Например, вы можете разрешить пользователям работать с запоминающими устройствами только в рабочее время.

e. Настройте разрешения пользователей для доступа к запоминающим устройствам в файловом менеджере (**Чтение** / **Запись**).

f. Нажмите на кнопку **Сохранить**.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить права доступа пользователей к данным на запоминающих устройствах в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Контроль безопасности → Контроль устройств**.

3. В блоке **Настройка доступа** перейдите по ссылке **Устройства и сети Wi-Fi**.

В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

4. Для настройки правил доступа к запоминающим устройствам откройте список правил щелчком мыши.

5. Настройте правило доступа к запоминающим устройствам:

a. В блоке **Права пользователей** нажмите на кнопку **Добавить**.

Откроется окно добавления нового правила доступа к запоминающим устройствам.

b. В поле **Приоритет** задайте приоритет *записи правила*. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтение / запись) и приоритет.

Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Endpoint Security позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Endpoint Security регулирует доступ по записи запрещающей доступ к устройству.

c. В блоке **Пользователи** выберите пользователей или группы пользователей. Вы можете выбрать пользователей в Active Directory или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

d. Нажмите на кнопку **ОК**.

6. В блоке **Расписания доступа к устройствам** настройте расписание доступа к запоминающим устройствам для пользователей.

   Например, вы можете разрешить пользователям работать с запоминающими устройствами только в рабочее время.

7. Настройте разрешения пользователей для доступа к запоминающим устройствам в файловом менеджере (**Чтение** / **Запись**).

8. Сохраните внесенные изменения.

Разграничение прав доступа пользователей к доверенным устройствам

Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства. Для работы с доверенными устройствами вы можете предоставить доступ отдельному пользователю, группе пользователей или всем пользователям организации. Вы можете настроить права доступа пользователей в свойствах доверенного устройства.

Контроль доступа к мобильным устройствам

Kaspersky Endpoint Security позволяет управлять доступом к данным на мобильных устройствах под управлением Android и iOS. Мобильные устройства относятся к портативным устройствам (MTP). Поэтому, чтобы настроить доступ к данным на мобильных устройствах вам нужно перейти в настройки доступа к портативным устройствам (MTP).

При подключении мобильного устройства к компьютеру операционная система определяет тип устройства. Если на компьютере установлены приложения Android Debug Bridge (ADB), iTunes или их аналоги, операционная система определяет мобильные устройства как ADB- или iTunes-устройства. В остальных случаях операционная система может определить тип мобильного устройства как портативное устройство (MTP) для передачи файлов, PTP-устройство (камера) для передачи изображений или другое устройство. Тип устройства зависит от модели мобильного устройства и выбранного режима подключения по USB. Kaspersky Endpoint Security позволяет настроить отдельные права доступа к данным на мобильных устройствах в приложениях ADB, iTunes или файловом менеджере. В остальных случаях Контроль устройств предоставляет доступ к мобильным устройствам согласно правилам доступа к портативным устройствам (MTP).

Доступ к мобильным устройствам

Так как мобильные устройства относятся к портативным устройствам (MTP), настройки доступа у этих устройств общие. Вы можете выбрать один из следующих режимов доступа к мобильным устройствам:

- **Разрешать**. Kaspersky Endpoint Security предоставляет полный доступ к мобильным устройствам. Вы можете открывать, создавать, изменять, копировать или удалять файлы на мобильных устройствах с помощью файлового менеджера или приложений ADB и iTunes. Также вы можете заряжать батарею устройства, подключив мобильное устройств через USB к компьютеру.

- **Запрещать**. Kaspersky Endpoint Security ограничивает доступ к мобильным устройствам в файловом менеджере и приложениях ADB и iTunes. Приложение разрешает доступ только к доверенным мобильным устройствам. Также вы можете заряжать батарею устройства, подключив мобильное устройство через USB к компьютеру.

- **Зависит от шины подключения**. Kaspersky Endpoint Security ограничивает доступ к мобильным устройствам в соответствии со статусом подключения к шине USB (**Разрешать** или **Запрещать**).

- **По правилам**. Kaspersky Endpoint Security ограничивает доступ к мобильным устройствам в соответствии с правилами. В правилах вы можете настроить права доступа (чтение / запись), выбрать пользователей или группу пользователей, которые имеют доступ к мобильным устройствам и задать расписание доступа к мобильным устройствам. Также вы можете ограничить доступ к данным на мобильных устройствах через приложения ADB и iTunes.

Настройка правил доступа к мобильным устройствам

Настройка правил доступа для портативных устройств (MTP), ADB- и iTunes-устройств отличается. Для портативных устройств (MTP) и ADB-устройств вы можете назначать правила для отдельных пользователей или групп пользователей и составлять расписание работы правил. Для iTunes-устройств таких возможностей нет. Вы можете только разрешить или запретить доступ к данным через приложение iTunes для всех пользователей.

Как настроить правила доступа к мобильным устройствам в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Контроль устройств**.
4. В блоке **Настройки Контроля устройств** выберите вкладку **Типы устройств**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.
5. В контекстном меню для типа устройств **Портативные устройства (MTP)** настройте режим доступа к мобильным устройствам: **Разрешать**, **Запрещать** или **Зависит от шины подключения**.
6. Для настройки правил доступа к мобильным устройствам откройте список правил двойным щелчком мыши.

7. Настройте правило доступа к мобильным устройствам:

   a. В блоке **Правила доступа** нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила доступа к мобильным устройствам.

   b. В поле **Приоритет** задайте приоритет записи правила. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтения / запись / доступ через ADB) и приоритет.

      Запись правила имеет приоритет. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Endpoint Security позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

      Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Endpoint Security регулирует доступ по записи, запрещающей доступ к устройству.

   c. В блоке **Правило для пользователей и групп** выберите пользователей или группы пользователей. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   d. Нажмите на кнопку **ОК**.

8. В блоке **Расписания для выбранного правила доступа** настройте расписание доступа к мобильным устройствам для пользователей.

   Настроить отдельное расписание доступа к ADB-устройствам невозможно. Вы можете настроить общее расписание для ADB-устройств и портативных устройств (MTP).

9. Настройте разрешения пользователей для доступа к мобильным устройствам в файловом менеджере (**Чтение** / **Запись**).

10. Настройте доступ к данным мобильного устройства через приложение ADB с помощью флажка **Доступ через ADB**.

    Если флажок снят, при подключении мобильного устройства приложение ADB не сможет обнаружить устройство.

11. В блоке **Доступ через iTunes** настройте доступ к данным мобильного устройства через приложение iTunes.

    Kaspersky Endpoint Security применяет настройки доступа к мобильным устройствам через приложение iTunes для всех пользователей. Настроить отдельное расписание доступа к iTunes-устройствам невозможно.

12. Сохраните внесенные изменения.

Как настроить правила доступа к мобильным устройствам в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль устройств**.
5. В блоке **Правила доступа к устройствам** перейдите по ссылке **Устройства и сети Wi-Fi**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.
6. Выберите тип устройств **Портативные устройства (MTP)**.

   Откроются правила доступа к портативным устройствам (MTP).
7. Настройте режим доступа к мобильным устройствам: **Разрешать**, **Запрещать**, **Зависит от шины** или **Пользовательское**.
8. С помощью переключателя **Доступ через iTunes для всех пользователей ВКЛЮЧЕН** настройте доступ к данным мобильного устройства через приложение iTunes.

   > Kaspersky Endpoint Security применяет настройки доступа к мобильным устройствам через приложение iTunes для всех пользователей. Настроить отдельное расписание доступа к iTunes-устройствам невозможно.

9. Если вы выбрали режим **Пользовательское**, вам нужно добавить правила доступа к устройствам. Для этого в блоке **Пользователи и их права** нажмите на кнопку **Добавить** и настройте правило доступа к мобильным устройствам:

   a. В поле **Приоритет** задайте приоритет записи правила. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтения / запись / доступ через ADB) и приоритет.

      Запись правила имеет приоритет. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Endpoint Security позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

      Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Endpoint Security регулирует доступ по записи, запрещающей доступ к устройству.

   b. В блоке **Пользователь или группа** выберите пользователей или группы пользователей для доступа к мобильным устройствам. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

c. В блоке **Расписание доступа** настройте расписание доступа к мобильным устройствам для пользователей.

> Настроить отдельное расписание доступа к ADB-устройствам невозможно. Вы можете настроить общее расписание для ADB-устройств и портативных устройств (MTP).

d. Настройте разрешения пользователей для доступа к мобильным устройствам в файловом менеджере (**Чтение** / **Запись**).

e. Настройте доступ к данным мобильного устройства через приложение ADB с помощью флажка **Доступ через ADB**.

Если флажок снят, при подключении мобильного устройства приложение ADB не сможет обнаружить устройство.

10. Сохраните внесенные изменения.

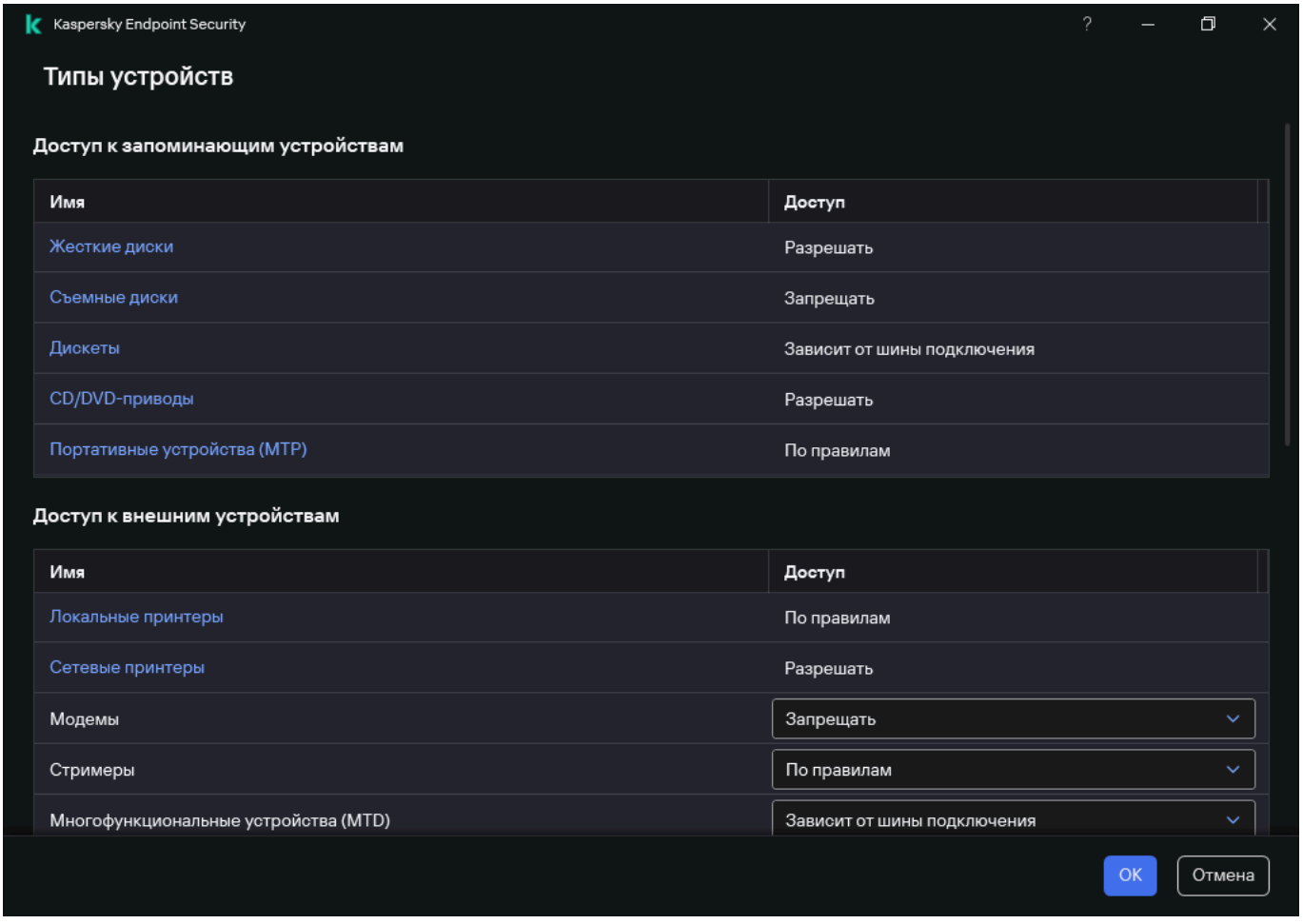
Как настроить правила доступа к мобильным устройствам в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.

3. В блоке **Настройка доступа** нажмите на кнопку **Устройства и сети Wi-Fi**.

В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.



Типы устройств Контроля устройств

4. В блоке **Доступ к запоминающим устройствам** перейдите по ссылке **Портативные устройства (MTP)**.

   В открывшемся окне находятся правила доступа к портативным устройствам (MTP).

5. В блоке **Доступ** настройте режим доступа к мобильным устройствам: **Разрешать**, **Запрещать**, **Зависит от шины подключения** или **По правилам**.

6. Если вы выбрали режим **По правилам**, вам нужно добавить правила доступа к устройствам:

   a. В блоке **Права пользователей** нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила доступа к мобильным устройствам.

   b. В поле **Приоритет** задайте приоритет записи правила. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтения / запись / доступ через ADB) и приоритет.

      Запись правила имеет приоритет. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Endpoint Security позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

      Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Endpoint Security регулирует доступ по записи, запрещающей доступ к устройству.

   c. В блоке **Состояние** включите правило доступа к мобильным устройствам.

   d. В блоке **Права доступа** настройте разрешения пользователей для доступа к мобильным устройствам.

      - Настройте разрешения пользователей для доступа к мобильным устройствам в файловом менеджере (**Чтение** / **Запись**).

      - Настройте доступ к данным мобильного устройства через приложение ADB с помощью флажка **Доступ через ADB**.

        Если флажок снят, при подключении мобильного устройства приложение ADB не сможет обнаружить устройство.

   e. В блоке **Пользователи** выберите пользователей или группы пользователей для доступа к мобильным устройствам. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   f. В блоке **Расписание доступа к устройствам** настройте расписание доступа к устройствам для пользователей.

      Настроить отдельное расписание доступа к ADB-устройствам невозможно. Вы можете настроить общее расписание для ADB-устройств и портативных устройств (MTP).

g. В блоке **Доступ через iTunes** настройте доступ к данным мобильного устройства через приложение iTunes.

> Kaspersky Endpoint Security применяет настройки доступа к мобильным устройствам через приложение iTunes для всех пользователей. Настроить отдельное расписание доступа к iTunes-устройствам невозможно.

7. Сохраните внесенные изменения.

В результате пользователям будет ограничен доступ к мобильным устройствам согласно правилам. Если вы запретили доступ к мобильным устройствам в приложениях ADB и iTunes, при подключении мобильного устройства приложения ADB и iTunes не смогут обнаружить мобильное устройство.

Доверенные мобильные устройства

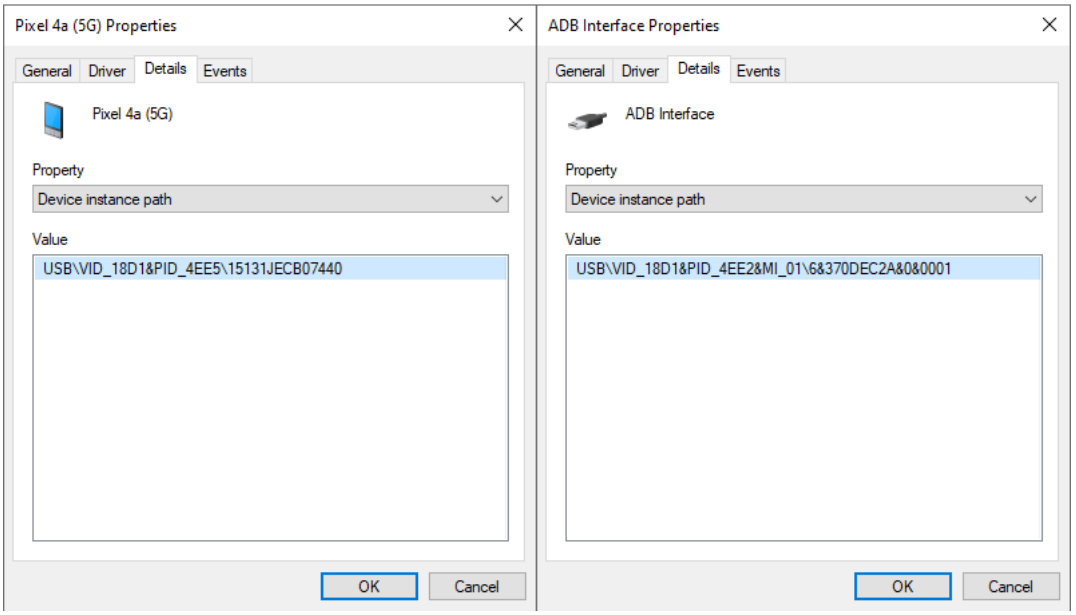
Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Добавление доверенного мобильного устройства ничем не отличается от добавления других типов доверенных устройств. Вы можете добавить мобильное устройство по идентификатору или модели устройства.

Для добавления доверенного мобильного устройства по идентификатору, вам понадобится уникальный идентификатор (англ. Hardware ID, HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы (см. рис. ниже). Для этого предназначен инструмент Диспетчер устройств (англ. Device Manager). Идентификаторы для портативных устройств (MTP) и ADB-, iTunes-устройств отличаются, даже если это одно мобильное устройство. Пример идентификатора портативного устройства (MTP): `15131JECB07440`. Пример идентификатора ADB-устройства: `6&370DEC2A&0&0001`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств. Также вы можете использовать маски.

> Если вы установили приложение ADB или iTunes после подключения устройства к компьютеру, уникальный идентификатор устройства может быть сброшен. То есть, Kaspersky Endpoint Security определит это устройство как новое. Если устройство доверенное, добавьте устройство в список доверенных повторно.

Для добавления доверенного мобильного устройства по модели, вам понадобятся идентификатор производителя (англ. Vendor ID, VID) и идентификатор продукта (англ. Product ID, PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы (см. рис. ниже). Шаблон для ввода VID и PID: `VID_18D1&PID_4EE5`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.



Идентификатор устройства в Диспетчере устройств

Контроль доступа к Bluetooth-устройствам

Kaspersky Endpoint Security позволяет управлять доступом к устройствам, подключенным по Bluetooth. К Bluetooth-устройствам относятся беспроводные клавиатуры, мыши, гарнитуры, принтеры и т.д. Также вы можете использовать Bluetooth для обмена данными, например, с мобильным устройством.

При подключении или отключении Bluetooth-устройств приложение может создавать несколько событий о действиях с устройством. Это связано с тем, что операционная система может определять Bluetooth-устройство как несколько устройств разных типов. Также Kaspersky Endpoint Security контролирует Bluetooth-адаптер, через который подключено устройство, как отдельное устройство. Поэтому приложение создает событие для всех обнаруженных устройств.

Вы можете выбрать один из следующих режимов доступа к Bluetooth-устройствам:

- **Разрешать и не записывать в отчет** . Kaspersky Endpoint Security позволяет подключать любые Bluetooth-устройства и не сохраняет информацию о подключении в журнал событий. Вы можете подключать устройства ввода по Bluetooth (клавиатуры, мыши и т.п.), передавать данные по Bluetooth, управлять другими устройствами по Bluetooth (гарнитура, наушники и т.п.).

- **Разрешать** . Kaspersky Endpoint Security позволяет подключать любые Bluetooth-устройства. Вы можете подключать устройства ввода по Bluetooth (клавиатуры, мыши и т.п.), передавать данные по Bluetooth, управлять другими устройствами по Bluetooth (гарнитура, наушники и т.п.).

- **Запрещать** . Kaspersky Endpoint Security ограничивает доступ к Bluetooth-устройствам. Вы можете разрешить подключение только устройств ввода по Bluetooth (класс HID-устройств – Human Interface Devices). К этим устройствам относятся клавиатуры, мыши, джойстики и т.п.

Сформировать список доверенных Bluetooth-устройств невозможно. Если вы ограничили доступ к Bluetooth-устройствам, вы можете разрешить подключение только устройств ввода по Bluetooth.

Как настроить правила доступа к Bluetooth-устройствам в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите папку **Политики**.

3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

4. В окне политики выберите **Контроль безопасности** → **Контроль устройств**.

5. В блоке **Настройки Контроля устройств** выберите вкладку **Типы устройств**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. В контекстном меню для типа устройств **Bluetooth** настройте режим доступа к Bluetooth-устройствам: **Разрешать** , **Запрещать** , **Разрешать и не записывать в отчет** .

7. Если вы выбрали режим **Запрещать**, вы можете разрешить подключение только устройств ввода по Bluetooth (клавиатуры, мыши и т.п.). Для этого в блоке **Исключения** установите флажок **Устройства ввода (мыши и клавиатуры)**.

8. Для применения политики на компьютерах закройте замки , сохраните внесенные изменения.

Как настроить правила доступа к Bluetooth-устройствам в Web Console и Cloud Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности** → **Контроль устройств**.

5. В блоке **Правила доступа к устройствам** перейдите по ссылке **Устройства и сети Wi-Fi**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. Выберите тип устройств **Bluetooth-устройства**.

   Откроются настройки доступа к Bluetooth-устройствам.

7. Настройте режим доступа к Bluetooth-устройствам: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет**.

8. Если вы выбрали режим **Запрещать**, вы можете разрешить подключение только устройств ввода по Bluetooth (клавиатуры, мыши и т.п.). Для этого в блоке **Исключения** установите флажок **Устройства ввода (мыши и клавиатуры)**.

9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

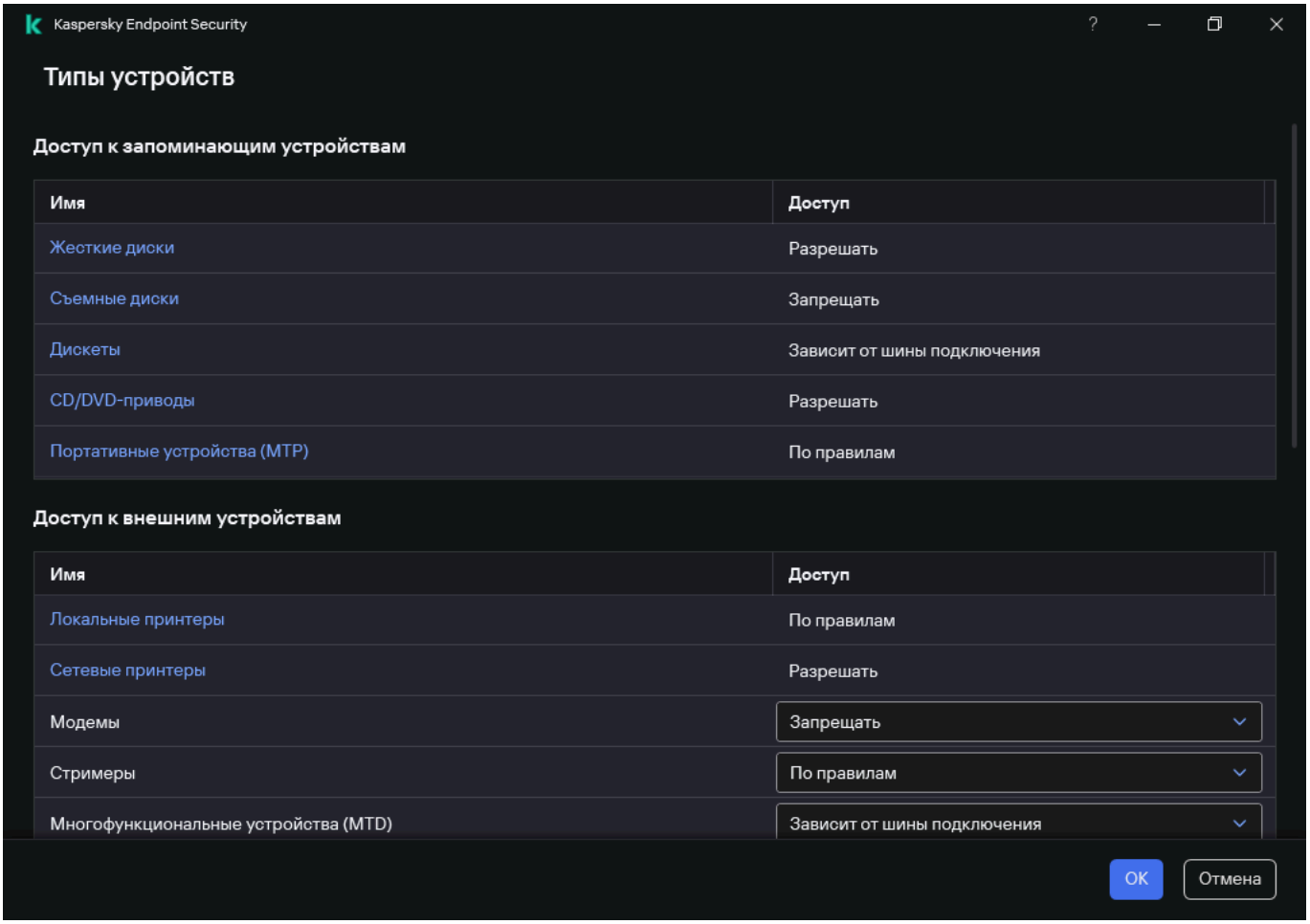
Как настроить правила доступа к Bluetooth-устройствам в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.

3. В блоке **Настройка доступа** нажмите на кнопку **Устройства и сети Wi-Fi**.

   В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.



Типы устройств Контроля устройств

4. В блоке **Доступ к внешним устройствам** перейдите по ссылке **Bluetooth**.

   Откроются настройки доступа к Bluetooth-устройствам.

5. В блоке **Доступ** настройте режим доступа к Bluetooth-устройствам: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет**.

6. Если вы выбрали режим **Запрещать**, вы можете разрешить подключение только устройств ввода по Bluetooth (клавиатуры, мыши и т.п.). Для этого в блоке **Исключения** установите флажок **Устройства ввода (мыши и клавиатуры)**.

7. Сохраните внесенные изменения.

Контроль печати

Контроль печати не поддерживается на компьютерах с Arm-архитектурой.

С помощью Контроля печати вы можете настроить доступ пользователей к локальным и сетевым принтерам.

Контроль локальных принтеров

Kaspersky Endpoint Security позволяет настроить доступ к локальным принтерам на двух уровнях: *подключение* и *печать*.

Kaspersky Endpoint Security управляет подключением локальных принтеров по следующим шинам: USB, Последовательный порт (COM), Параллельный порт (LPT).

Kaspersky Endpoint Security контролирует подключение локальных принтеров через COM и LPT только на уровне шины. То есть, чтобы запретить подключение принтеров через COM и LPT вам нужно выбрать режим доступа к локальным принтерам Зависит от шины подключения и запретить подключение к шинам COM и LPT.

Принтеры, подключенные через USB, приложение контролирует на двух уровнях: тип устройств (локальные принтеры) и шина подключения (USB).

Вы можете выбрать один следующих режимов доступа к локальным принтерам через USB:

- **Разрешать** ✓. Kaspersky Endpoint Security предоставляет полный доступ к локальным принтерам для всех пользователей. Пользователи могут подключать принтеры и печатать документы средствами операционной системы.
- **Запрещать** ⊘. Kaspersky Endpoint Security блокирует подключение локальных принтеров. Приложение разрешает подключить только доверенные принтеры.

- **Зависит от шины подключения**. Kaspersky Endpoint Security ограничивает доступ к локальным принтерам в соответствии со статусом подключения к шине USB (**Разрешать** или **Запрещать**).

- **По правилам**. Для контроля печати вам нужно добавить *правила печати*. В правилах вы можете выбрать пользователей или группу пользователей, которым будет разрешено или запрещено печатать документы на локальных принтерах.

Контроль сетевых принтеров

Kaspersky Endpoint Security позволяет настроить доступ к печати на сетевых принтерах. Вы можете выбрать один следующих режимов доступа к сетевым принтерам:

- **Разрешать и не записывать в отчет**. Kaspersky Endpoint Security не контролирует печать на сетевых принтерах. Приложение предоставляет доступ к печати на сетевых принтерах для всех пользователей и не сохраняет информацию о печати в журнал событий.

- **Разрешать**. Kaspersky Endpoint Security предоставляет доступ к печати на сетевых принтерах для всех пользователей.

- **Запрещать**. Kaspersky Endpoint Security ограничивает доступ к печати на сетевых принтерах для всех пользователей. Приложение разрешает доступ только к доверенным принтерам.

- **По правилам**. Kaspersky Endpoint Security предоставляет доступ к печати для в соответствии с правилами печати. В правилах вы можете выбрать пользователей или группу пользователей, которым будет разрешено или запрещено печатать документы на сетевых принтерах.

Добавление правил печати для принтеров

Как добавить правила печати в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Контроль безопасности** → **Контроль устройств**.

4. В блоке **Настройки Контроля устройств** выберите вкладку **Типы устройств**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

5. В контекстном меню для типов устройств **Локальные принтеры** и **Сетевые принтеры** настройте режим доступа к соответствующим принтерам: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет** (только для сетевых принтеров) или **Зависит от шины подключения** (только для локальных принтеров).

6. Для настройки правил печати на локальных и сетевых принтерах откройте списки правил двойным щелчком мыши.

7. Выберите режим доступа к принтерам **По правилам**.

8. Выберите пользователей или группы пользователей, к которым вы хотите применить правило печати:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила печати.

   b. Назначьте приоритет записи правила. Запись правила включает в себя следующие атрибуты: учетная запись, действие (разрешено / запрещено) и приоритет.

      Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Endpoint Security позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

      Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Endpoint Security регулирует доступ по записи запрещающей доступ к устройству.

   c. В блоке **Действие** настройте доступ пользователя к печати на принтере.

   d. Нажмите на кнопку **Пользователи и группы** и выберите пользователей или группы пользователей для доступа к печати. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   e. Нажмите на кнопку **OK**.

9. Сохраните внесенные изменения.

Как добавить правила печати в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности** → **Контроль устройств**.

5. В блоке **Правила доступа к устройствам** перейдите по ссылке **Устройства и сети Wi-Fi**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. Выберите тип устройств **Локальные принтеры** или **Сетевые принтеры**.

   Откроются правила доступа к принтерам.

7. Настройте режим доступа к соответствующим принтерам: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет** (только для сетевых принтеров), **Зависит от шины** (только для локальных принтеров) или **Пользовательское**.

8. Если вы выбрали режим **Пользовательское**, вам нужно добавить правила печати для локальных или сетевых принтеров. Для этого в таблице правил печати нажмите на кнопку **Добавить**.

   Откроются параметры нового правила печати.

9. Назначьте приоритет записи правила. Запись правила включает в себя следующие атрибуты: учетная запись, действие (разрешено / запрещено) и приоритет.

   Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Endpoint Security позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

   Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

   Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Endpoint Security регулирует доступ по записи запрещающей доступ к устройству.

10. В блоке **Действие** настройте доступ пользователя к печати на принтере.

11. В блоке **Пользователь или группа** выберите пользователей или группы пользователей для доступа к печати. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

12. Сохраните внесенные изменения.

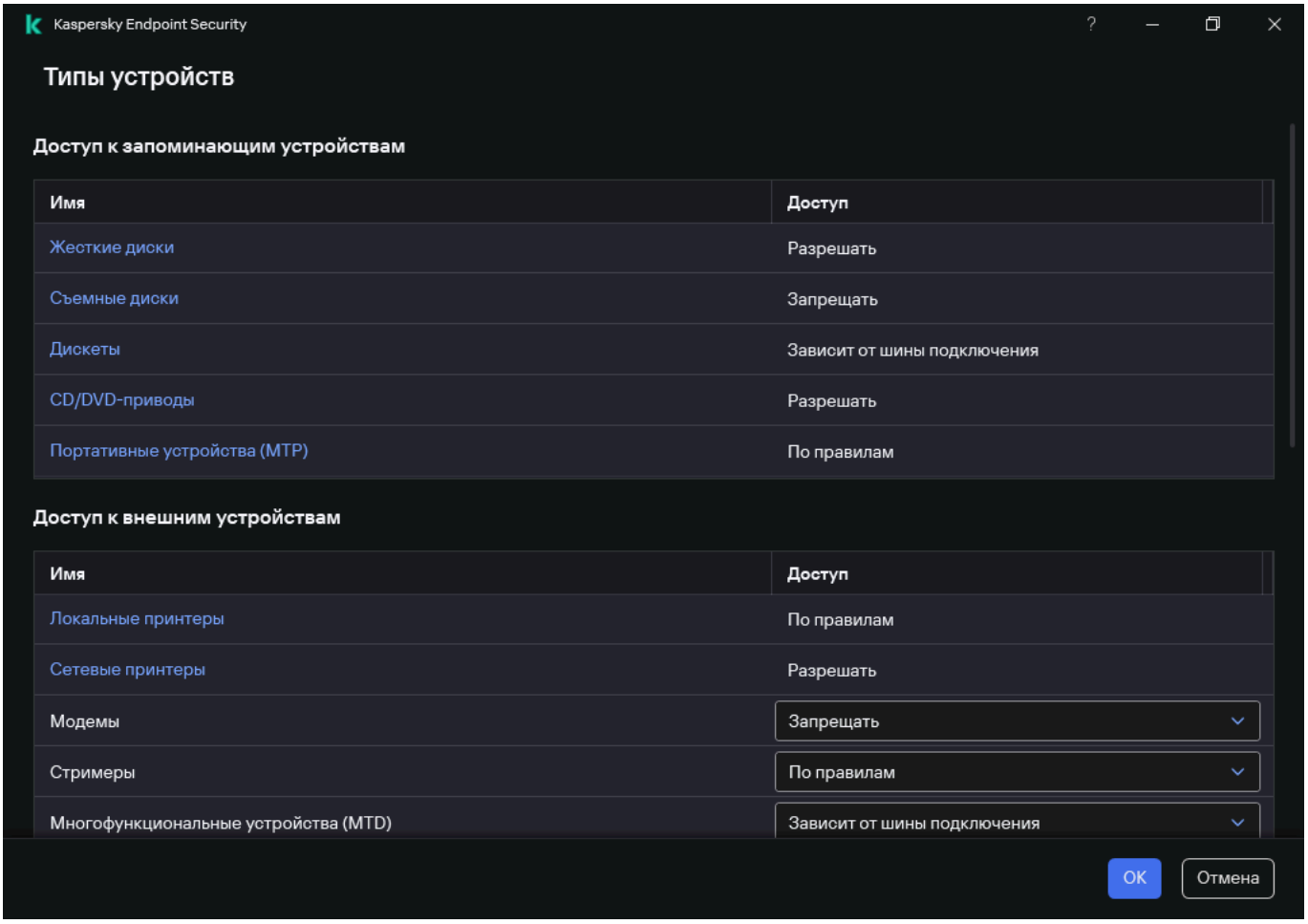
Как добавить правила печати в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.

3. В блоке **Настройка доступа** нажмите на кнопку **Устройства и сети Wi-Fi**.

В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.



Типы устройств Контроля устройств

4. В блоке **Доступ к внешним устройствам** перейдите по ссылке **Локальные принтеры** или **Сетевые принтеры**.

   В открывшемся окне находятся правила доступа к принтерам.

5. В блоке **Доступ к локальным принтерам** или **Доступ к сетевым принтерам** настройте режим доступа к принтерам: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет** (только для сетевых принтеров), **Зависит от шины подключения** (только для локальных принтеров) или **По правилам**.

6. Если вы выбрали режим **По правилам**, вам нужно добавить правила печати для принтеров. Выберите пользователей или группы пользователей, к которым вы хотите применить правило печати:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила печати.

   b. Назначьте приоритет записи правила. Запись правила включает в себя следующие атрибуты: учетная запись, разрешения (разрешено / запрещено) и приоритет.

      Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Endpoint Security позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Endpoint Security регулирует доступ по записи, запрещающей доступ к устройству.

c. В блоке **Действие** настройте разрешения пользователей для доступа печати.

d. В блоке **Пользователи и группы** выберите пользователей или группы пользователей для доступа к печати. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

7. Сохраните внесенные изменения.

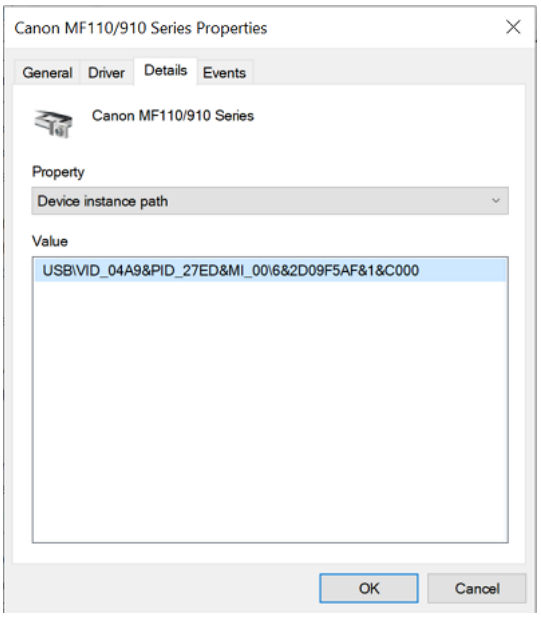
Доверенные принтеры

Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Добавление доверенных принтеров ничем не отличается от добавления других типов доверенных устройств. Локальные принтеры вы можете добавить по идентификатору или модели устройства. Сетевые принтеры вы можете добавить только по идентификатору устройства.

Для добавления доверенного локального принтера по идентификатору, вам понадобится уникальный идентификатор (англ. Hardware ID, HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы (см. рис. ниже). Для этого предназначен инструмент Диспетчер устройств (англ. Device Manager). Пример идентификатора локального принтера: `6&2D09F5AF&1&C000`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств. Также вы можете использовать маски.

Для добавления доверенного локального принтера по модели, вам понадобятся идентификатор производителя (англ. Vendor ID, VID) и идентификатор продукта (англ. Product ID, PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы (см. рис. ниже). Шаблон для ввода VID и PID: `VID_04A9&PID_27FD`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.



Идентификатор устройств в Диспетчере устройств

Для добавления доверенного сетевого принтера, вам понадобится идентификатор устройства. Для сетевых принтеров идентификатором может быть сетевое имя принтера (имя общего принтера), IP-адрес принтера или URL-адрес принтера.

Контроль подключения к Wi-Fi

Контроль устройств позволяет управлять подключением компьютера (ноутбука) к сетям Wi-Fi. Публичные сети Wi-Fi могут быть не защищены, и использование таких сетей может привести к потере данных. С помощью Контроля устройств вы можете запретить пользователю подключение к Wi-Fi или разрешить подключение только к доверенным сетям. Например, вы можете разрешить подключение только к корпоративной сети Wi-Fi, которая достаточно защищена. Контроль устройств будет блокировать доступ ко всем сетям Wi-Fi, кроме тех, которые указаны в списке доверенных.

На компьютерах под управлением Windows 11 для контроля подключения к Wi-Fi нужно включить службы определения местоположения. Для этого вам нужно включить переключатель **Службы определения местоположения** в параметрах операционной системы (**Настройки** → **Конфиденциальность и защита** → **Расположение**). Если службы определения местоположения выключены, Kaspersky Endpoint Security не контролирует подключение к сетям Wi-Fi.

Как ограничить подключения к Wi-Fi в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Контроль устройств**.

4. В блоке **Настройки Контроля устройств** выберите вкладку **Типы устройств**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

5. В контекстном меню для типа устройств **Wi-Fi** выберите действие Контроля устройств при подключения к Wi-Fi: **Разрешать** (), **Запрещать** () или **Запрещать с исключениями** ().

6. Если вы выбрали вариант **Запрещать с исключениями**, сформируйте список доверенных сетей Wi-Fi:

   a. Откройте список доверенных сетей Wi-Fi двойным щелчком мыши.

   b. В блоке **Доверенные сети Wi-Fi** нажмите на кнопку **Добавить**.

   c. В открывшемся окне задайте параметры доверенной сети Wi-Fi (см. рис. ниже):

   - **Имя сети**. Имя сети Wi-Fi или SSID (Service Set Identifier).
   - **Тип аутентификации**. Тип аутентификации при подключении к сети Wi-Fi.

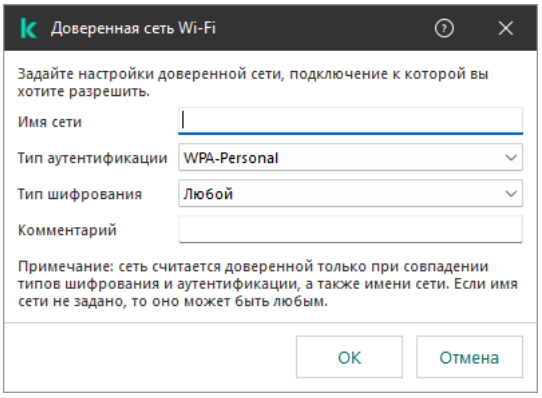
     Начиная с версии Kaspersky Endpoint Security для Windows 12.0 в приложение добавлена поддержка протокола WPA3. Если на компьютере применена политика Kaspersky Endpoint Security версии 12.2, на компьютерах с установленным приложением Kaspersky Endpoint Security версии 11.11.0 и более ранних версий будет выбран протокол WPA2, для версий 12.0 – 12.1 будет выбран протокол WPA2 / WPA3, для версии 12.2 и выше – WPA3.

   - **Тип шифрования**. Тип шифрования, используемый для защиты трафика сети Wi-Fi.
   - **Комментарий**. Дополнительная информация о добавленной сети Wi-Fi.

   Вы можете посмотреть параметры доверенной сети Wi-Fi в параметрах роутера.

   Сеть Wi-Fi считается доверенной, если ее параметры соответствуют всем параметрам, указанным в правиле.

7. Сохраните внесенные изменения.



Параметры доверенной сети Wi-Fi

Как ограничить подключение к Wi-Fi в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль устройств**.
5. В блоке **Правила доступа к устройствам** выберите вкладку **Устройства и сети Wi-Fi**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.
6. В блоке **Сети Wi-Fi** перейдите по ссылке **Wi-Fi**.
7. В открывшемся окне выберите действие Контроля устройств при подключения к Wi-Fi: **Разрешать**, **Запрещать** или **Запрещать с исключениями**.
8. Если вы выбрали вариант **Запрещать с исключениями**, сформируйте список доверенных сетей Wi-Fi:

   a. Откройте список доверенных сетей Wi-Fi двойным щелчком мыши.

   b. В блоке **Доверенные сети Wi-Fi** нажмите на кнопку **Добавить**.

   c. В открывшемся окне задайте параметры доверенной сети Wi-Fi (см. рис. ниже):

   - **Имя**. Имя сети Wi-Fi или SSID (Service Set Identifier).
   - **Тип аутентификации**. Тип аутентификации при подключении к сети Wi-Fi.

     Начиная с версии Kaspersky Endpoint Security для Windows 12.0 в приложение добавлена поддержка протокола WPA3. Если на компьютере применена политика Kaspersky Endpoint Security версии 12.2, на компьютерах с установленным приложением Kaspersky Endpoint Security версии 11.11.0 и более ранних версий будет выбран протокол WPA2, для версий 12.0 – 12.1 будет выбран протокол WPA2 / WPA3, для версии 12.2 и выше – WPA3.
   - **Тип шифрования**. Тип шифрования, используемый для защиты трафика сети Wi-Fi.
   - **Комментарий**. Дополнительная информация о добавленной сети Wi-Fi.

   Вы можете посмотреть параметры доверенной сети Wi-Fi в параметрах роутера.

   Сеть Wi-Fi считается доверенной, если ее параметры соответствуют всем параметрам, указанным в правиле.
9. Сохраните внесенные изменения.

Как ограничить подключение к Wi-Fi в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

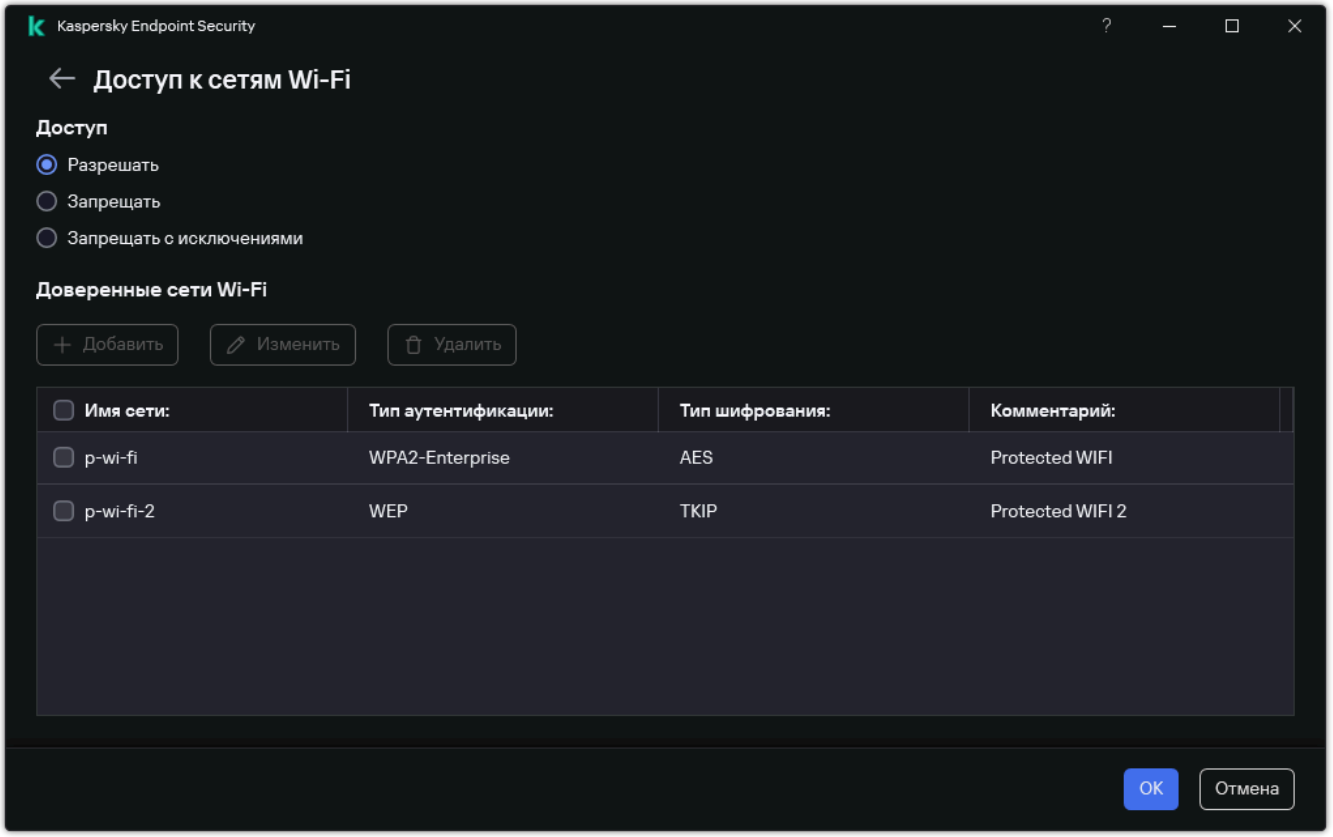
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.

3. В блоке **Настройка доступа** нажмите на кнопку **Устройства и сети Wi-Fi**.

   В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

4. В блоке **Доступ к сетям Wi-Fi** перейдите по ссылке **Wi-Fi**.

   В открывшемся окне находятся правила доступа к сетям Wi-Fi.



Настройки доступа к Wi-Fi

5. В блоке **Доступ** выберите действие Контроля устройств при подключения к Wi-Fi: **Разрешать**, **Запрещать** или **Запрещать с исключениями**.

6. Если вы выбрали вариант **Запрещать с исключениями**, сформируйте список доверенных сетей Wi-Fi:

   a. В блоке **Доверенные сети Wi-Fi** нажмите на кнопку **Добавить**.

   b. В открывшемся окне задайте параметры доверенной сети Wi-Fi (см. рис. ниже):

   - **Имя сети**. Имя сети Wi-Fi или SSID (Service Set Identifier).
   - **Тип аутентификации**. Тип аутентификации при подключении к сети Wi-Fi.

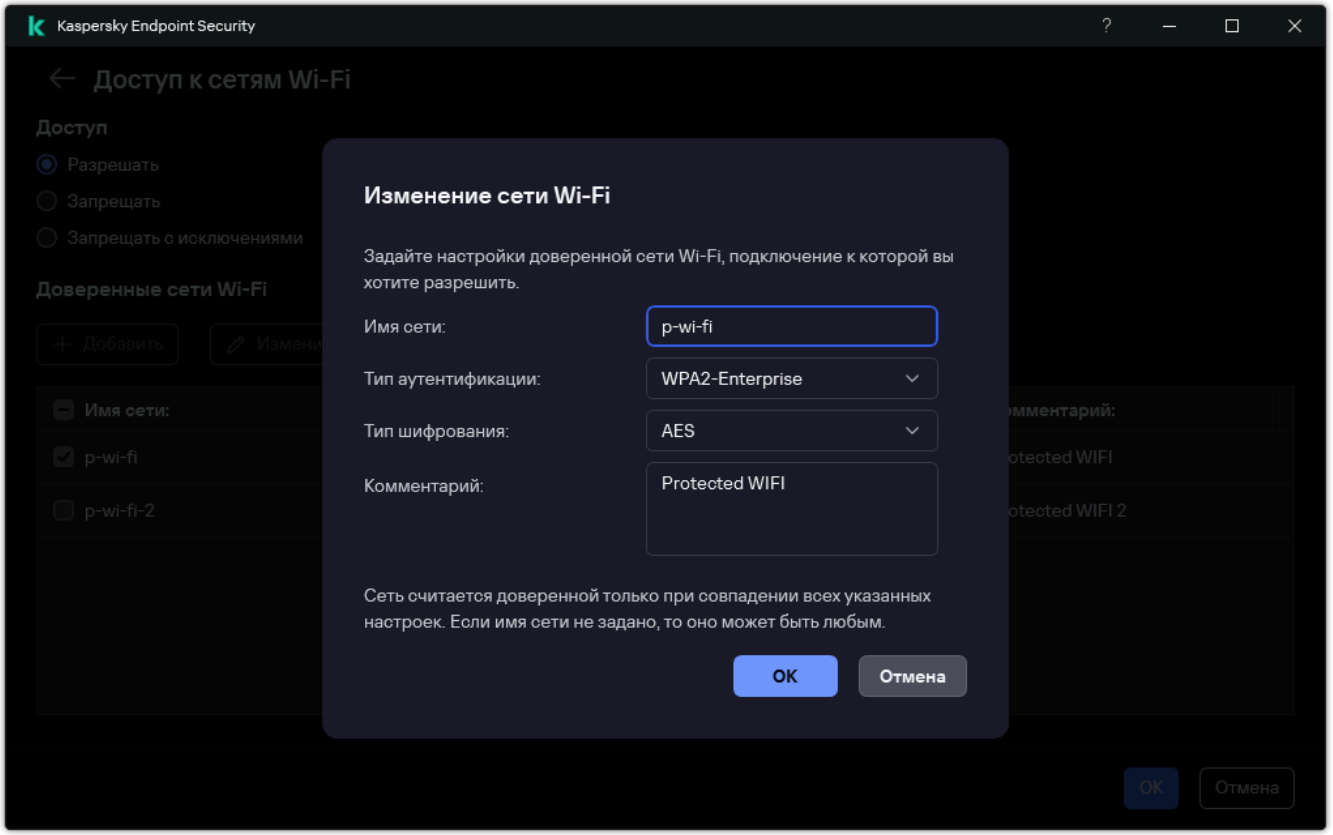
     Начиная с версии Kaspersky Endpoint Security для Windows 12.0 в приложение добавлена поддержка протокола WPA3. Если на компьютере применена политика Kaspersky Endpoint Security версии 12.2, на компьютерах с установленным приложением Kaspersky Endpoint Security версии 11.11.0 и более ранних версий будет выбран протокол WPA2, для версий 12.0 – 12.1 будет выбран протокол WPA2 / WPA3, для версии 12.2 и выше – WPA3.

   - **Тип шифрования**. Тип шифрования, используемый для защиты трафика сети Wi-Fi.
   - **Комментарий**. Дополнительная информация о добавленной сети Wi-Fi.

   Вы можете посмотреть параметры доверенной сети Wi-Fi в параметрах роутера.

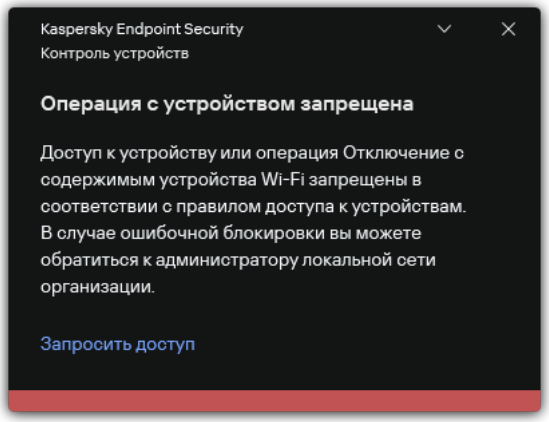
   Сеть Wi-Fi считается доверенной, если ее параметры соответствуют всем параметрам, указанным в правиле.

7. Сохраните внесенные изменения.



Параметры доверенной сети Wi-Fi

В результате при попытке пользователя подключиться к сети Wi-Fi, которая не указана в списке доверенных, приложение заблокирует подключение и покажет уведомление (см. рис. ниже).



Уведомление Контроля устройств

Мониторинг использования съемных дисков

Мониторинг использования съемных дисков включает в себя следующие инструменты:

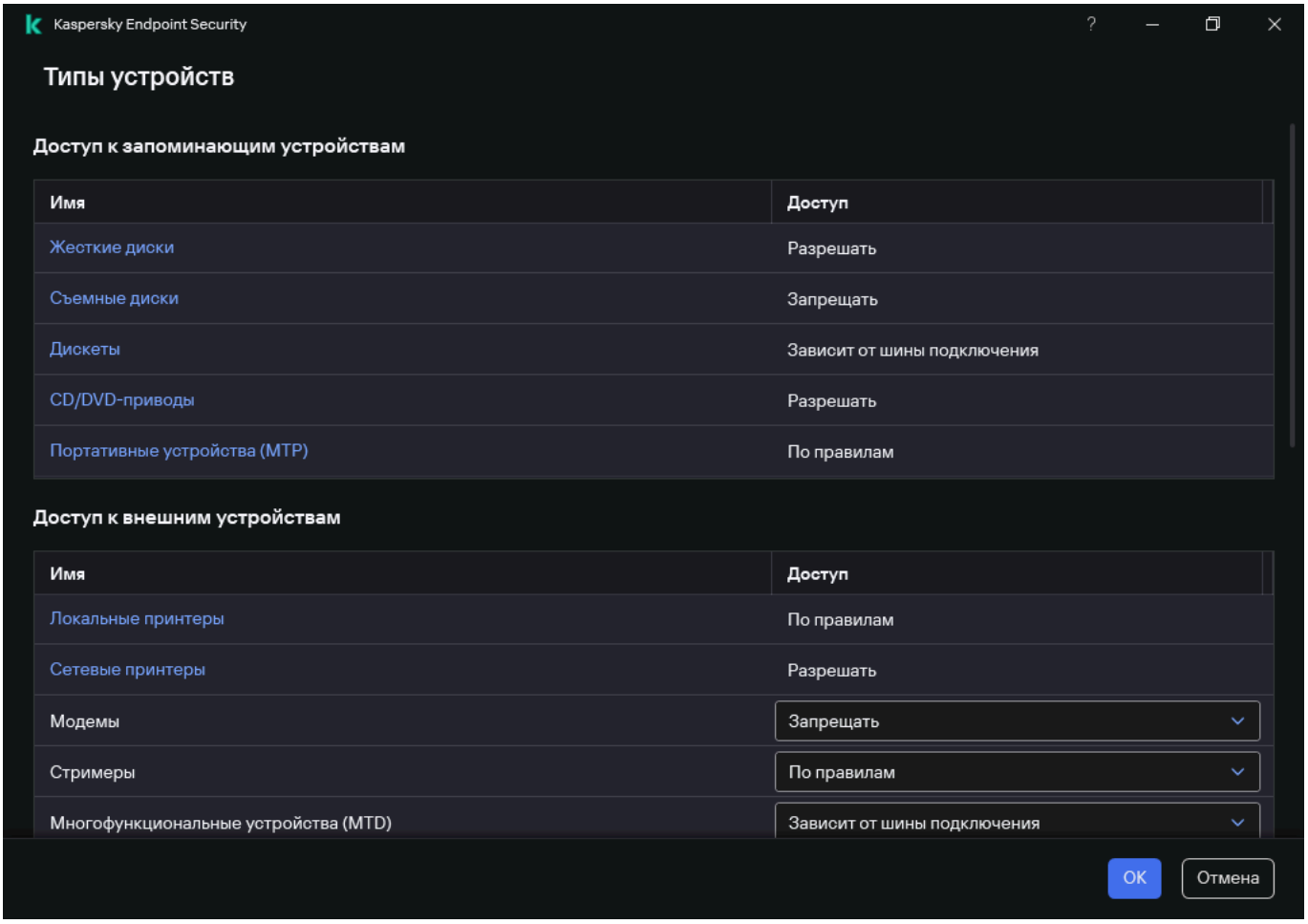
- Контроль операций с файлами на съемных дисках.
- Контроль подключения и отключения доверенных съемных дисков.

  Kaspersky Endpoint Security позволяет контролировать подключение и отключение всех доверенных устройств, не только съемных дисков. Вы можете включить запись событий в параметрах уведомлений для компонента Контроль устройств. События имеют уровень важности *Информационное сообщение*.

Чтобы включить мониторинг использования съемных дисков, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Устройства и сети Wi-Fi**.

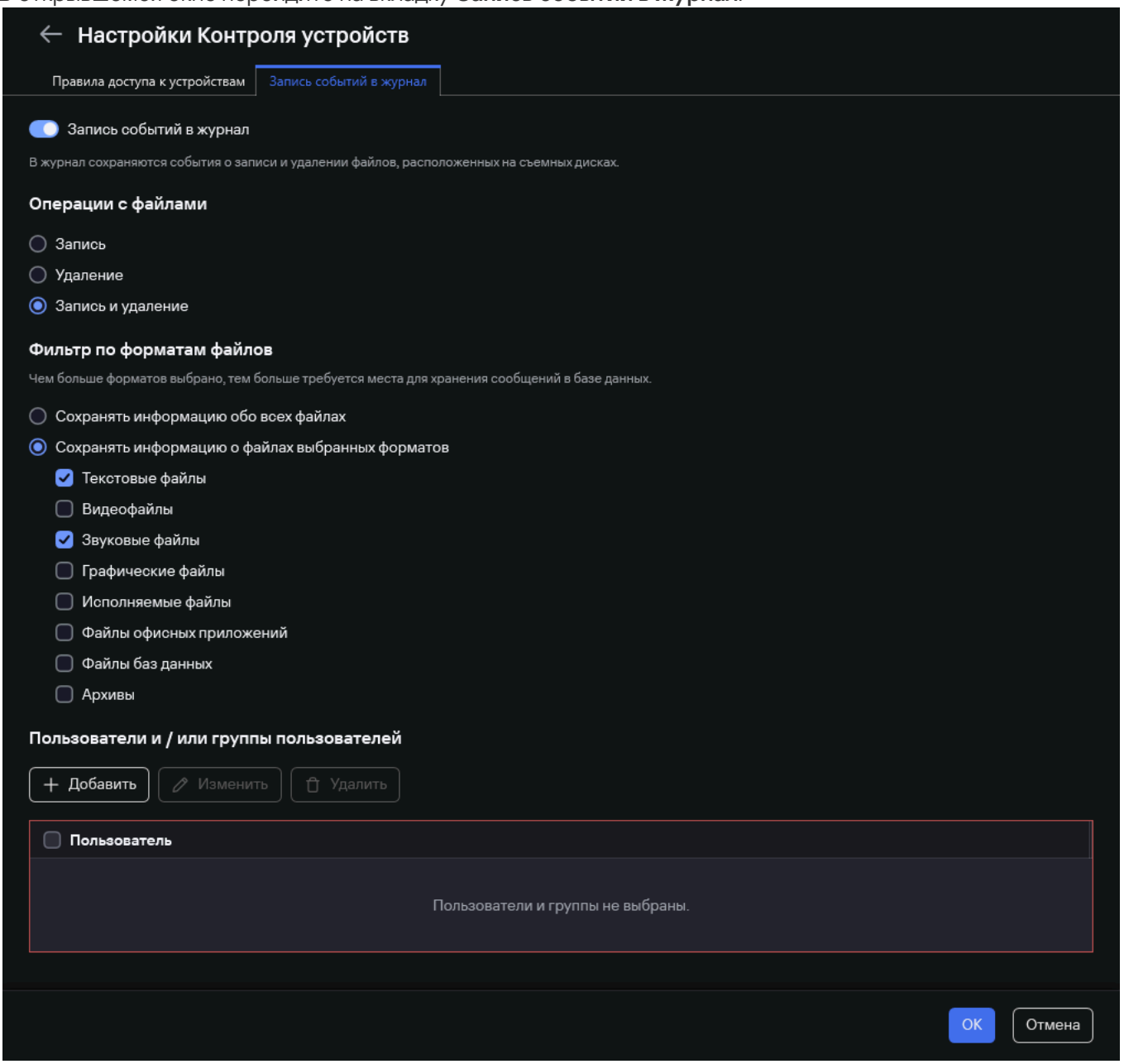
В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.



Типы устройств Контроля устройств

4. В блоке **Доступ к запоминающим устройствам** выберите элемент **Съемные диски**.

5. В открывшемся окне перейдите на вкладку **Запись событий в журнал**.



Параметры мониторинга использования съемных дисков

6. Включите переключатель **Запись событий в журнал**.

7. В блоке **Операции с файлами** выберите операции, которые вы хотите контролировать: **Запись**, **Удаление**.

8. В блоке **Фильтр по форматам файлов** выберите форматы файлов, информацию об операциях с которыми Контроль устройств должен записывать в журнал.

9. Выберите пользователей или группы пользователей, использование съемных дисков которых вы хотите контролировать.

10. Сохраните внесенные изменения.

В результате, когда пользователи будут производить запись в файлы, расположенные на съемных дисках, или удалять файлы со съемных дисков, Kaspersky Endpoint Security будет сохранять информацию о совершенной операции в журнал событий и отправлять события в Kaspersky Security Center. Вы можете просмотреть события, связанные с файлами на съемных дисках, в Консоли администрирования Kaspersky Security Center в рабочей области для узла **Сервер администрирования** на вкладке **События**. Чтобы

события отображались в локальном журнале событий Kaspersky Endpoint Security, требуется установить флажок **Выполнена операция с файлом** в параметрах уведомлений для компонента Контроль устройств.

Изменение периода кеширования

Компонент Контроль устройств регистрирует события, связанные с контролируемыми устройствами, такие как подключение и отключение устройства, чтение файла с устройства, запись файла на устройство и другие события. Далее Контроль устройств разрешает или запрещает выполнение действия в соответствии с параметрами Kaspersky Endpoint Security.

Контроль устройств хранит информацию о событиях в течение определенного времени, которое называется *периодом кеширования*. Кеширование информации о событии позволяет при повторении этого события не уведомлять Kaspersky Endpoint Security о нем и не запрашивать повторно доступ на выполнение соответствующего действия, например, подключение устройства. Это позволяет ускорить работу с устройством.

Событие считается повторяющимся, если все следующие параметры события совпадают с записью в кеше:

- идентификатор устройства;
- SID пользователя, от имени которого происходит обращение;
- класс устройства;
- действие с устройством;
- разрешение приложения для этого действия: разрешено или запрещено;
- путь к процессу, от имени которого совершается действие;
- файл, к которому происходит обращение.

Перед изменением периода кеширования выключите самозащиту Kaspersky Endpoint Security. После изменения периода кеширования включите самозащиту.

Чтобы изменить период кеширования, выполните следующие действия:

1. Откройте редактор реестра на компьютере.
2. В редакторе реестра перейдите в раздел:
   - для 64-битных операционных систем: `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.3\environment]`
   - для 32-битных операционных систем: `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.3\environment]`.
3. Откройте параметр `DeviceControlEventsCachePeriod` на редактирование.
4. Укажите количество минут, по истечении которых информация о событии в Контроле устройств должна удаляться.

Действия с доверенными устройствами

Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Для работы с доверенными устройствами вы можете предоставить доступ отдельному пользователю, группе пользователей или всем пользователям организации.

Например, если в вашей организации запрещено использование съемных дисков, но администраторы используют съемные диски в своей работе, вы можете разрешить использование съемных дисков только для группы администраторов. Для этого необходимо добавить съемные диски в список доверенных и настроить права доступа пользователей.

Не рекомендуется добавлять более 5000 доверенных устройств, поскольку это может привести к нестабильности системы.

Kaspersky Endpoint Security позволяет добавить устройство в список доверенных следующими способами:

- Если в вашей организации не развернуто решение Kaspersky Security Center, вы можете подключить устройство к компьютеру и добавить его в список доверенных в параметрах приложения. Чтобы распространить список доверенных устройств на все компьютеры организации, вы можете включить функцию объединения списков доверенных устройств в политике или использовать процедуру экспорта / импорта.

- Если в вашей организации развернуто решение Kaspersky Security Center, вы можете обнаружить все подключенные устройства удаленно и создать список доверенных устройств в политике. Список доверенных устройств будет доступен на всех компьютерах, к которым применена политика.

Kaspersky Endpoint Security позволяет контролировать использование доверенных устройств (подключение и отключение). Вы можете включить запись событий в параметрах уведомлений для компонента Контроль устройств. События имеют уровень важности *Информационные сообщения*.

Добавление устройства в список доверенных

Kaspersky Security Center получает информацию об устройствах, если на компьютерах установлено приложение Kaspersky Endpoint Security, включен Контроль устройств и включена передача данных об устройствах. Добавить устройство в список доверенных, информации о котором в Kaspersky Security Center нет, невозможно.

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей "Все").

Вы можете добавить устройство в список доверенных по следующим данным:

- **Устройства по идентификатору**. Каждое устройство имеет уникальный идентификатор (англ. Hardware ID, HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы. Пример идентификатора устройства: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств.

- **Устройства по модели**. Каждое устройство имеет идентификатор производителя (англ. Vendor ID, VID) и идентификатор продукта (англ. Product ID, PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы. Шаблон для ввода VID и PID: `VID_1234&PID_5678`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.

- **Устройства по маске идентификатора**. Если вы используете несколько устройств с похожими идентификаторами, вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security не поддерживает символ `?` при вводе маски. Например, `WDC_C*`.

- **Устройства по маске модели**. Если вы используете несколько устройств с похожими VID или PID (например, устройства одного производителя), вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security не поддерживает символ `?` при вводе маски. Например, `VID_05AC&PID_*`.

Как добавить устройство в список доверенных в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Контроль безопасности** → **Контроль устройств**.
5. В правой части окна выберите вкладку **Доверенные устройства**.
6. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных устройств для всех компьютеров организации.

   Списки доверенных устройств родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные устройства родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных устройств родительской политики невозможно.
7. Нажмите на кнопку **Добавить** и выберите способ добавления устройства в список доверенных.
8. Для фильтрации устройств в раскрывающемся списке **Тип устройств** выберите тип устройств (например, **Съемные диски**).

   Kaspersky Endpoint Security не поддерживает добавление устройств типа **Дискеты** в список доверенных.

9. В поле **Название / Модель** введите идентификатор устройства, модель (VID и PID) или маску в зависимости от выбранного способа добавления.

   Способ добавления устройств по маске модели (VID и PID) имеет особенность. Если вы ввели маску модели, которая не соответствует ни одной модели, Kaspersky Endpoint Security проверяет идентификатор устройства (HWID) на соответствие маске. Kaspersky Endpoint Security проверяет на соответствие только часть идентификатора устройства, определяющую поставщика и тип устройства (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Если маска модели соответствует этой части идентификатора устройства, на компьютере в список доверенных устройств будут добавлены устройства удовлетворяющие маске. При этом в Kaspersky Security Center по кнопке **Обновить** отобразится пустой список устройств. Для корректного отображения списка устройств вы можете использовать способ добавления по маске идентификатора устройства.

10. Для фильтрации устройств в поле **Компьютер** введите имя компьютера или маску имени компьютера, к которому подключено устройство.

    Символ `*` заменяет любой набор символов. Символ `?` заменяет любой один символ.

11. Нажмите на кнопку **Обновить**.

    В таблице отобразится список устройств, которые удовлетворяют заданным параметрам фильтрации.

12. Установите флажки напротив названий устройств, которые вы хотите добавить в список доверенных.

13. В поле **Комментарий** введите описание причины добавления устройств в список доверенных.

14. Справа от поля **Разрешать пользователям и / или группам пользователей** нажмите на кнопку **Выбрать**.

    Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

    По умолчанию доступ к доверенным устройствам разрешен для группы "Все".

15. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как добавить устройство в список доверенных в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Доверенная зона**.

5. В открывшемся окне перейдите по ссылке **Устройства**.

   Откроется окно со списком доверенных устройств.

6. В правой части окна выберите вкладку **Доверенные устройства**.

7. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных устройств для всех компьютеров организации.

   Списки доверенных устройств родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные устройства родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных устройств родительской политики невозможно.

8. Нажмите на кнопку **Добавить**.

   Откроется форма добавления доверенного устройства.

9. В блоке **Пользователь или группа** выберите пользователей, которым будет разрешен доступ к доверенным устройствам.

   Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   По умолчанию доступ к доверенным устройствам разрешен для группы "Все".

10. Для фильтрации устройств в раскрывающемся списке **Тип устройства** выберите тип устройств (например, **Съемные диски**).

    Kaspersky Endpoint Security не поддерживает добавление устройств типа **Дискеты** в список доверенных.

11. Если вам неизвестен точный идентификатор устройства или модель устройства, установите флажок **Использовать маску**.

12. Выберите способ добавления устройства: идентификатор устройства или модель (VID и PID).

    Способ добавления устройств по маске модели (VID и PID) имеет особенность. Если вы ввели маску модели, которая не соответствует ни одной модели, Kaspersky Endpoint Security проверяет идентификатор устройства (HWID) на соответствие маске. Kaspersky Endpoint Security проверяет на соответствие только часть идентификатора устройства, определяющую поставщика и тип устройства (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Если маска модели соответствует этой части идентификатора устройства, на компьютере в список доверенных устройств будут добавлены устройства удовлетворяющие маске. При этом в Kaspersky Security Center отобразится пустой список устройств. Для корректного отображения списка устройств вы можете использовать способ добавления по маске идентификатора устройства.

13. Для фильтрации устройств в поле **Поиск доверенных устройств** введите имя компьютера или маску имени компьютера, к которому подключено устройство.

    Символ `*` заменяет любой набор символов. Символ `?` заменяет любой один символ.

    В таблице отобразится список устройств, которые удовлетворяют заданным параметрам фильтрации.

14. Установите флажки напротив названий устройств, которые вы хотите добавить в список доверенных.

15. В поле **Комментарий** введите описание причины добавления устройств в список доверенных.

16. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как добавить устройство в список доверенных в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Доверенные устройства**.

   Откроется список доверенных устройств.
4. Нажмите на кнопку **Выбрать**.

   Откроется список подключенных устройств. Список устройств зависит от того, какое значение выбрано в раскрывающемся списке **Отображать подключенные устройства**.
5. В списке устройств выберите устройство, которое вы хотите добавить в список доверенных.

   > Kaspersky Endpoint Security не поддерживает добавление устройств типа **Дискеты** в список доверенных.
6. В поле **Комментарий** вы можете указать любую информацию о доверенном устройстве.
7. Выберите пользователей или группы пользователей, для которых вы хотите разрешить доступ к доверенным устройствам.

   Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.
8. Сохраните внесенные изменения.

При подключении устройства Kaspersky Endpoint Security проверяет список доверенных устройств для авторизованного пользователя. Если устройство доверенное, Kaspersky Endpoint Security разрешает доступ к устройству со всеми правами, даже если доступ к типу устройств или шине подключения запрещен. Если устройство недоверенное и доступ запрещен, вы можете запросить доступ к заблокированному устройству.

Экспорт и импорт списка доверенных устройств

Для распространения списка доверенных устройств на всех компьютеры организации вы можете использовать процедуру экспорта / импорта.

Например, если вам нужно распространить список доверенных съемных дисков, нужно выполнить следующие действия:

1. Последовательно подключите съемные диски к компьютеру.
2. В параметрах Kaspersky Endpoint Security добавьте съемные диски в список доверенных. Если требуется, настройте права доступа пользователей. Например, разрешите доступ к съемным дискам только администраторам.
3. Экспортируйте список доверенных устройств в параметрах Kaspersky Endpoint Security (см. инструкцию ниже).

4. Распространите файл с списком доверенных устройств на остальные компьютеры организации. Например, разместите файл в общей папке.

5. Импортируйте список доверенных устройств в параметрах Kaspersky Endpoint Security на остальных компьютерах организации (см. инструкцию ниже).

Чтобы импортировать или экспортировать список доверенных устройств, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.

3. В блоке **Настройка доступа** нажмите на кнопку **Доверенные устройства**.

   Откроется список доверенных устройств.

4. Для экспорта списка доверенных устройств выполните следующие действия:

   a. Выберите доверенные устройства, которые вы хотите экспортировать.

   b. Нажмите на кнопку **Экспорт**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список доверенных устройств, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует весь список доверенных устройств в XML-файл.

5. Для импорта списка доверенных устройств, выполните следующие действия:

   a. В раскрывающемся списке **Импорт** выберите нужное действие: **Импортировать и добавить к существующим** или **Импортировать и заменить существующие**.

   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных устройств.

   c. Откройте файл.

6. Сохраните внесенные изменения.

При подключении устройства Kaspersky Endpoint Security проверяет список доверенных устройств для авторизованного пользователя. Если устройство доверенное, Kaspersky Endpoint Security разрешает доступ к устройству со всеми правами, даже если доступ к типу устройств или шине подключения запрещен.

Получение доступа к заблокированному устройству

При настройке Контроля устройств вы можете случайно запретить доступ к необходимому для работы устройству.

Если в вашей организации не развернуто решение Kaspersky Security Center, то вы можете предоставить доступ к устройству в параметрах Kaspersky Endpoint Security. Например, вы можете добавить устройство в список доверенных или временно выключить Контроль устройств.

Если в вашей организации развернуто решение Kaspersky Security Center и к компьютерам применена политика, вы можете предоставить доступ к устройству в Консоли администрирования.

Онлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в онлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. Компьютер должен иметь возможность установить связь с Сервером администрирования.

Предоставление доступа в онлайн-режиме состоит из следующих этапов:

1. Пользователь отправляет администратору сообщение с запросом на предоставление доступа.
2. Администратор получает сообщение с запросом в консоли Kaspersky Security Center.

   В консоли Kaspersky Security Center предустановлена выборка событий *Запросы пользователей* для удобного поиска сообщений от пользователей.
3. Администратор добавляет устройство в список доверенных.

   Вы можете добавить доверенное устройство в политике для группы администрирования или в локальных параметрах приложения для отдельного компьютера.
4. Администратор обновляет параметры Kaspersky Endpoint Security на компьютере пользователя.

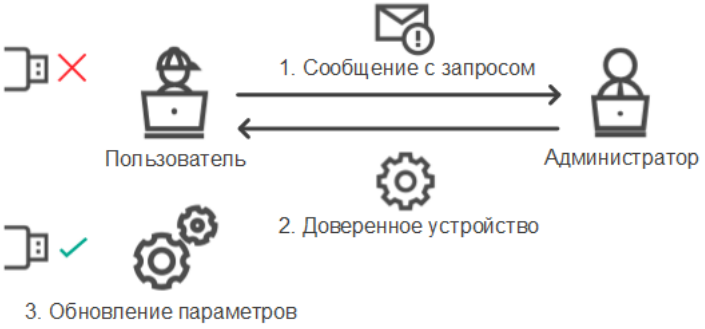


Схема предоставления доступа к устройству в онлайн-режиме

Офлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в офлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. В параметрах политики в разделе **Контроль устройств** должен быть установлен флажок **Разрешать запрашивать временный доступ**.

Если вам необходимо предоставить временный доступ к заблокированному устройству, а добавить устройство в список доверенных невозможно, вы можете предоставить доступ к устройству в офлайн-режиме. Таким образом, вы можете предоставить доступ к заблокированному устройству, если у компьютера отсутствует доступ к сети или компьютер находится за пределами сети организации.

Предоставление доступа в офлайн-режиме состоит из следующих этапов:

1. Пользователь создает файл запроса и передает его администратору.
2. Администратор создает из файла запроса ключ доступа и передает его пользователю.
3. Пользователь активирует ключ доступа.

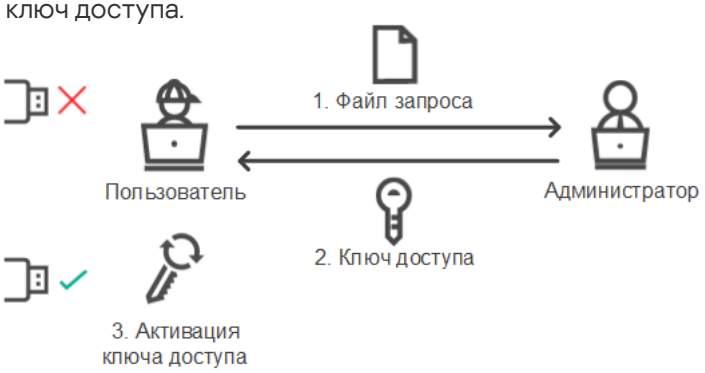


Схема предоставления доступа к устройству в офлайн-режиме

Онлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в онлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. Компьютер должен иметь возможность установить связь с Сервером администрирования.

Чтобы пользователю запросить доступ к заблокированному устройству, выполните следующие действия:

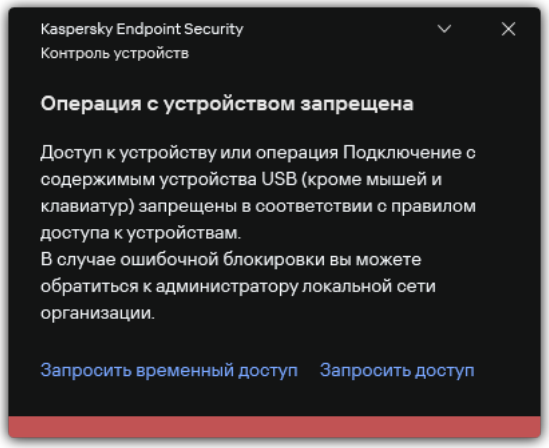
1. Подключите устройство к компьютеру.

   Kaspersky Endpoint Security покажет уведомление блокировки доступа к устройству (см. рис. ниже).

2. Нажмите на ссылку **Запросить доступ**.

   Откроется окно с сообщением для администратора. В сообщении содержится информация о заблокированном устройстве.

3. Нажмите на кнопку **Отправить**.



Уведомление Контроля устройств

Далее администратор в консоли Kaspersky Security Center получит событие *Сообщение администратору о запрете доступа к устройству*. Событие содержит имя пользователя, имя компьютера, данные об устройстве, к которому пользователь пытается получить доступ, и другие данные. Вы можете настроить способ уведомления администратора о получении таких событий и, например, выбрать уведомление по электронной почте. В консоли Kaspersky Security Center предустановлена выборка событий *Запросы пользователей* для удобного поиска сообщений от пользователей.

Для того, чтобы предоставить доступ вам нужно добавить устройство в список доверенных. После обновления параметров Kaspersky Endpoint Security на компьютере пользователь получит доступ к устройству.

Офлайн-режим предоставления доступа

Предоставление доступа к заблокированному устройству в офлайн-режиме доступно только в том случае, если в организации развернуто решение Kaspersky Security Center и к компьютеру применена политика. В параметрах политики в разделе **Контроль устройств** должен быть установлен флажок **Разрешать запрашивать временный доступ**.

Чтобы пользователю запросить доступ к заблокированному устройству, выполните следующие действия:

1. Подключите устройство к компьютеру.

   Kaspersky Endpoint Security покажет уведомление блокировки доступа к устройству (см. рис. ниже).

2. Нажмите на ссылку **Запросить временный доступ**.

   Откроется окно со списком подключенных устройств.

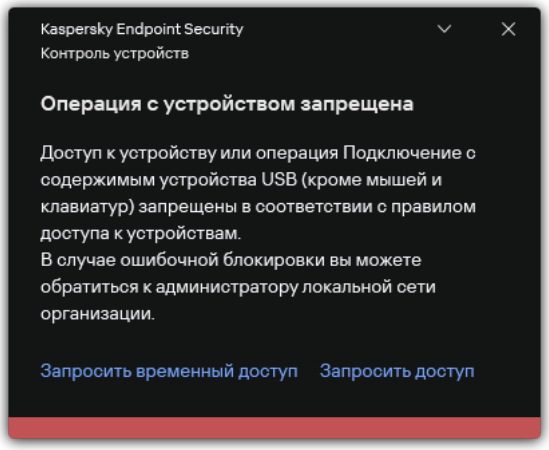
3. В списке подключенных устройств выберите устройство, к которому вы хотите получить доступ.

4. Нажмите на кнопку **Сформировать файл запроса**.

5. В поле **Длительность доступа к устройству** укажите, на какое время вы хотите получить доступ к устройству.

6. Сохраните файл в память компьютера.

В результате в память компьютера будет загружен файл запроса с расширением *.akey. Передайте файл запроса доступа к устройству администратору локальной сети организации любым доступным способом.



Уведомление Контроля устройств

Как администратору создать ключ доступа к заблокированному устройству в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите вкладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, пользователю которого вы хотите дать временный доступ к заблокированному устройству.
5. В контекстном меню компьютера выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите вкладку **Контроль устройств**.
7. Нажмите на кнопку **Обзор** и загрузите полученный от пользователя файл запроса.

   Отобразится информация о заблокированном устройстве, к которому пользователь запросил доступ.
8. Если требуется, измените значение параметра **Длительность доступа к устройству**.

   По умолчанию для параметра **Длительность доступа к устройству** выбрано значение, указанное пользователем при формировании файла запроса.
9. Укажите значение параметра **Срок активации**.

   Параметр содержит период времени, в течение которого пользователь может активировать доступ к заблокированному устройству с помощью предоставленного ключа доступа.
10. Сохраните файл ключа доступа в память компьютера.

Как администратору создать ключ доступа к заблокированному устройству в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. В списке клиентских компьютеров выберите компьютер, пользователю которого вы хотите дать временный доступ к заблокированному устройству.
3. Над списком компьютеров нажмите на кнопку с многоточием (...) и нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.
4. В открывшемся окне выберите раздел **Контроль устройств**.
5. Нажмите на кнопку **Обзор** и загрузите полученный от пользователя файл запроса.

   Отобразится информация о заблокированном устройстве, к которому пользователь запросил доступ.
6. Если требуется, измените значение параметра **Длительность доступа (в часах)**.

   По умолчанию для параметра **Длительность доступа (в часах)** выбрано значение, указанное пользователем при формировании файла запроса.

7. Укажите срок, в течение которого можно активировать ключ доступа на устройстве.

   Параметр содержит период времени, в течение которого пользователь может активировать доступ к заблокированному устройству с помощью предоставленного ключа доступа.

8. Сохраните файл ключа доступа в память компьютера.

В результате в память компьютера будет загружен ключ доступа к заблокированному устройству. Файл ключа доступа имеет расширение *.acode. Передайте ключ доступа к заблокированному устройству пользователю любым доступным способом.

Чтобы пользователю активировать ключ доступа, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.

3. В блоке **Запрос доступа** нажмите на кнопку **Запросить доступ к устройству**.

4. В открывшемся окне нажмите на кнопку **Активировать ключ доступа**.

5. В открывшемся окне выберите файл с ключом доступа к устройству, полученный от администратора локальной сети организации.

   Откроется окно с информацией о предоставленном доступе.

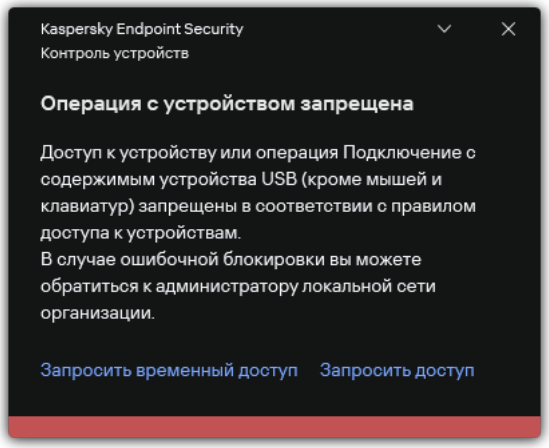
6. Нажмите на кнопку **ОК**.

   В результате пользователь получит доступ к устройству на срок, установленный администратором. Пользователь получит полный набор прав доступа к устройству (запись и чтение). По истечении срока действия ключа доступ к устройству будет заблокирован. Если пользователю требуется постоянный доступ к устройству, добавьте устройство в список доверенных.

Изменение шаблонов сообщений Контроля устройств

Когда пользователь пытается обратиться к заблокированному устройству, Kaspersky Endpoint Security выводит сообщение о блокировке доступа к устройству или о запрете операции над содержимым устройства. Специалисты "Лаборатории Касперского" составили шаблон сообщения пользователю, которое описывает причины блокировки доступа к устройству (см. рис. ниже).

Для работы с шаблонами сообщений предусмотрены специальные переменные (например, %USER_NAME%). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров. При формировании сообщения Kaspersky Endpoint Security определяет значение переменной из настроек операционной системы и подставляет это значение в сообщение, соответствующие конкретному компьютеру, пользователю и событию.



Уведомление Контроля устройств

Если блокировка доступа к устройству или запрет операции с содержимым устройства, по мнению пользователя, произошло ошибочно, пользователь может отправить сообщение администратору локальной сети организации по ссылке из текста сообщения о блокировке. Для этого пользователю нужно нажать на кнопку **Запросить доступ** или **Запросить временный доступ** и отправить администратору сообщение с описанием ситуации. Вы также можете подготовить шаблон сообщения администратору и добавить в текст сообщения данные, которые могут быть вам нужны для принятия решения о разрешении доступа к устройству. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете доступа к устройству**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

Как изменить шаблоны сообщений Контроля устройств в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Контроль устройств**.
4. В блоке **Настройки шаблонов сообщений** нажмите на кнопку **Шаблоны**.
5. В открывшемся окне настройте шаблоны сообщений Контроля приложений:

   - **Сообщение о блокировке**. Шаблон сообщения, которое появляется при обращении пользователя к заблокированному устройству. Также сообщение появляется при попытке пользователя совершить операцию над содержимым устройства, которая запрещена для этого пользователя.
   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к устройству или запрет операции над содержимым устройства, по мнению пользователя, произошли ошибочно.

Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Переменная** и выберите нужную переменную из списка доступных.

Также вы можете восстановить текст шаблона по умолчанию.

6. Сохраните внесенные изменения.

Как изменить шаблоны сообщений Контроля устройств в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль устройств**.
5. В блоке **Шаблоны сообщений** настройте шаблоны сообщений Контроля приложений:

   - **Сообщение пользователю**. Шаблон сообщения, которое появляется при обращении пользователя к заблокированному устройству. Также сообщение появляется при попытке пользователя совершить операцию над содержимым устройства, которая запрещена для этого пользователя.
   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к устройству или запрет операции над содержимым устройства, по мнению пользователя, произошли ошибочно.

   Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Добавить переменную** и выберите нужную переменную из списка доступных.

   Также вы можете восстановить текст шаблона по умолчанию.
6. Сохраните внесенные изменения.

Как изменить шаблоны сообщений Контроля устройств в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.
3. В блоке **Шаблоны сообщений** настройте шаблоны сообщений Контроля приложений:

   - **Сообщение о блокировке**. Шаблон сообщения, которое появляется при обращении пользователя к заблокированному устройству. Также сообщение появляется при попытке пользователя совершить операцию над содержимым устройства, которая запрещена для этого пользователя.
   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к устройству или запрет операции над содержимым устройства, по мнению пользователя, произошли ошибочно.

   Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Добавить переменную** и выберите нужную переменную из списка доступных.

   Также вы можете восстановить текст шаблона по умолчанию.
4. Сохраните внесенные изменения.

Анти-Бриджинг

Анти-Бриджинг предотвращает создание сетевых мостов, исключая возможность одновременной установки нескольких сетевых соединений для компьютера. Это позволяет защитить корпоративную сеть от атак через незащищенные, несанкционированные сети.

Анти-Бриджинг регулирует установку сетевых соединений с помощью *правил установки соединений*.

Правила установки соединений созданы для следующих предустановленных типов устройств:

- сетевые адаптеры;
- адаптеры Wi-Fi;
- модемы.

Если правило установки соединений включено, то Kaspersky Endpoint Security выполняет следующие действия:

- блокирует активное соединение при установке нового соединения, если для обоих соединений используется указанный в правиле тип устройств;
- блокирует соединения, установленные или устанавливаемые с помощью тех типов устройств, для которых используются правила с более низким приоритетом.

Включение Анти-Бриджинга

По умолчанию функция Анти-Бриджинг выключена.

Чтобы включить функцию Анти-Бриджинг, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Анти-Бриджинг**.
4. Используйте переключатель **Включить Анти-Бриджинг**, чтобы включить или выключить функцию.
5. Сохраните внесенные изменения.

После включения функции Анти-Бриджинг Kaspersky Endpoint Security блокирует уже установленные соединения в соответствии с правилами установки соединений.

Изменение статуса правила установки соединений

Чтобы изменить статус правила установки соединений, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Анти-Бриджинг**.
4. В блоке **Правила устройств** выберите правило, статус которого вы хотите изменить.
5. Используйте переключатели в графе **Контроль**, чтобы включить или выключить правило.
6. Сохраните внесенные изменения.

Изменение приоритета правила установки соединений

Чтобы изменить приоритет правила установки соединений, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль устройств**.
3. В блоке **Настройка доступа** нажмите на кнопку **Анти-Бриджинг**.
4. В блоке **Правила устройств** выберите правило, приоритет которого вы хотите изменить.
5. Кнопками **Вверх** / **Вниз** установите приоритет правила установки соединений.

   Чем выше правило в таблице правил, тем выше у него приоритет. Функция Анти-Бриджинг блокирует все соединения, кроме одного соединения, установленного с помощью того типа устройств, для которого используется правило с наиболее высоким приоритетом.
6. Сохраните внесенные изменения.

Адаптивный контроль аномалий

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов.

Компонент Адаптивный контроль аномалий отслеживает и блокирует действия, нехарактерные для компьютеров сети организации. Для отслеживания нехарактерных действий Адаптивный контроль аномалий использует набор правил (например, правило *Запуск Windows PowerShell из офисного приложения*). Правила созданы специалистами "Лаборатории Касперского" на основе типичных сценариев вредоносной активности. Вы можете выбрать поведение Адаптивного контроля аномалий для каждого из правил и, например, разрешить запуск PowerShell-скриптов для автоматизации решения корпоративных задач. Kaspersky Endpoint Security обновляет набор правил с базами приложения. Обновление набора правил нужно подтверждать вручную.

Настройка Адаптивного контроля аномалий

Настройка Адаптивного контроля аномалий состоит из следующих этапов:

1. Обучение Адаптивного контроля аномалий.

   После включения Адаптивного контроля аномалий правила работают в *обучающем режиме*. В ходе обучения Адаптивный контроль аномалий отслеживает срабатывание правил и отправляет события срабатывания в Kaspersky Security Center. Каждое правило имеет свой срок действия обучающего режима. Срок действия обучающего режима устанавливают специалисты "Лаборатории Касперского". Обычно срок действия обучающего режима составляет 2 недели.

   Если в ходе обучения правило ни разу не сработало, Адаптивный контроль аномалий будет считать действия, связанные с этим правилом, нехарактерным. Kaspersky Endpoint Security будет блокировать все действия, связанные с этим правилом.

   Если в ходе обучения правило сработало, Kaspersky Endpoint Security регистрирует события в отчете о срабатываниях правил и в хранилище **Правила срабатываний в статусе Интеллектуальное обучение**.

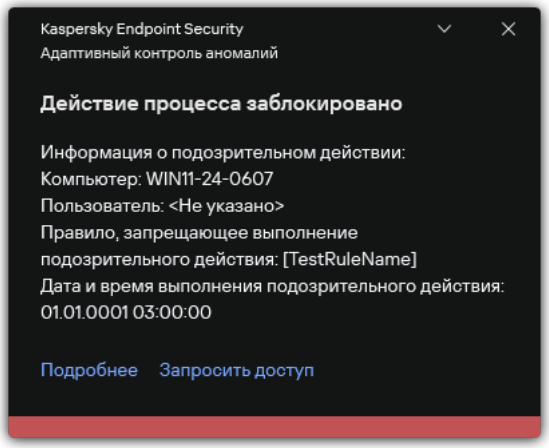
2. Анализ отчета о срабатывании правил.

   Администратор анализирует отчет о срабатываниях правил или содержание хранилища **Правила срабатываний в статусе Интеллектуальное обучение**. Далее администратор может выбрать поведение Адаптивного контроля аномалий при срабатывании правила: блокировать или разрешить. Также администратор может продолжить отслеживать срабатывание правила и продлить работу приложения в обучающем режиме. Если администратор не предпринимает никаких мер, приложение также продолжит работать в обучающем режиме. Отсчет срока действия обучающего режима начинается заново.

Настройка Адаптивного контроля аномалий происходит в режиме реального времени и осуществляется по следующим каналам:

- Адаптивный контроль аномалий автоматически начинает блокировать действия, связанные с правилами, которые не сработали в течение обучающего режима.
- Kaspersky Endpoint Security добавляет новые правила или удаляет неактуальные.
- Администратор настраивает работу Адаптивного контроля аномалий после анализа отчета о срабатывании правил и содержимого хранилища **Правила срабатываний в статусе Интеллектуальное обучение**. Рекомендуется проверять отчет о срабатывании правил и содержимое хранилища **Правила срабатываний в статусе Интеллектуальное обучение**.

При попытке вредоносного приложения выполнить действие, Kaspersky Endpoint Security заблокирует действие и покажет уведомление (см. рис. ниже).



Уведомление Адаптивного контроля аномалий

Алгоритм работы Адаптивного контроля аномалий

Kaspersky Endpoint Security принимает решение о выполнении действия, связанного с правилом, по следующему алгоритму (см. рис. ниже).



Алгоритм работы Адаптивного контроля аномалий

Обучение Адаптивного контроля аномалий

Адаптивный контроль аномалий включает в себя набор правил (шаблонов поведения). После включения Адаптивного контроля аномалий правила работают в *обучающем режиме*. В ходе обучения Адаптивный контроль аномалий отслеживает срабатывание правил и отправляет события срабатывания в Kaspersky Security Center. Адаптивный контроль аномалий не блокирует активность приложений на компьютере, а только информирует администратора. Вы также можете вручную выбрать действие при срабатывании правила Адаптивного контроля аномалий.

Как просмотреть список правил Адаптивного контроля аномалий в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

4. В окне политики выберите **Контроль безопасности → Адаптивный контроль аномалий**.

5. Установите флажок **Адаптивный контроль аномалий**.

6. В блоке **Настройки правил Адаптивного контроля аномалий** ознакомьтесь со списком правил.

   По умолчанию все правила работают в режиме **Интеллектуальное**.

7. Если требуется, подтвердите обновление правила Адаптивного контроля аномалий.

8. Если требуется, выберите действие при срабатывании правил Адаптивного контроля аномалий:

   - **Блокировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security блокирует активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.

   - **Информировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.

9. Если требуется, выключите правила, которые вы не хотите использовать.

10. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как просмотреть список правил Адаптивного контроля аномалий в Web Console и Cloud Console

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности → Адаптивный контроль аномалий**.

5. Включите переключатель **Адаптивный контроль аномалий ВКЛЮЧЕН**.

6. В блоке **Правила** ознакомьтесь со списком правил.

   По умолчанию все правила работают в режиме **Интеллектуальный**.

7. Если требуется, подтвердите обновление правила Адаптивного контроля аномалий.

8. Если требуется, выберите действие при срабатывании правил Адаптивного контроля аномалий:

   - **Блокировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security блокирует активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.

   - **Информировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.

9. Если требуется, выключите правила, которые вы не хотите использовать.

10. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как просмотреть список правил Адаптивного контроля аномалий в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. Включите переключатель **Адаптивный контроль аномалий**.
4. В блоке **Правила** перейдите по ссылке **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий. По умолчанию все правила работают в режиме **Интеллектуальное**.
5. Если требуется, подтвердите обновление правила Адаптивного контроля аномалий.
6. Если требуется, выберите действие при срабатывании правил Адаптивного контроля аномалий:

   - **Блокировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security блокирует активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.
   - **Информировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.
7. Если требуется, выключите правила, которые вы не хотите использовать.
8. Сохраните внесенные изменения.

Каждое правило имеет свой срок действия обучающего режима. Срок действия обучающего режима устанавливают специалисты "Лаборатории Касперского". Обычно срок действия обучающего режима составляет две недели.

Если в течение срока действия обучающего режима правило ни разу не сработало, то Адаптивный контроль аномалий считает такое поведение нетипичным и меняет статус правила на **Интеллектуальное блокирование**. Далее приложение будет блокировать активность, которая соответствует этому правилу.

Если в течение срока действия обучающего режима правило сработало, вам нужно вручную задать действие приложения при обнаружении активности, которая соответствует этому правилу. Если вы не выберите действие при срабатывании правила, Адаптивный контроль аномалий продолжит работать в режиме обучения.

Включение и выключение правила Адаптивного контроля аномалий

Чтобы включить или выключить правило Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.

4. В таблице выберите набор правил (например, *Активность офисных приложений*) и разверните набор.
5. Выберите правило (например, *Запуск Windows PowerShell из офисного приложения*).
6. Используйте переключатель в графе **Состояние**, чтобы включить или выключить правило Адаптивного контроля аномалий.
7. Сохраните внесенные изменения.

Изменение действия при срабатывании правила Адаптивного контроля аномалий

Чтобы изменить действие при срабатывании правила Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.
4. В таблице выберите правило.
5. Нажмите на кнопку **Изменить**.

   Откроется окно свойств правила Адаптивного контроля аномалий.
6. В блоке **Действие** выберите один из следующих пунктов:

   - **Интеллектуальное**. Если выбран этот вариант, то правило Адаптивного контроля аномалий работает в обучающем режиме в течение периода, определенного специалистами "Лаборатории Касперского". В этом режиме при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает запись в хранилище **Правила срабатываний в статусе Интеллектуальное обучение** Сервера администрирования Kaspersky Security Center. По истечении периода работы обучающего режима Kaspersky Endpoint Security блокирует активность, подпадающую под правило Адаптивного контроля аномалий, и создает в журнале запись, содержащую информацию об этой активности.
   - **Блокировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security блокирует активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.
   - **Информировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.
7. Сохраните внесенные изменения.

Создание исключения для правила Адаптивного контроля аномалий

Для правил Адаптивного контроля аномалий невозможно создать более 1000 исключений. Не рекомендуется создавать более 200 исключений. Чтобы уменьшить количество используемых исключений, рекомендуется использовать маски в параметрах исключений.

Исключение для правила Адаптивного контроля аномалий включает в себя описание исходных и целевых объектов. *Исходный объект* – объект, который выполняет действия. *Целевой объект* – объект, над которым выполняются действия. Например, вы открыли файл `file.xlsx`. В результате в память компьютера была добавлена библиотека с расширением dll, которую использует браузер (исполняемый файл `browser.exe`). В этом примере `file.xlsx` – исходный объект, Excel – исходный процесс, `browser.exe` – целевой объект, Browser – целевой процесс.

Как создать исключение для правила Адаптивного контроля аномалий в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.
5. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.
6. В таблице выберите правило.
7. Нажмите на кнопку **Изменить**.

   Откроется окно свойств правила Адаптивного контроля аномалий.
8. В блоке **Исключения** нажмите на кнопку **Добавить**.

   Откроется окно свойств исключения.
9. Выберите пользователя, для которого вы хотите настроить исключение.

   Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   Адаптивный контроль аномалий не поддерживает исключения для групп пользователей. Если вы выберите группу пользователей, Kaspersky Endpoint Security не применит исключение.
10. В поле **Описание** введите описание исключения.

11. Задайте параметры исходного объекта или исходного процесса, запущенных объектом:

    - **Исходный процесс**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`).
    - **Хеш исходного процесса**. Хеш файла (SHA256).
    - **Исходный объект**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`). Например, путь к файлу `document.docm`, который запускает целевые процессы с помощью скрипта или макроса.

      Вы также можете указать другие объекты для исключения, например, веб-адрес, макрос, команду в командной строке, путь реестра и другие. Укажите объект по следующему шаблону: `object://<object>`, где `<object>` – название объекта, например, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Вы также можете использовать маски, например, `object://*C:\Windows\temp\*`.
    - **Хеш исходного объекта**. Хеш файла (SHA256).

    Правило Адаптивного контроля аномалий не распространяется на действия, выполняемые объектом, или на процессы, запущенные объектом.

12. Задайте параметры целевого объекта или целевых процессов, запущенных над объектом.

    - **Целевой процесс**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`).
    - **Хеш целевого процесса**. Хеш файла (SHA256).
    - **Целевой объект**. Команда запуска целевого процесса. Укажите команду по следующему шаблону `object://<command>`, например, `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Также вы можете использовать маски, например, `object://*C:\Windows\temp\*`.
    - **Хеш целевого объекта**. Хеш файла (SHA256).

    Правило Адаптивного контроля аномалий не распространяется на действия над объектом или на процессы, запущенные над объектом.

13. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как создать исключение для правила Адаптивного контроля аномалий в Web Console

Как создать исключение для правила Адаптивного контроля аномалий в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.
4. В таблице выберите правило.

5. Нажмите на кнопку **Изменить**.

   Откроется окно свойств правила Адаптивного контроля аномалий.

6. В блоке **Исключения** нажмите на кнопку **Добавить**.

   Откроется окно свойств исключения.

7. Выберите пользователя, для которого вы хотите настроить исключение.

   Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   > Адаптивный контроль аномалий не поддерживает исключения для групп пользователей. Если вы выберите группу пользователей, Kaspersky Endpoint Security не применит исключение.

8. В поле **Описание** введите описание исключения.

9. Задайте параметры исходного объекта или исходного процесса, запущенных объектом:

   - **Исходный процесс**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`).
   - **Хеш исходного процесса**. Хеш файла (SHA256).
   - **Исходный объект**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`). Например, путь к файлу `document.docm`, который запускает целевые процессы с помощью скрипта или макроса.

     Вы также можете указать другие объекты для исключения, например, веб-адрес, макрос, команду в командной строке, путь реестра и другие. Укажите объект по следующему шаблону: `object://<object>`, где `<object>` – название объекта, например, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Вы также можете использовать маски, например, `object://*C:\Windows\temp\*`.
   - **Хеш исходного объекта**. Хеш файла (SHA256).

   Правило Адаптивного контроля аномалий не распространяется на действия, выполняемые объектом, или на процессы, запущенные объектом.

10. Задайте параметры целевого объекта или целевых процессов, запущенных над объектом.

    - **Целевой процесс**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`).
    - **Хеш целевого процесса**. Хеш файла (SHA256).
    - **Целевой объект**. Команда запуска целевого процесса. Укажите команду по следующему шаблону `object://<command>`, например, `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Также вы можете использовать маски, например, `object://*C:\Windows\temp\*`.
    - **Хеш целевого объекта**. Хеш файла (SHA256).

Правило Адаптивного контроля аномалий не распространяется на действия над объектом или на процессы, запущенные над объектом.

11. Сохраните внесенные изменения.

Экспорт и импорт исключений для правил Адаптивного контроля аномалий

Чтобы экспортировать или импортировать список исключений для выбранных правил, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.

3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.

4. Для экспорта списка исключений выполните следующие действия:

   a. Выберите правила, исключения для которых вы хотите экспортировать.

   b. Нажмите на кнопку **Экспорт**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список исключений, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Подтвердите, что вы хотите экспортировать только выбранные исключения, или экспортируйте весь список.

   e. Сохраните файл.

5. Для импорта списка исключений выполните следующие действия:

   a. Нажмите на кнопку **Импорт**.

   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

   c. Откройте файл.

      Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

6. Сохраните внесенные изменения.

Применение обновлений для правил Адаптивного контроля аномалий

Новые правила Адаптивного контроля аномалий могут быть добавлены в таблицу правил и существующие правила Адаптивного контроля аномалий могут быть удалены из таблицы правил по результату обновления антивирусных баз. Kaspersky Endpoint Security выделяет удаляемые и добавляемые правила Адаптивного контроля аномалий в таблице, если для этих правил обновление не было применено.

До тех пор, пока обновление не применено, Kaspersky Endpoint Security отображает удаленные в результате обновления правила Адаптивного контроля аномалий в таблице правил и присваивает этим правилам статус *Выключено*. Изменение параметров этих правил невозможно.

Чтобы применить обновления для правил Адаптивного контроля аномалий, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.
4. В открывшемся окне нажмите на кнопку **Подтвердить обновления**.

   Кнопка **Подтвердить обновления** доступна, если доступно обновление для правил Адаптивного контроля аномалий.
5. Сохраните внесенные изменения.

Изменение шаблонов сообщений Адаптивного контроля аномалий

Когда пользователь пытается выполнить действие, запрещенное правилами Адаптивного контроля аномалий, Kaspersky Endpoint Security выводит сообщение о блокировке потенциально опасных действий. Если блокировка, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить сообщение администратору локальной сети организации.

Для сообщений администратору о блокировке потенциально опасных действий предусмотрены шаблоны. Для работы с шаблонами сообщений предусмотрены специальные переменные (например, `%USER_NAME%`). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров. При формировании сообщения Kaspersky Endpoint Security определяет значение переменной из настроек операционной системы и подставляет это значение в сообщение, соответствующие конкретному компьютеру, пользователю и событию.

Чтобы изменить шаблон сообщения, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Адаптивный контроль аномалий**.

3. В блоке **Шаблоны** настройте шаблоны сообщений Адаптивного контроля аномалий:

   - **Сообщение о блокировке**. Шаблон сообщения для пользователя, которое появляется при срабатывании правила Адаптивного контроля аномалий, блокирующего нехарактерное действие.

   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка действия, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете действия приложения**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

   Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Добавить переменную** и выберите нужную переменную из списка доступных.

   Также вы можете восстановить текст шаблона по умолчанию с помощью кнопки **Сбросить**.

4. Сохраните внесенные изменения.

Мониторинг работы Адаптивного контроля аномалий

Адаптивный контроль аномалий включает в себя несколько инструментов мониторинга. Мониторинг работы Адаптивного контроля аномалий нужен в первую очередь для настройки компонента во время обучения.

Отчеты Адаптивного контроля аномалий

Адаптивный контроль аномалий использует следующие отчеты:

- **Отчет о состоянии правил Адаптивного контроля аномалий**. Отчет содержит информацию о статусе правил Адаптивного контроля аномалий (*Выключено*, *Интеллектуальное обучение*, *Интеллектуальное блокирование*, *Уведомлять*, *Блокировать*). Отчет позволяет проанализировать уровень обучения Адаптивного контроля аномалий и оценить количество правил, которые перешли из режима *Интеллектуальное обучение* в рабочий режим (например, *Интеллектуальное блокирование*).

- **Отчет о срабатываниях правил Адаптивного контроля аномалий**. Отчет содержит информацию о срабатываниях правил. Также отчет показывает режим срабатывания правила: *Блокировать* (включая *Интеллектуальное блокирование*) или *Уведомлять*. Отчет позволяет оценить активность Адаптивного контроля аномалий на компьютерах пользователей.

Как посмотреть отчеты Адаптивного контроля аномалий в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности → Адаптивный контроль аномалий**.
4. Выполните одно из следующих действий:
   - Если вы хотите просмотреть отчет о параметрах правил Адаптивного контроля аномалий, перейдите по ссылке **Отчет о состоянии правил Адаптивного контроля аномалий**.
   - Если вы хотите просмотреть отчет о срабатываниях правил Адаптивного контроля аномалий, перейдите по ссылке **Отчет о срабатываниях правил Адаптивного контроля аномалий**.
5. Запустится процесс формирования отчета.

Отчет отобразится в новом окне.

Как посмотреть отчеты Адаптивного контроля аномалий в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности → Адаптивный контроль аномалий**.
5. В блоке **Правила** выполните одно из следующих действий:
   - Если вы хотите просмотреть отчет о параметрах правил Адаптивного контроля аномалий, выберите **Посмотреть отчет → Состояние правил**.
   - Если вы хотите просмотреть отчет о срабатываниях правил Адаптивного контроля аномалий, перейдите по ссылке **Посмотреть отчет → Срабатывания**.
6. Запустится процесс формирования отчета.

Отчет отобразится в новом окне.

Для формирования отчетов в консоли Kaspersky Security Center необходимо включить передачу данных на Сервер администрирования. По умолчанию передача данных включена.

Как включить передачу данных для отчетов Адаптивного контроля аномалий в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки → Отчеты и хранилище**.
4. В блоке **Передача данных на Сервер администрирования** нажмите на кнопку **Настройка**.

5. Установите следующие флажки:

   - **Отчет о состоянии правил Адаптивного контроля аномалий**.
   - **Отчет о срабатываниях правил Адаптивного контроля аномалий**.

6. Сохраните внесенные изменения.

Как включить передачу данных для отчетов Адаптивного контроля аномалий в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Интеграция с KSC**.
5. В блоке **Передача данных на Сервер администрирования** установите следующие флажки:

   - **Отчет о состоянии правил Адаптивного контроля аномалий**.
   - **Отчет о срабатываниях правил Адаптивного контроля аномалий**.

6. Сохраните внесенные изменения.

Хранилище Правила срабатываний в статусе Интеллектуальное обучение

В режиме обучения Адаптивный контроль аномалий отправляет информацию о срабатывании правил в отдельное хранилище **Правила срабатываний в статусе Интеллектуальное обучение**. Информация о срабатывании правил представлена в хранилище в виде списка событий. Для настройки Адаптивного контроля аномалий вы можете или подтвердить нетипичное поведение на компьютере, или добавить исключение для правила.

События Адаптивного контроля аномалий

Адаптивный контроль аномалий регистрирует события срабатывания правил в режимах *Блокировать* (включая *Интеллектуальное блокирование*) и *Уведомлять*. Для этого предусмотрены следующие события:

Действие процесса заблокировано;

Действие процесса пропущено.

События содержат информацию о подозрительной активности, включая контрольные суммы файлов, учетные записи пользователей, время срабатывания правила и имя компьютера. После анализа события вы можете сразу добавить исключения для правила, если активность является легитимной.

Контроль приложений

Контроль приложений управляет запуском приложений на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании приложений. Также Контроль приложений снижает риск заражения компьютера, ограничивая доступ к приложениям.

Настройка Контроля приложений состоит из следующих этапов:

1. Создание категорий приложений.

   Администратор создает категории приложений, которыми администратор хочет управлять. Категории приложений предназначены для всех компьютеров сети организации независимо от групп администрирования. Для создания категории вы можете использовать следующие критерии: KL-категория (например, *Браузеры* или другая категория), хеш файла, производитель приложения и другие.

2. Создание правил Контроля приложений.

   Администратор создает правила Контроля приложений в политике для группы администрирования. Правило включает в себя категории приложений и статус запуска приложений из этих категорий: запрещен или разрешен. Администратор может создать множество правил. При этом одно приложение может соответствовать критериям нескольких правил. Приоритет запрещающего правила выше разрешающего. Kaspersky Endpoint Security проверяет приложение на принадлежность к правилу при каждом запуске. Kaspersky Endpoint Security последовательно проверяет приложение по всем правилам Контроля приложения.

3. Выбор режима работы Контроля приложений.

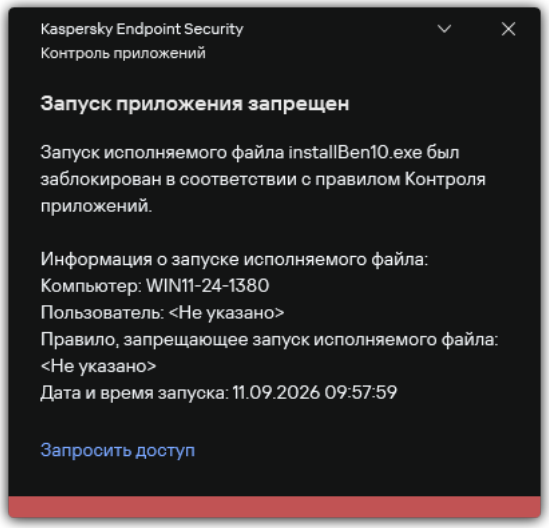
   Администратор выбирает режим работы с приложениями, которые не входят ни в одно из правил (списки запрещенных и разрешенных приложений).

При попытке пользователя запустить запрещенное приложение, Kaspersky Endpoint Security заблокирует запуск приложения и покажет уведомление (см. рис. ниже).

Для проверки настройки Контроля приложений предусмотрен *тестовый режим*. В этом режиме Kaspersky Endpoint Security выполняет следующие действия:

- разрешает запуск приложений, в том числе запрещенных;
- показывает уведомление о запуске запрещенного приложения и добавляет информацию в отчет на компьютере пользователя;

- отправляет данные о запуске запрещенных приложений в Kaspersky Security Center.



Уведомление Контроля приложений

Режимы работы Контроля приложений

Компонент Контроль приложений может работать в двух режимах:

- **Список запрещенных**. Режим, при котором Контроль приложений разрешает пользователям запуск любых приложений, кроме тех, которые запрещены в правилах Контроля приложений.

  Этот режим работы Контроля приложений установлен по умолчанию.

- **Список разрешенных**. Режим, при котором Контроль приложений запрещает пользователям запуск любых приложений, кроме тех, которые разрешены и не запрещены в правилах Контроля приложений.

  Если разрешающие правила Контроля приложений сформированы максимально полно, компонент запрещает запуск всех новых приложений, не проверенных администратором локальной сети организации, но обеспечивает работоспособность операционной системы и проверенных приложений, которые нужны пользователям для выполнения должностных обязанностей.

  Вы можете ознакомиться с рекомендациями по настройке правил Контроля приложений в режиме списка разрешенных приложений.

Настройка Контроля приложений для работы в этих режимах возможна как в локальном интерфейсе Kaspersky Endpoint Security, так и с помощью Kaspersky Security Center.

Однако Kaspersky Security Center предоставляет инструменты, недоступные в локальном интерфейсе Kaspersky Endpoint Security и необходимые для следующих задач:

- Создание категорий приложений.

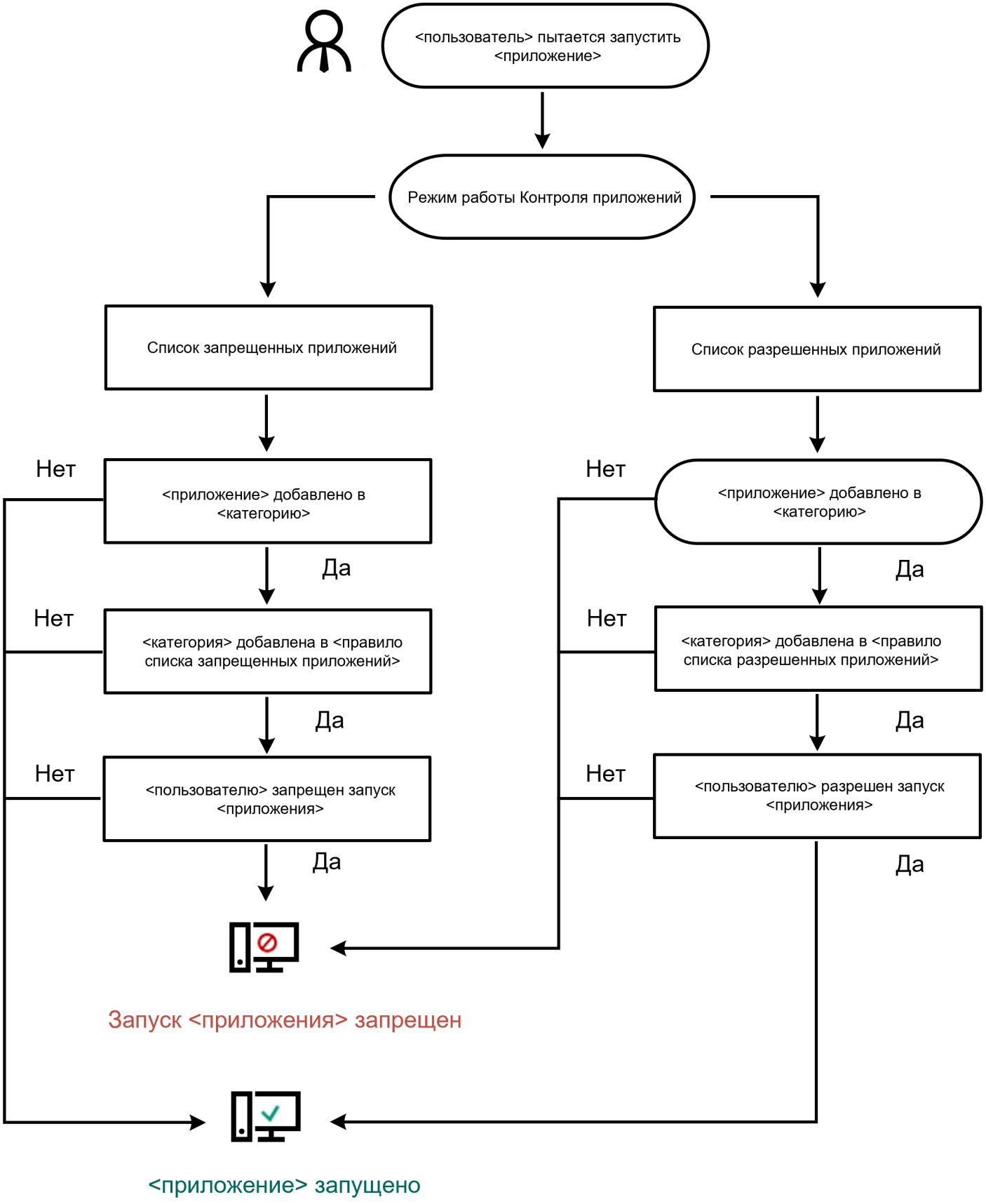
  Правила Контроля приложений, сформированные в Консоли администрирования Kaspersky Security Center, основываются на созданных вами категориях приложений, а не на включающих и исключающих условиях, как в локальном интерфейсе Kaspersky Endpoint Security.

- Получение информации о приложениях, которые установлены на компьютерах локальной сети организации.

Поэтому настройку работы компонента Контроль приложений рекомендуется выполнять с помощью Kaspersky Security Center.

Алгоритм работы Контроля приложений

Kaspersky Endpoint Security использует алгоритм для принятия решения о запуске приложения (см. рис. ниже).



Ограничения функциональности Контроля приложений

Работа компонента Контроль приложений ограничена в следующих случаях:

- При обновлении версии приложения импорт параметров компонента Контроль приложений не поддерживается.
- При отсутствии соединения с серверами KSN Kaspersky Endpoint Security получает информацию о репутации приложения и их модулей только из локальных баз.

  Список приложений, для которых Kaspersky Endpoint Security определяет KL-категорию **Другие приложения\Приложения, доверенные согласно репутации в KSN**, при наличии соединения с серверами KSN может отличаться от списка приложений, для которых Kaspersky Endpoint Security определяет KL-категорию **Другие приложения\Приложения, доверенные согласно репутации в KSN**, при отсутствии соединения с KSN.

- В базе данных Kaspersky Security Center может храниться информация о 150 000 обработанных файлов. При достижении этого количества записей новые файлы не будут обработаны. Для возобновления работы инвентаризации требуется удалить с компьютера, на котором установлено приложение Kaspersky Endpoint Security, файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.
- Компонент не контролирует запуск скриптов, если скрипт передается интерпретатору не через командную строку.

  Если запуск интерпретатора разрешен правилами Контроля приложений, то компонент не блокирует скрипт, запущенный из этого интерпретатора.

  Если запуск хотя бы одного из скриптов, указанных в командной строке интерпретатора, запрещен правилами Контроля приложений, то компонент блокирует все скрипты, указанные в командной строке интерпретатора.

- Компонент не контролирует запуск скриптов из интерпретаторов, не поддерживаемых приложением Kaspersky Endpoint Security.

  Kaspersky Endpoint Security поддерживает следующие интерпретаторы:

  - Java;
  - PowerShell.

  Поддерживаются следующие типы интерпретаторов:

  - %ComSpec%;
  - %SystemRoot%\system32\regedit.exe;
  - %SystemRoot%\regedit.exe;

- %SystemRoot%\system32\regedt32.exe;
- %SystemRoot%\system32\cscript.exe;
- %SystemRoot%\system32\wscript.exe;
- %SystemRoot%\system32\msiexec.exe;
- %SystemRoot%\system32\mshta.exe;
- %SystemRoot%\system32\rundll32.exe;
- %SystemRoot%\system32\wwahost.exe;
- %SystemRoot%\syswow64\cmd.exe;
- %SystemRoot%\syswow64\regedit.exe;
- %SystemRoot%\syswow64\regedt32.exe;
- %SystemRoot%\syswow64\cscript.exe;
- %SystemRoot%\syswow64\wscript.exe;
- %SystemRoot%\syswow64\msiexec.exe;
- %SystemRoot%\syswow64\mshta.exe;
- %SystemRoot%\syswow64\rundll32.exe;
- %SystemRoot%\syswow64\wwahost.exe.

Получение данных об установленных приложениях

Для создания оптимальных правил Контроля приложений рекомендуется получить представление о приложениях, используемых на компьютерах локальной сети организации. Для этого вы можете получить следующую информацию:

- производители, версии и локализации приложений, которые используются в локальной сети организации;
- регулярность обновлений приложений;
- политики использования приложений, принятые в организации (это могут быть политики безопасности или административные политики);
- расположение хранилища дистрибутивов приложений.

Просмотр информации о приложениях

Данные об установленных приложениях предоставляет Агент администрирования Kaspersky Security Center. Данные об установленных приложениях доступны в консоли Kaspersky Security Center в папке **Реестр приложений**. Агент администрирования обновляет данные при каждой синхронизации с Kaspersky Security Center. Подробнее о данных, отправляемых Агентом администрирования, см. в справке Kaspersky Security Center.

Чтобы открыть окно свойств приложения в папке Реестр программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите **Дополнительно** → **Управление приложениями** → **Реестр приложений**.
3. Выберите приложение.
4. В контекстном меню приложения выберите пункт **Свойства**.

Просмотр информации об исполняемых файлах

Вы можете снизить нагрузку на базу данных при получении информации об исполняемых файлах. Для этого рекомендуется запускать задачу *Инвентаризация* на нескольких эталонных компьютерах, на которых установлен стандартный набор приложений.

Данные об исполняемых файлах предоставляет Kaspersky Endpoint Security. Для получения данных об оборудовании нужно применить активную политику, в которой включена передача данных об установленных приложениях (по умолчанию передача данных включена).

Как включить передачу данных о приложениях в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Отчеты и хранилище**.
4. В блоке **Передача данных на Сервер администрирования** нажмите на кнопку **Настройка**.
5. Установите флажок **Запускаемые приложения**.
6. Сохраните внесенные изменения.

Как включить передачу данных о приложениях в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки → Интеграция с KSC**.

5. В блоке **Передача данных на Сервер администрирования** нажмите на кнопку **Дополнительные настройки**.

6. В открывшемся окне установите флажок **О запускаемых приложениях**.

7. Сохраните внесенные изменения.

Вы можете получить список исполняемых файлов с помощью задачи Kaspersky Endpoint Security *Инвентаризация*. Список исполняемых файлов доступен в консоли Kaspersky Security Center в папке **Исполняемые файлы**.

Перед запуском задачи *Инвентаризация* убедитесь, что база данных соответствует рекомендациям Kaspersky Security Center. Подробнее об ограничениям СУБД см. в справке Kaspersky Security Center.

Как запустить задачу Инвентаризация в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3) → Инвентаризация**.

Шаг 2. Область инвентаризации

Создайте список папок, в которых Kaspersky Endpoint Security будет искать исполняемые файлы. Настройте параметры инвентаризации (см. таблицу ниже).

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Выбор учетной записи для запуска задачи

Выберите учетную запись для запуска задачи *Инвентаризация*. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя. Если в область инвентаризации входят сетевые диски или другие объекты, доступ к которым ограничен, выберите учетную запись пользователя с необходимыми правами доступа.

Шаг 5. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную.

Шаг 6. Определение названия задачи

Введите название задачи, например, *Инвентаризация эталона*.

Шаг 7. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи. В результате на компьютерах пользователей будет выполнен поиск исполняемых файлов в соответствии с установленным расписанием.

Как запустить задачу Инвентаризация в Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Инвентаризация**.

   c. В поле **Название задачи** введите короткое описание, например, *Инвентаризация эталона*.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

5. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.

6. Завершите работу мастера.

   В списке задач отобразится новая задача.

7. Для настройки параметров задачи перейдите в свойства задачи (см. таблицу ниже).

8. Установите флажок напротив задачи.

9. Нажмите на кнопку **Запустить**.

   Вы можете отслеживать статус задачи, количество устройств, на которых задача выполнена успешно или завершилась с ошибкой. В результате на компьютерах пользователей будет выполняться поиск исполняемых файлов в соответствии с установленным расписанием.

Чтобы открыть окно свойств исполняемого файла в папке Исполняемые файлы, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве Консоли администрирования выберите папку **Дополнительно → Управление приложениями → Исполняемые файлы**.

3. Выберите исполняемый файл.

4. В контекстном меню исполняемого файла выберите пункт **Свойства**.

Открыв окно свойств выбранного приложения в папке **Реестр приложений** или **Исполняемые файлы**, вы можете получить общую информацию о приложении и о его исполняемых файлах, а также просмотреть список компьютеров, на которых установлено это приложение.

Обновление данных об установленных приложениях и исполняемых файлах

В Kaspersky Endpoint Security оптимизирована работа Контроля приложений с базой данных исполняемых файлов. Kaspersky Endpoint Security автоматически обновляет базу данных после удаления файла с компьютера. Это позволяет поддерживать базу данных в актуальном состоянии и экономить ресурсы Kaspersky Security Center. Для поддержания базы данных установленных приложений в актуальном состоянии необходимо включить передачу данных о приложениях на Сервер администрирования (по умолчанию включено).

Параметры инвентаризации

Параметр	Описание
Области инвентаризации	Список объектов, которые будут составлять область инвентаризации.
Инвентаризация DLL-модулей	Kaspersky Endpoint Security проверяет наличие DLL-модулей в области инвентаризации и отправляет информацию в Kaspersky Security Center. Включение инвентаризации DLL-модулей значительно увеличивает время выполнения задачи инвентаризации и размер базы данных.
Инвентаризация файлов скриптов	Kaspersky Endpoint Security проверяет наличие скриптов в области инвентаризации и отправляет информацию в Kaspersky Security Center. Включение инвентаризации файлов скриптов значительно увеличивает время выполнения задачи инвентаризации и размер базы данных.
Выполнять только во время простоя компьютера	Отложенный запуск задачи, если ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка. Если вы прервали выполнение задачи и, например, разблокировали компьютер, Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана. Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.
Проверять только новые и измененные файлы	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Пропускать файл, если его проверка длится более (сек.)	Ограничение длительности проверки файла. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку текущего файла и начинает проверку следующего. Это ускоряет проверку компьютера, но снижает уровень защиты. По умолчанию Kaspersky Endpoint Security прекращает проверку файла по истечении 30 секунд.
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	Проверка дистрибутивов сторонних приложений.
Не распаковывать составные файлы большого размера	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.

Включение режима блокирования только запрещенных приложений

Режим *Запрещенные приложения* – это режим, при котором Контроль приложений разрешает пользователям запуск любых приложений, кроме тех, которые запрещены в правилах Контроля приложений. То есть, если запрещающего правила нет, Контроль приложений разрешает запуск приложения. Этот режим работы Контроля приложений установлен по умолчанию.

Перед включением режима *Запрещенные приложения* рекомендуется проверить работу правил Контроля приложений. Для этого вы можете включить режим тестирования.

Как включить режим блокирования только запрещенных приложений в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Контроль безопасности** → **Контроль приложений**.
5. Установите флажок **Контроль приложений**.
6. В блоке **Настройки Контроля приложений** в раскрывающемся списке **Режим контроля** выберите вариант **Список запрещенных**.
7. В раскрывающемся списке **Действие** выберите действие Контроля приложения:
   - **Тестировать правила**. Контроль приложений не блокирует приложения, запуск которых запрещен правилами, но формирует события о запуске запрещенных приложений.
   - **Применять правила**. Контроль приложений блокирует запуск запрещенных приложений и формирует соответствующих события.
8. Выберите статус для правил Контроля приложений:
   - **Вкл**. Статус означает, что правило используется во время работы компонента Контроль приложений.
   - **Выкл**. Статус означает, что правило не используется во время работы компонента Контроль приложений.
   - **Тест**. Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск приложений, на которые распространяется действие правила, но заносит информацию о запуске этих приложений в отчет.

   Если требуется, добавьте новые правила Контроля приложений.

9. Настройте дополнительные параметры Контроля приложений:

   - **Контролировать загрузку динамических библиотек (значительно увеличивает нагрузку на систему)**. Если флажок установлен, то Kaspersky Endpoint Security контролирует загрузку DLL-модулей при запуске пользователями приложений. Информация о DLL-модуле и приложении, загрузившем этот DLL-модуль, сохраняется в отчет.

     При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в параметрах Контроля приложений включено правило по умолчанию **Приложения ОС** или другое правило, которое содержит KL-категорию **Приложения ОС\Доверенные сертификаты** и обеспечивает загрузку доверенных DLL-модулей и драйверов до запуска Kaspersky Endpoint Security. Включение контроля загрузки DLL-модулей и драйверов при выключенном правиле **Приложения ОС** может привести к нестабильности операционной системы.

     Kaspersky Endpoint Security контролирует только DLL-модули и драйверы, загруженные с момента установки флажка. Рекомендуется перезагрузить компьютер после установки флажка, чтобы приложение контролировало все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security.

   - **Использовать строгую проверку цифровой подписи**. Вы можете выбрать сертификат в качестве условия срабатывания правила Контроля приложений. Если флажок установлен, то Kaspersky Endpoint Security применяет правила к приложениям, подписанным сертификатом только из доверенного системного хранилища сертификатов приложения. Приложения, подписанные таким сертификатом, также являются доверенными для компонентов защиты, например, для задачи *Поиск вредоносного ПО*. При этом, если в правиле Контроля приложений указать сертификат из другого хранилища, Kaspersky Endpoint Security не применит такое правило.

     Если флажок снят, Kaspersky Endpoint Security применяет правила к приложениям, подписанным сертификатом из хранилища доверенных корневых центров Windows (англ. Trusted Root Certificate Store). Такие приложения не входят в доверенную зону. Компоненты защиты контролируют активность таких приложений.

   - **Сообщение о блокировке**. Шаблон сообщения, которое появляется при срабатывании правила Контроля приложений, блокирующего запуск приложения.

   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка приложения, по мнению пользователя, произошла ошибочно.

10. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить режим блокирования только запрещенных приложений в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль приложений**.
5. Включите переключатель **Контроль приложений ВКЛЮЧЕН**.
6. В блоке **Режим работы** выберите вариант **Блокировать все, не указанное в списке правил**.

7. В блоке **Действие** выберите действие Контроля приложения:

- **Информировать**. Контроль приложений не блокирует приложения, запуск которых запрещен правилами, но формирует события о запуске запрещенных приложений.
- **Применять правила**. Контроль приложений блокирует запуск запрещенных приложений и формирует соответствующих события.

8. Выберите статус для правил Контроля приложений:

- **Включено**. Статус означает, что правило используется во время работы компонента Контроль приложений.
- **Выключено**. Статус означает, что правило не используется во время работы компонента Контроль приложений.
- **Тестовый режим**. Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск приложений, на которые распространяется действие правила, но заносит информацию о запуске этих приложений в отчет.

Если требуется, добавьте новые правила Контроля приложений.

9. Настройте дополнительные параметры Контроля приложений:

- **Контролировать загрузку DLL-модулей**. Если флажок установлен, то Kaspersky Endpoint Security контролирует загрузку DLL-модулей при запуске пользователями приложений. Информация о DLL-модуле и приложении, загрузившем этот DLL-модуль, сохраняется в отчет.

  При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в параметрах Контроля приложений включено правило по умолчанию **Приложения ОС** или другое правило, которое содержит KL-категорию **Приложения ОС\Доверенные сертификаты** и обеспечивает загрузку доверенных DLL-модулей и драйверов до запуска Kaspersky Endpoint Security. Включение контроля загрузки DLL-модулей и драйверов при выключенном правиле **Приложения ОС** может привести к нестабильности операционной системы.

  Kaspersky Endpoint Security контролирует только DLL-модули и драйверы, загруженные с момента установки флажка. Рекомендуется перезагрузить компьютер после установки флажка, чтобы приложение контролировало все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security.

- **Использовать строгую проверку цифровой подписи**. Вы можете выбрать сертификат в качестве условия срабатывания правила Контроля приложений. Если флажок установлен, то Kaspersky Endpoint Security применяет правила к приложениям, подписанным сертификатом только из доверенного системного хранилища сертификатов приложения. Приложения, подписанные таким сертификатом, также являются доверенными для компонентов защиты, например, для задачи *Поиск вредоносного ПО*. При этом, если в правиле Контроля приложений указать сертификат из другого хранилища, Kaspersky Endpoint Security не применит такое правило.

  Если флажок снят, Kaspersky Endpoint Security применяет правила к приложениям, подписанным сертификатом из хранилища доверенных корневых центров Windows (англ. Trusted Root Certificate Store). Такие приложения не входят в доверенную зону. Компоненты защиты контролируют активность таких приложений.

- **Сообщение пользователю**. Шаблон сообщения, которое появляется при срабатывании правила Контроля приложений, блокирующего запуск приложения.

- **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка приложения, по мнению пользователя, произошла ошибочно.

10. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить режим блокирования только запрещенных приложений в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.

3. Включите переключатель **Контроль приложений**.

4. В блоке **Режим контроля запуска приложений** выберите вариант **Список запрещенных. Разрешены все приложения, кроме указанных в списке**.

5. В блоке **Действие при запуске приложений, запрещенных правилами** выберите действие Контроля приложения:

   - **Информировать (тестовый режим) и записывать в отчет**. Контроль приложений не блокирует приложения, запуск которых запрещен правилами, но формирует события о запуске запрещенных приложений.

   - **Блокировать**. Контроль приложений блокирует запуск запрещенных приложений и формирует соответствующих события.

6. Выберите статус для правил Контроля приложений:

   - **Включено**. Статус означает, что правило используется во время работы компонента Контроль приложений.

   - **Выключено**. Статус означает, что правило не используется во время работы компонента Контроль приложений.

   - **Тестовый режим**. Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск приложений, на которые распространяется действие правила, но заносит информацию о запуске этих приложений в отчет.

   Если требуется, добавьте новые правила Контроля приложений.

7. Настройте дополнительные параметры Контроля приложений:

   - **Контролировать загрузку динамических библиотек**. Если флажок установлен, то Kaspersky Endpoint Security контролирует загрузку DLL-модулей при запуске пользователями приложений. Информация о DLL-модуле и приложении, загрузившем этот DLL-модуль, сохраняется в отчет.

При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в параметрах Контроля приложений включено правило по умолчанию **Приложения ОС** или другое правило, которое содержит KL-категорию **Приложения ОС\Доверенные сертификаты** и обеспечивает загрузку доверенных DLL-модулей и драйверов до запуска Kaspersky Endpoint Security. Включение контроля загрузки DLL-модулей и драйверов при выключенном правиле **Приложения ОС** может привести к нестабильности операционной системы.

Kaspersky Endpoint Security контролирует только DLL-модули и драйверы, загруженные с момента установки флажка. Рекомендуется перезагрузить компьютер после установки флажка, чтобы приложение контролировало все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security.

- **Использовать строгую проверку цифровой подписи**. Вы можете выбрать сертификат в качестве условия срабатывания правила Контроля приложений. Если флажок установлен, то Kaspersky Endpoint Security применяет правила к приложениям, подписанным сертификатом только из доверенного системного хранилища сертификатов приложения. Приложения, подписанные таким сертификатом, также являются доверенными для компонентов защиты, например, для задачи *Поиск вредоносного ПО*. При этом, если в правиле Контроля приложений указать сертификат из другого хранилища, Kaspersky Endpoint Security не применит такое правило.

  Если флажок снят, Kaspersky Endpoint Security применяет правила к приложениям, подписанным сертификатом из хранилища доверенных корневых центров Windows (англ. Trusted Root Certificate Store). Такие приложения не входят в доверенную зону. Компоненты защиты контролируют активность таких приложений.

- **Шаблоны сообщений о блокировке приложений**. Шаблон сообщения, которое появляется при срабатывании правила Контроля приложений, блокирующего запуск приложения.

- **Шаблон сообщения, появляющегося при блокировке запуска приложения**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка приложения, по мнению пользователя, произошла ошибочно.

8. Сохраните внесенные изменения.

В результате Контроль приложений будет блокировать запрещенные приложения. Также Kaspersky Endpoint Security формирует события *Запуск приложения запрещен*. На основании этих событий вы можете сформировать в консоли Kaspersky Security Center отчет – *Отчет о запрещенных приложениях*. В сводной информации отчета вы можете просмотреть список приложений и компьютеров, на которых сработало правило Контроля приложений.

Контроль приложений на основе эталонного компьютера

Вы можете использовать эталонный компьютер для создания образа с набором необходимых приложений. Далее вы можете использовать образ для развертывания операционной системы и приложений на других компьютерах. Поддерживать образ в актуальном состоянии не всегда возможно. Контроль приложений позволяет поддерживать список разрешенных приложений на основе эталонного компьютера. Контроль приложений автоматически определяет набор установленных приложений на эталонном компьютере и обновляет категорию. Таким образом, компьютеры получают актуальный список разрешенных приложений.

Настройка Контроля приложений на основе эталонного компьютера состоит из следующих этапов:

1. Создание автоматически пополняемой категории. При создании новой категории вам нужно выбрать тип **Категория, в которую входят исполняемые файлы из указанной папки** и выбрать эталонный компьютер.

Как создать автоматически пополняемую категорию в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Дополнительно → Управление приложениями → Категории приложений**.
3. В рабочей области нажмите на кнопку **Новая категория**.

   Запустится мастер создания категории приложений.
4. Следуйте указаниям мастера создания категории приложений.

Шаг 1. Выбор типа категории

Выберите тип категории **Категория, в которую входят исполняемые файлы с выбранных устройств**.

Шаг 2. Ввод названия пользовательской категории

На этом шаге укажите название категории приложений.

Шаг 3. Параметры

> Этот шаг доступен, если вы выбрали тип категории **Категория, в которую входят исполняемые файлы с выбранных устройств**.

На этом шаге нажмите на кнопку **Добавить** и укажите компьютеры, исполняемые файлы с которых Kaspersky Security Center добавит в категорию приложений. Kaspersky Security Center добавит в категорию приложений все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.

Также на этом шаге вы можете настроить следующие параметры:

- Алгоритм вычисления хеш-функции. Для выбора алгоритма необходимо установить хотя бы один из следующих флажков:
  - **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**.
  - **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**.

- Флажок **Синхронизировать данные с хранилищем Сервера администрирования**. Установите этот флажок, если вы хотите, чтобы Kaspersky Security Center периодически очищал категорию приложений и добавлял в нее все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.

  Если флажок **Синхронизировать данные с хранилищем Сервера администрирования** снят, то после создания категории приложений Kaspersky Security Center не будет вносить в нее изменения.

Шаг 4. Фильтр

На этом шаге настройте фильтр для файлов.

Вы можете указать тип файла, который используется для создания категории приложений.

- **Все файлы**. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.
- **Только файлы вне категорий приложений**. Для создаваемой категории учитываются только файлы вне категорий приложений.

Вы можете указать папки выбранных компьютеров, содержащие файлы, которые используются для создания категории приложений.

- **Все папки**. Для создаваемой категории учитываются все папки. По умолчанию выбран этот вариант.
- **Указанная папка**. Для создаваемой категории учитывается только указанная папка. Если вы выбрали этот параметр, вам нужно указать путь к папке.

Шаг 5. Создание пользовательской категории

Завершите работу мастера.

Как создать автоматически пополняемую категорию в Web Console и Cloud Console

1. В главном окне Web Console выберите **Операции → Сторонние приложения → Категории приложений**.

   Откроется список категорий приложений.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории приложений.

3. Настройте основные параметры категории приложений:

   - Название категории.
   - Способ создания категории. Выберите тип категории **Категория, в которую входят исполняемые файлы с выбранных устройств**.

   Перейдите к следующему шагу.

4. Настройте дополнительные параметры категории приложений:

   - Укажите компьютеры, исполняемые файлы с которых Kaspersky Security Center добавит в категорию приложений. Kaspersky Security Center добавит в категорию приложений все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.
   - Выберите алгоритм вычисления хеш-функции.
   - Настройте период синхронизации данных с хранилищем Сервера администрирования.
   - Настройте фильтр для файлов.

5. Завершите работу мастера.

При создании автоматически пополняемой категории может быть удобно разделить файлы на несколько категорий. Например, файлы операционной системы и файлы из папки Program Files. Для этого вы можете использовать фильтр в параметрах категории и выбрать отдельные папки.

2. Выбор режима Контроля приложений. Вам нужно запретить запуск всех приложений кроме разрешенных. Для этого выберите режим *Запрещенные приложения*.

3. Создание правила Контроля приложений. В параметрах правила нужно выбрать категорию, в которую входят исполняемые файлы с эталонного компьютера.

   Как настроить Контроль приложений на основе эталонного компьютера в Консоли администрирования (MMC)

   1. Откройте Консоль администрирования Kaspersky Security Center.
   2. В дереве консоли выберите папку **Политики**.
   3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
   4. В окне политики выберите **Контроль безопасности** → **Контроль приложений**.
   5. Установите флажок **Контроль приложений**.
   6. В блоке **Настройки Контроля приложений** в раскрывающемся списке **Режим контроля** выберите вариант **Список запрещенных**.
   7. В раскрывающемся списке **Действие** выберите действие Контроля приложения:

      - **Тестировать правила**. Контроль приложений не блокирует приложения, запуск которых запрещен правилами, но формирует события о запуске запрещенных приложений.
      - **Применять правила**. Контроль приложений блокирует запуск запрещенных приложений и формирует соответствующих события.

   8. В списке правил Контроля приложений нажмите на кнопку **Добавить**.

      Запустится мастер добавления правила Контроля приложений.

   9. В раскрывающемся списке **Категория** выберите автоматически пополняемую категорию на основе эталонного компьютера.
   10. Выберите пользователей или группы пользователей, к которым вы хотите применить правило Контроля приложений.

11. Настройте дополнительные параметры правила Контроля приложений:

    - **Запретить остальным пользователям**. Приложение запрещает запуск приложений, принадлежащих к выбранной категории, всем пользователям, которые не указаны в списке.

    - **Доверенные приложения обновления**. Приложения, входящие в выбранную категорию, Kaspersky Endpoint Security считает доверенными приложениями обновления с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

12. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить Контроль приложений на основе эталонного компьютера в Web Console и Cloud Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности** → **Контроль приложений**.

5. Включите переключатель **Контроль приложений ВКЛЮЧЕН**.

6. В блоке **Режим работы** выберите вариант **Блокировать все, не указанное в списке правил**.

7. В блоке **Действие** выберите действие Контроля приложения:

    - **Информировать**. Контроль приложений не блокирует приложения, запуск которых запрещен правилами, но формирует события о запуске запрещенных приложений.

    - **Применять правила**. Контроль приложений блокирует запуск запрещенных приложений и формирует соответствующих события.

8. В списке правил Контроля приложений нажмите на кнопку **Добавить**.

   Запустится мастер добавления правила Контроля приложений.

9. В блоке **Категории/Приложения** выберите автоматически пополняемую категорию на основе эталонного компьютера.

10. Выберите пользователей или группы пользователей, к которым вы хотите применить правило Контроля приложений.

11. Настройте дополнительные параметры правила Контроля приложений:

    - **Пользователи**. Приложение запрещает запуск приложений, принадлежащих к выбранной категории, всем пользователям, которые не указаны в списке.

    - **Доверенные приложения обновления**. Приложения, входящие в выбранную категорию, Kaspersky Endpoint Security считает доверенными приложениями обновления с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

12. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить Контроль приложений на основе эталонного компьютера в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** → **Контроль приложений**.
3. Включите переключатель **Контроль приложений**.
4. В блоке **Режим контроля запуска приложений** выберите вариант **Список запрещенных. Разрешены все приложения, кроме указанных в списке**.
5. В блоке **Действие при запуске приложений, запрещенных правилами** выберите действие Контроля приложения:
   - **Информировать (тестовый режим) и записывать в отчет**. Контроль приложений не блокирует приложения, запуск которых запрещен правилами, но формирует события о запуске запрещенных приложений.
   - **Блокировать**. Контроль приложений блокирует запуск запрещенных приложений и формирует соответствующих события.
6. В списке правил Контроля приложений нажмите на кнопку **Добавить**.

   Запустится мастер добавления правила Контроля приложений.
7. В блоке **Категория** выберите автоматически пополняемую категорию на основе эталонного компьютера.
8. Выберите пользователей или группы пользователей, к которым вы хотите применить правило Контроля приложений.
9. Настройте дополнительные параметры правила Контроля приложений:
   - **Запретить остальным пользователям**. Приложение запрещает запуск приложений, принадлежащих к выбранной категории, всем пользователям, которые не указаны в списке.
   - **Доверенные приложения обновления**. Приложения, входящие в выбранную категорию, Kaspersky Endpoint Security считает доверенными приложениями обновления с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.
10. Сохраните внесенные изменения.

Управление правилами Контроля приложений

Kaspersky Endpoint Security контролирует запуск приложений пользователями с помощью правил. В правиле Контроля приложений содержатся условия срабатывания и действия компонента Контроль приложений при срабатывании правила (разрешение или запрещение пользователям запускать приложение).

Условия срабатывания правила

Условие срабатывания правила представляет собой соответствие "тип условия – критерий условия – значение условия". На основании условий срабатывания правила Kaspersky Endpoint Security применяет (или не применяет) правило к приложению.

В правилах используются следующие типы условий:

- *Включающие условия*. Kaspersky Endpoint Security применяет правило к приложению, если приложение соответствует хотя бы одному включающему условию.
- *Исключающие условия*. Kaspersky Endpoint Security не применяет правило к приложению, если приложение соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию.

Условия срабатывания правила формируются с помощью критериев. Для формирования условий в Kaspersky Endpoint Security используются следующие критерии:

- путь к папке с исполняемым файлом приложения или путь к исполняемому файлу приложения;
- метаданные: название исполняемого файла приложения, версия исполняемого файла приложения, название приложения, версия приложения, производитель приложения;
- хеш исполняемого файла приложения;
- сертификат: издатель, субъект, отпечаток;
- принадлежность приложения к KL-категории;
- расположение исполняемого файла приложения на съемном диске.

Для каждого критерия, используемого в условии, нужно указать его значение. Если параметры запускаемого приложения соответствуют значениям критериев, указанных во включающем условии, правило срабатывает. В этом случае Контроль приложений выполняет действие, прописанное в правиле. Если параметры приложения соответствуют значениям критериев, указанных в исключающем условии, Контроль приложений не контролирует запуск приложения.

Если в качестве условия срабатывания правила вы выбрали сертификат, вам нужно убедиться, что этот сертификат добавлен в доверенное системное хранилище на компьютере, и проверить параметры использования доверенного системного хранилища в приложении.

Решения компонента Контроль приложений при срабатывании правила

При срабатывании правила Контроль приложений в соответствии с правилом разрешает или запрещает пользователям (группам пользователей) запускать приложения. Вы можете выбирать отдельных пользователей или группы пользователей, которым разрешен или запрещен запуск приложений, для которых срабатывает правило.

Если в правиле не указан ни один пользователь, которому разрешен запуск приложений, удовлетворяющих правилу, правило называется *запрещающим*.

Если в правиле не указан ни один пользователь, которому запрещен запуск приложений, удовлетворяющих правилу, правило называется *разрешающим*.

Приоритет запрещающего правила выше приоритета разрешающего правила. Например, если для группы пользователей назначено разрешающее правило Контроля приложений и для одного из пользователей этой группы назначено запрещающее правило Контроля приложений, то этому пользователю будет запрещен запуск приложения.

Статус работы правила

Правила Контроля приложений могут иметь один из следующих статусов работы:

- **Включено**. Статус означает, что правило используется во время работы компонента Контроль приложений.
- **Выключено**. Статус означает, что правило не используется во время работы компонента Контроль приложений.
- **Тестовый режим**. Статус означает, что Kaspersky Endpoint Security разрешает запуск приложений, на которые распространяется действие правила, но заносит информацию о запуске этих приложений в отчет.

Добавление условия срабатывания правила Контроля приложений

Для удобства формирования правил Контроля приложений вы можете создать категории приложений.

Рекомендуется создать категорию "приложения для работы", которая включает в себя стандартный набор приложений, используемых в организации. Если различные группы пользователей используют различные наборы приложений для работы, вы можете создать отдельную категорию приложений для работы каждой группы пользователей.

Чтобы создать категорию приложений в Консоли администрирования, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Дополнительно → Управление приложениями → Категории приложений**.
3. В рабочей области нажмите на кнопку **Новая категория**.

   Запустится мастер создания пользовательской категории.
4. Следуйте указаниям мастера создания пользовательской категории.

Шаг 1. Выбор типа категории

На этом шаге выберите один из следующих типов категорий приложений:

- Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную. Если вы выбрали этот тип категории, то на шаге *Настройка условий для включения приложений в категории* и шаге *Настройка условий для исключения приложений из категории* вы сможете задать критерии, по которым исполняемые файлы будут попадать в категорию.

- Категория, в которую входят исполняемые файлы с выбранных устройств. Исполняемые файлы обрабатываются автоматически, их метрики заносятся в категорию. Если вы выбрали этот тип категории, то на шаге *Параметры* вы сможете указать компьютер, исполняемые файлы с которого будут автоматически попадать в категорию.

- Категория, в которую входят исполняемые файлы из указанной папки. Исполняемые файлы приложений, копируемых в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию. Если вы выбрали этот тип категории, то на шаге *Папка хранилища* вы сможете указать папку, исполняемые файлы из которой будут автоматически попадать в категорию.

При создании автоматически пополняемой категории Kaspersky Security Center выполняет инвентаризацию файлов следующих форматов: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, SCR.

Шаг 2. Ввод названия пользовательской категории

На этом шаге укажите название категории приложений.

Шаг 3. Настройка условий для включения приложений в категорию

При добавлении значительного количества условий в правила Контроля приложений (например, хешей файлов) возрастает потребление ресурсов компьютера. Когда общее количество условий достигает 50 000, возможны проблемы с производительностью компьютера. Для оптимизации производительности рекомендуется проанализировать и сократить количество условий.

Этот шаг доступен, если вы выбрали тип категории **Пополняемая вручную категория**.

На этом шаге в раскрывающемся списке **Добавить** выберите условия для включения приложений в категорию:

- **Из списка исполняемых файлов**. Добавьте приложения из списка исполняемых файлов на клиентском устройстве в пользовательскую категорию.

- **Из свойств файла**. Укажите детальные данные исполняемых файлов в качестве условия добавления приложений в пользовательскую категорию.

- **Метаданные файлов папки**. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет метаданные этих исполняемых файлов в качестве условия добавления приложений в пользовательскую категорию.

- **Хеши файлов папки**. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет хеши этих исполняемых файлов в качестве условия добавления приложений в пользовательскую категорию.

- **Сертификаты файлов из папки**. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Kaspersky Security Center укажет сертификаты этих исполняемых файлов в качестве условия добавления приложений в пользовательскую категорию.

  Не рекомендуется использовать условия, в свойствах которых не указывается параметр **Отпечаток сертификата**.

- **Метаданные файлов установщика MSI**. Выберите MSI-пакет. Kaspersky Security Center укажет метаданные исполняемых файлов, упакованных в этот MSI-пакет, в качестве условия добавления приложений в пользовательскую категорию.

- **Контрольные суммы файлов msi-инсталлятора приложения**. Выберите MSI-пакет. Kaspersky Security Center укажет хеши исполняемых файлов, упакованных в этот MSI-пакет, в качестве условия добавления приложений в пользовательскую категорию.

- **Из KL-категории**. Укажите KL-категорию в качестве условия добавления приложений в пользовательскую категорию. *KL-категория* – сформированный специалистами "Лаборатории Касперского" список приложений, обладающих общими тематическими признаками. Например, KL-категория *Офисные приложения* включает в себя приложения из пакетов Microsoft Office, Adobe Acrobat и другие.

  Вы можете выбрать все KL-категории, чтобы сформировать расширенный список доверенных приложений.

- **Задайте путь к приложению (поддерживаются маски)**. Выберите папку на клиентском устройстве. Kaspersky Security Center добавит исполняемые файлы из этой папки в пользовательскую категорию.

- **Выберите сертификат из хранилища сертификатов**. Выберите сертификаты, которыми подписаны исполняемые файлы, в качестве условия добавления приложений в пользовательскую категорию.

  Не рекомендуется использовать условия, в свойствах которых не указывается параметр **Отпечаток сертификата**.

  Вы можете выбрать хранилище сертификатов. По умолчанию Контроль приложений применяет правила только для приложений, подписанных сертификатом из системного доверенного хранилища сертификатов. Для этого предназначен флажок **Использовать строгую проверку цифровой подписи**.

- **Тип носителя**. Укажите тип запоминающего устройства (все жесткие и съемные диски или только съемные диски) в качестве условия добавления приложений в пользовательскую категорию.

Шаг 4. Настройка условий для исключения приложений из категории

Этот шаг доступен, если вы выбрали тип категории **Пополняемая вручную категория**.

Приложения, указанные на этом шаге, исключаются из категории, даже если эти приложения были указаны на шаге "Настройка условий для включения приложений в категорию".

На этом шаге в раскрывающемся списке **Добавить** выберите условия для исключения приложений из категории:

- **Из списка исполняемых файлов**. Добавьте приложения из списка исполняемых файлов на клиентском устройстве в пользовательскую категорию.
- **Из свойств файла**. Укажите детальные данные исполняемых файлов в качестве условия добавления приложений в пользовательскую категорию.
- **Метаданные файлов папки**. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет метаданные этих исполняемых файлов в качестве условия добавления приложений в пользовательскую категорию.
- **Хеши файлов папки**. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет хеши этих исполняемых файлов в качестве условия добавления приложений в пользовательскую категорию.
- **Сертификаты файлов из папки**. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Kaspersky Security Center укажет сертификаты этих исполняемых файлов в качестве условия добавления приложений в пользовательскую категорию.
- **Метаданные файлов установщика MSI**. Выберите MSI-пакет. Kaspersky Security Center укажет метаданные исполняемых файлов, упакованных в этот MSI-пакет, в качестве условия добавления приложений в пользовательскую категорию.
- **Контрольные суммы файлов msi-инсталлятора приложения**. Выберите MSI-пакет. Kaspersky Security Center укажет хеши исполняемых файлов, упакованных в этот MSI-пакет, в качестве условия добавления приложений в пользовательскую категорию.
- **Из KL-категории**. Укажите KL-категорию в качестве условия добавления приложений в пользовательскую категорию. *KL-категория* – сформированный специалистами "Лаборатории Касперского" список приложений, обладающих общими тематическими признаками. Например, KL-категория *Офисные приложения* включает в себя приложения из пакетов Microsoft Office, Adobe Acrobat и другие.

  Вы можете выбрать все KL-категории, чтобы сформировать расширенный список доверенных приложений.
- **Задайте путь к приложению (поддерживаются маски)**. Выберите папку на клиентском устройстве. Kaspersky Security Center добавит исполняемые файлы из этой папки в пользовательскую категорию.
- **Выберите сертификат из хранилища сертификатов**. Выберите сертификаты, которыми подписаны исполняемые файлы, в качестве условия добавления приложений в пользовательскую категорию.
- **Тип носителя**. Укажите тип запоминающего устройства (все жесткие и съемные диски или только съемные диски) в качестве условия добавления приложений в пользовательскую категорию.

Шаг 5. Параметры

Этот шаг доступен, если вы выбрали тип категории **Категория, в которую входят исполняемые файлы с выбранных устройств**.

На этом шаге нажмите на кнопку **Добавить** и укажите компьютеры, исполняемые файлы с которых Kaspersky Security Center добавит в категорию приложений. Kaspersky Security Center добавит в категорию приложений все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.

Также на этом шаге вы можете настроить следующие параметры:

- Алгоритм вычисления хеш-функции. Для выбора алгоритма необходимо установить хотя бы один из следующих флажков:
  - **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**.
  - **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**.
- Флажок **Синхронизировать данные с хранилищем Сервера администрирования**. Установите этот флажок, если вы хотите, чтобы Kaspersky Security Center периодически очищал категорию приложений и добавлял в нее все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.

  Если флажок **Синхронизировать данные с хранилищем Сервера администрирования** снят, то после создания категории приложений Kaspersky Security Center не будет вносить в нее изменения.

Шаг 6. Папка хранилища

Этот шаг доступен, если вы выбрали тип категории **Категория, в которую входят исполняемые файлы из указанной папки**.

На этом шаге укажите папку, в которой Kaspersky Security Center будет выполнять поиск исполняемых файлов для автоматического добавления в категорию приложений.

Также на этом шаге вы можете настроить следующие параметры:

- Флажок **Включать в категорию динамически подключаемые библиотеки (DLL)**. Установите этот флажок, если вы хотите, чтобы в категорию приложений включались динамически подключаемые библиотеки (файлы формата DLL).

  При включении файлов формата DLL в категорию приложений возможно снижение производительности работы Kaspersky Security Center.

- Флажок **Включать в категорию данные о скриптах**. Установите этот флажок, если вы хотите, чтобы в категорию приложений включались скрипты.

  При включении скриптов в категорию приложений возможно снижение производительности работы Kaspersky Security Center.

- Алгоритм вычисления хеш-функции. Для выбора алгоритма необходимо установить хотя бы один из следующих флажков:

  - **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**.

  - **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**.

- Флажок **Принудительно проверять папку на наличие изменений**. Установите этот флажок, если вы хотите, чтобы Kaspersky Security Center периодически выполнял поиск исполняемых файлов в папке автоматического пополнения категории приложений.

  Если флажок **Принудительно проверять папку на наличие изменений** снят, Kaspersky Security Center выполняет поиск исполняемых файлов в папке автоматического пополнения категории приложений, только если в этой папке были изменены, добавлены или удалены файлы.

- Поле **Период проверки (1–168 часов)**. В поле вы можете указать период времени в часах, по истечении которого Kaspersky Security Center выполняет поиск исполняемых файлов в папке автоматического пополнения категории приложений.

  Поле доступно, если установлен флажок **Принудительно проверять папку на наличие изменений**.

Шаг 7. Создание пользовательской категории

Завершите работу мастера.

Чтобы добавить новое условие срабатывания в правило Контроля приложений в интерфейсе приложения, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.

3. Нажмите на кнопку **Запрещенные приложения** или **Разрешенные приложения**.

   Откроется список правил Контроля приложений.

4. Выберите правило, для которого вы хотите добавить условие срабатывания.

   Откроются свойства правила Контроля приложений.

5. Перейдите на вкладку **Условия: N** или **Исключения: N** и нажмите на кнопку **Добавить**.

6. Выберите условия срабатывания правила Контроля приложений:

- **Условия из свойств запускавшихся приложений**. Вы можете выбрать приложения, к которым будет применено правило Контроля приложений, из списка запущенных приложений. Kaspersky Endpoint Security также добавляет в этот список приложения, которые когда-либо были запущены на компьютере. Вам нужно выбрать критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Хеш файла**, **Сертификат**, **KL-категория**, **Метаданные** или **Путь к файлу или папке**.

- **Условия "KL-категория"**. *KL-категория* – сформированный специалистами "Лаборатории Касперского" список приложений, обладающих общими тематическими признаками. Например, KL-категория "Офисные приложения" включает в себя приложения из пакетов Microsoft Office, Adobe® Acrobat® и другие.

- **Условие вручную**. Вы можете выбрать файл приложения и выбрать одно из условий срабатывания правила: **Хеш файла**, **Сертификат**, **Метаданные** или **Путь к файлу или папке**.

- **Условие по носителю файла (съемный диск)**. Правило Контроля приложений применяется только к файлам, которые запускаются на съемном диске.

- **Условия из свойств файлов указанной папки**. Правило Контроля приложений применяется только к файлам, которые расположены в указанной папке. Вы также можете включить или исключить файлы из вложенных папок. Вам нужно выбрать критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Хеш файла**, **Сертификат**, **KL-категория**, **Метаданные** или **Путь к файлу или папке**.

7. Сохраните внесенные изменения.

При добавлении условий учитывайте следующие особенности работы Контроля приложений:

- Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски в метаданных: **Имя файла**, **Название программы**, **Поставщик**.

- Kaspersky Endpoint Security не поддерживает MD5-хеш файла и не контролирует запуск приложений на основе MD5-хеша. В качестве условия срабатывания правила используется SHA256-хеш.

- Не рекомендуется использовать в качестве условий срабатывания правил только критерии **Издатель** и **Субъект сертификата**. Использование этих критериев является ненадежным.

- Если вы используете символьную ссылку в поле **Путь к файлу или папке**, рекомендуется развернуть символьную ссылку для корректной работы правила Контроля приложений. Для этого нажмите на кнопку **Развернуть символьную ссылку**.

Добавление в категорию приложений исполняемых файлов из папки Исполняемые файлы

В папке **Исполняемые файлы** отображается список исполняемых файлов, обнаруженных на компьютерах. Kaspersky Endpoint Security формирует список исполняемых файлов после выполнения задачи инвентаризации.

Чтобы добавить в категорию приложений исполняемые файлы из папки Исполняемые файлы, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите **Дополнительно → Управление приложениями → Исполняемые файлы**.
3. В рабочей области выберите исполняемые файлы, которые вы хотите добавить в категорию приложений.
4. По правой клавише мыши откройте контекстное меню для выбранных исполняемых файлов и выберите пункт **Добавить в категорию**.
5. В открывшемся окне выполните следующие действия:
   - В верхней части окна выберите один из следующих вариантов:
     - **Добавить в новую категорию приложений**. Выберите этот вариант, если вы хотите создать новую категорию приложений и добавить в нее исполняемые файлы.
     - **Добавить в существующую категорию**. Выберите этот вариант, если вы хотите выбрать существующую категорию приложений и добавить в нее исполняемые файлы.
   - В блоке **Тип правила** выберите один из следующих вариантов:
     - **Правила для добавления в область действия**. Выберите этот вариант, если вы хотите создать условия, добавляющие исполняемые файлы в категорию приложений.
     - **Правила для добавления в исключения**. Выберите этот вариант, если вы хотите создать условия, исключающие исполняемые файлы из категории приложений.
   - В блоке **Параметр, используемый в качестве условия** выберите один из следующих вариантов:
     - **Данные сертификата (или SHA256 для файлов без сертификата)**.
     - **Данные сертификата (файлы без сертификата пропускаются)**.
     - **Только SHA256 (файлы без SHA256 пропускаются)**.
     - **Только MD5 (для совместимости с Kaspersky Endpoint Security 10 Service Pack 1)**.
6. Сохраните внесенные изменения.

Добавление в категорию приложений исполняемых файлов, связанных с событиями

Чтобы добавить в категорию приложений исполняемые файлы, связанные с событиями Контроля приложений, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите вкладку **События**.

3. Выберите выборку событий о работе компонента Контроль приложений (Просмотр событий по результатам работы компонента Контроль приложений, Просмотр событий по результатам тестовой работы компонента Контроля приложений) в раскрывающемся списке **Выборки событий**.

4. Нажмите на кнопку **Запустить выборку**.

5. Выберите события, в связи с которыми вы хотите добавить в категорию приложений исполняемые файлы.

6. По правой клавише мыши откройте контекстное меню для выбранных событий и выберите пункт **Добавить в категорию**.

7. В открывшемся окне настройте параметры категории приложений:

   - В верхней части окна выберите один из следующих вариантов:

     - **Добавить в новую категорию программ**. Выберите этот вариант, если вы хотите создать новую категорию приложений и добавить в нее исполняемые файлы.

     - **Добавить в существующую категорию**. Выберите этот вариант, если вы хотите выбрать существующую категорию приложений и добавить в нее исполняемые файлы.

   - В блоке **Тип правила** выберите один из следующих вариантов:

     - **Правила для добавления в область действия**. Выберите этот вариант, если вы хотите создать условия, добавляющие исполняемые файлы в категорию приложений.

     - **Правила для добавления в исключения**. Выберите этот вариант, если вы хотите создать условия, исключающие исполняемые файлы из категории приложений.

   - В блоке **Параметр, используемый в качестве условия** выберите один из следующих вариантов:

     - **Данные сертификата (или SHA-256 для файлов без сертификата)**.

     - **Данные сертификата (файлы без сертификата пропускаются)**.

     - **Только SHA-256 (файлы без SHA-256 пропускаются)**.

     - **Только MD5 (для совместимости с Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Сохраните внесенные изменения.

Добавление правила Контроля приложений

Чтобы добавить правило Контроля приложений с помощью Kaspersky Security Center, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Контроль безопасности** → **Контроль приложений**.

   В правой части окна отобразятся параметры компонента Контроль приложений.

4. Нажмите на кнопку **Добавить**.

   Откроется окно **Правило Контроля приложений**.

5. Выполните одно из следующих действий:

   - Если вы хотите создать новую категорию, выполните следующие действия:

     a. Нажмите на кнопку **Создать категорию**.

        Запустится мастер создания пользовательской категории.

     b. Следуйте указаниям мастера создания пользовательской категории.

     c. Из раскрывающегося списка **Категория** выберите созданную категорию приложений.

   - Если вы хотите изменить существующую категорию, выполните следующие действия:

     a. Из раскрывающегося списка **Категория** выберите созданную категорию приложений, которую вы хотите изменить.

     b. Нажмите на кнопку **Свойства**.

     c. Измените параметры выбранной категории приложений.

     d. Сохраните внесенные изменения.

     e. Из раскрывающегося списка **Категория** выберите созданную категорию приложений, на основе которой вы хотите создать правило.

6. В таблице **Пользователи и их права** нажмите на кнопку **Добавить**.

   Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

7. В таблице **Пользователи и их права** выполните следующие действия:

   - Если вы хотите разрешить пользователям и / или группам пользователей запуск приложений, принадлежащих к выбранной категории, установите флажок **Разрешить** в нужных строках.

   - Если вы хотите запретить пользователям и / или группам пользователей запуск приложений, принадлежащих к выбранной категории, установите флажок **Запретить** в нужных строках.

8. Установите флажок **Запретить остальным пользователям**, если вы хотите, чтобы приложение запрещало запуск приложений, принадлежащих к выбранной категории, всем пользователям, которые не указаны в графе **Пользователь или группа** и не входят в группы пользователей, указанные в графе **Пользователь или группа**.

9. Установите флажок **Доверенные приложения обновления**, если вы хотите, чтобы приложения, входящие в выбранную категорию приложений, Kaspersky Endpoint Security считал доверенными приложения обновления с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

   При миграции параметров Kaspersky Endpoint Security осуществляется также миграция списка исполняемых файлов, созданных доверенными приложениями обновления.

10. Сохраните внесенные изменения.

Чтобы добавить правило Контроля приложений, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.
3. Нажмите на кнопку **Запрещенные приложения** или **Разрешенные приложения**.

   Откроется список правил Контроля приложений.

4. Нажмите на кнопку **Добавить**.

   Откроется окно с параметрами правила Контроля приложений.

5. На вкладке **Общие настройки** задайте основные параметры правила:

   a. В поле **Название правила** введите название правила.

   b. В поле **Описание** введите описание правила.

   c. В таблице **Пользователи и их права** нажмите на кнопку **Добавить**.

      Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

      По умолчанию действие правила распространяется на всех пользователей.

      Если в таблице не указан ни один пользователь, правило не может быть сохранено.

   d. В таблице **Пользователи и их права** определите право пользователей на запуск приложений с помощью переключателя.

   e. Установите флажок **Запретить остальным пользователям**, если вы хотите, чтобы приложение запрещало запуск приложений, удовлетворяющих условиям срабатывания правила, всем пользователям, которые не указаны в таблице **Пользователи и их права** и не входят в группы пользователей, указанные в таблице **Пользователи и их права**.

      Если флажок **Запретить остальным пользователям** снят, Kaspersky Endpoint Security не контролирует запуск приложений пользователями, которые не указаны в таблице **Пользователи и их права** и не входят в группы пользователей, указанные в таблице **Пользователи и их права**.

f. Установите флажок **Доверенные приложения обновления**, если вы хотите, чтобы приложения, удовлетворяющие условиям срабатывания правила, Kaspersky Endpoint Security считал доверенными приложения обновления. *Доверенные приложения обновления* – приложения с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

Если приложение соответствует условиям срабатывания нескольких правил, Kaspersky Endpoint Security устанавливает признак *Доверенные приложения обновления* при выполнении следующих требований:

- запуск приложения разрешен во всех правилах;
- хотя бы в одном правиле установлен флажок **Доверенные приложения обновления**.

6. На вкладке **Условия: N** сформируйте или измените список включающих условий срабатывания правила.
7. На вкладке **Исключения: N** сформируйте или измените список исключающих условий срабатывания правила.

   При миграции параметров Kaspersky Endpoint Security осуществляется также миграция списка исполняемых файлов, созданных доверенными приложениями обновления.
8. Сохраните внесенные изменения.

Изменение статуса правила Контроля приложений с помощью Kaspersky Security Center

Чтобы изменить статус правила Контроля приложений в Консоли администрирования, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Контроль приложений**.

   В правой части окна отобразятся параметры компонента Контроль приложений.
4. В графе **Статус** по левой клавише мыши откройте контекстное меню и выберите один из следующих пунктов:
   - **Вкл**. Статус означает, что правило используется во время работы компонента Контроль приложений.
   - **Выкл**. Статус означает, что правило не используется во время работы компонента Контроль приложений.
   - **Тест**. Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск приложений, на которые распространяется действие правила, но заносит информацию о запуске этих приложений в отчет.
5. Сохраните внесенные изменения.

Чтобы изменить статус правила Контроля приложений в интерфейсе приложения, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.
3. Нажмите на кнопку **Запрещенные приложения** или **Разрешенные приложения**.

   Откроется список правил Контроля приложений.
4. В графе **Статус** откройте контекстное меню и выберите один из следующих пунктов:
   - **Включено**. Статус означает, что правило используется во время работы компонента Контроль приложений.
   - **Выключено**. Статус означает, что правило не используется во время работы компонента Контроль приложений.
   - **Тестовый режим**. Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск приложений, на которые распространяется действие этого правила, но заносит информацию о запуске этих приложений в отчет.
5. Сохраните внесенные изменения.

Экспорт и импорт правил Контроля приложений

Вы можете экспортировать список правил Контроля приложений в файл в формате XML. Вы можете использовать функцию экспорта / импорта для резервного копирования списка правил Контроля приложений или для миграции списка на другой сервер.

Экспорт и импорт правил Контроля приложений имеет следующие особенности:

- Kaspersky Endpoint Security экспортирует список правил только для активного режима Контроля приложений. То есть, если Контроль приложений работает в режиме запрещенного списка, Kaspersky Endpoint Security экспортирует правила только для этого режима. Для экспорта списка правил для режима разрешенного списка вам нужно переключить режим и выполнить экспорт повторно.
- Kaspersky Endpoint Security использует категории приложений для работы правил Контроля приложений. При миграции списка правил Контроля приложений на другой сервер вам также нужно выполнить миграцию списка категорий приложений. Подробнее об экспорте / импорте категорий приложений см. в справке Kaspersky Security Center.

Как экспортировать / импортировать список правил Контроля приложений в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Контроль приложений**.

4. Для экспорта списка правил Контроля приложений выполните следующие действия:

   a. Выберите правила, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

      Если вы не выбрали ни одного правила, Kaspersky Endpoint Security экспортирует все правила.

   b. Нажмите на ссылку **Экспортировать**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список правил, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл.

5. Для импорта списка правил Контроля приложений выполните следующие действия:

   a. Нажмите на ссылку **Импортировать**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

   b. Откройте файл.

      Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

6. Сохраните внесенные изменения.

Как экспортировать / импортировать список правил Контроля приложений в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль приложений**.
5. В блоке **Режим работы** выберите список правил: списки запрещенных или разрешенных приложений.
6. Для экспорта списка правил выполните следующие действия:

   a. Выберите правила, которые вы хотите экспортировать.

   b. Нажмите на кнопку → **Экспортировать**.

      Kaspersky Endpoint Security экспортирует список правил в JSON-файл в папку для загрузки по умолчанию.

7. Для импорта списка правил выполните следующие действия:

   a. Нажмите на кнопку → **Импортировать**.

      В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список правил.

b. Откройте файл.

Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.

8. Сохраните внесенные изменения.

Просмотр событий по результатам работы компонента Контроль приложений

Чтобы просмотреть приходящие в Kaspersky Security Center события по результатам работы компонента Контроль приложений, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите вкладку **События**.
3. Нажмите на кнопку **Создать выборку**.
4. В открывшемся окне перейдите в раздел **События**.
5. Нажмите на кнопку **Очистить все**.
6. В таблице **События** установите флажок **Запуск приложения запрещен**.
7. Сохраните внесенные изменения.
8. В раскрывающемся списке **Выборки событий** выберите созданную выборку.
9. Нажмите на кнопку **Запустить выборку**.

Просмотр отчета о запрещенных приложениях

Чтобы просмотреть отчет о запрещенных приложениях, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите вкладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**.

   Запустится мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. На шаге **Выбор типа шаблона отчета** выберите **Другое → Отчет о запрещенных приложениях**.

   После завершения работы мастера создания шаблона отчета в таблице на вкладке **Отчеты** появится новый шаблон отчета.
5. Откройте отчет двойным щелчком мыши.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Тестирование правил Контроля приложений

Чтобы убедиться, что правила Контроля приложений не блокируют приложения, необходимые для работы, рекомендуется после создания правил включить тестирование правил Контроля приложений и проанализировать их работу. При включении тестирования правил Контроля приложений Kaspersky Endpoint Security не будет блокировать приложения, запуск которых запрещен Контролем приложений, но будет отправлять уведомления об их запуске на Сервер администрирования.

Для анализа работы правил Контроля приложений требуется изучить события по результатам работы компонента Контроль приложений, приходящие в Kaspersky Security Center. Если для всех приложений, которые необходимы для работы пользователю компьютера, отсутствуют события о запрете запуска в тестовом режиме, то созданы верные правила. В противном случае рекомендуется уточнить параметры созданных вами правил, создать дополнительные или удалить существующие правила.

По умолчанию Kaspersky Endpoint Security разрешает запуск всех приложений, кроме приложений, запрещенных правилами.

Включение и выключение тестирования правил Контроля приложений

Чтобы включить или выключить тестирование правил Контроля приложений в Kaspersky Security Center, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Контроль приложений**.

   В правой части окна отобразятся параметры компонента Контроль приложений.
4. В раскрывающемся списке **Режим контроля** выберите один из следующих элементов:

   - **Список запрещенных**. Если выбран этот вариант, Контроль приложений разрешает всем пользователям запуск любых приложений, кроме случаев, удовлетворяющих условиям запрещающих правил Контроля приложений.
   - **Список разрешенных**. Если выбран этот вариант, Контроль приложений запрещает всем пользователям запуск любых приложений, кроме случаев, удовлетворяющих условиям разрешающих правил Контроля приложений.
5. Выполните одно из следующих действий:

   - Если вы хотите включить тестирование правил Контроля приложений, в раскрывающемся списке **Действие** выберите элемент **Тестировать правила**.
   - Если вы хотите включить Контроль приложений для управления запуском приложений на компьютерах пользователей, в раскрывающемся списке выберите элемент **Применять правила**.
6. Сохраните внесенные изменения.

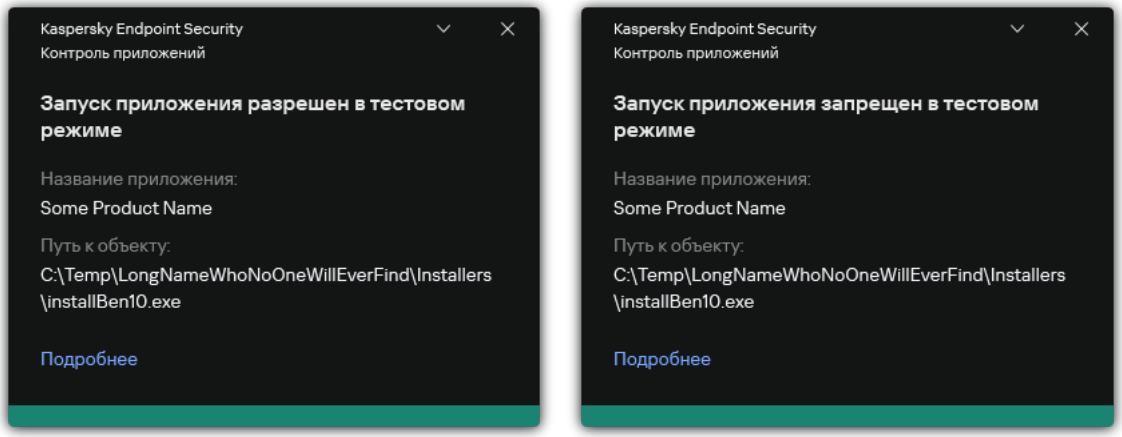
Чтобы включить тестирование правил Контроля приложений или выбрать блокирующее действие Контроля приложений, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.
3. Нажмите на кнопку **Запрещенные приложения** или **Разрешенные приложения**.

   Откроется список правил Контроля приложений.
4. В графе **Статус** выберите пункт **Тестовый режим**.

   Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск приложений, на которые распространяется действие этого правила, но заносит информацию о запуске этих приложений в отчет.
5. Сохраните внесенные изменения.

Kaspersky Endpoint Security не будет блокировать приложения, запуск которых запрещен компонентом Контроль приложений, но будет отправлять уведомления об их запуске на Сервер администрирования. Также вы можете настроить отображение уведомлений о тестировании правил на компьютере пользователя (см. рис. ниже).



Уведомления Контроля приложений в тестовом режиме

Просмотр отчета о запрещенных приложениях в тестовом режиме

Чтобы просмотреть отчет о запрещенных приложениях в тестовом режиме, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите вкладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**.

   Запустится мастер создания шаблона отчета.

4. Следуйте указаниям мастера создания шаблона отчета. На шаге **Выбор типа шаблона отчета** выберите **Другое → Отчет о запрещенных программах в тестовом режиме**.

   После завершения работы мастера создания шаблона отчета в таблице на вкладке **Отчеты** появится новый шаблон отчета.

5. Откройте отчет двойным щелчком мыши.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Просмотр событий по результатам тестовой работы компонента Контроля приложений

Чтобы просмотреть приходящие на Kaspersky Security Center события по результатам тестовой работы компонента Контроль приложений, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите вкладку **События**.
3. Нажмите на кнопку **Создать выборку**.
4. В открывшемся окне перейдите в раздел **События**.
5. Нажмите на кнопку **Очистить все**.
6. В таблице **События** установите флажки **Запуск приложения запрещен в тестовом режиме** и **Запуск приложения разрешен в тестовом режиме**.
7. Сохраните внесенные изменения.
8. В раскрывающемся списке **Выборки событий** выберите созданную выборку.
9. Нажмите на кнопку **Запустить выборку**.

Мониторинг активности приложений

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов.

Мониторинг активности приложений – это инструмент, предназначенный для просмотра информации об активности приложений на компьютере пользователя в режиме реального времени.

Для работы Мониторинга активности приложений вам нужно установить компоненты Контроль приложений и Предотвращение вторжений. Если эти компоненты не установлены, в главном окне приложения раздел Мониторинг активности приложений скрыт.

Чтобы запустить Мониторинг активности приложений,

в главном окне приложения в разделе **Мониторинг** нажмите на плитку **Мониторинг активности приложений**.

В открывшемся окне информация об активности приложений на компьютере пользователя представлена на трех вкладках:

- На вкладке **Все приложения** отображается информация о всех приложениях, установленных на компьютере.
- На вкладке **Работающие** отображается информация о потреблении ресурсов компьютера каждого из приложений в режиме реального времени. На этой вкладке вы можете, а также перейти к настройке разрешений для отдельного приложения.
- На вкладке **Запускаемые при старте** отображается список приложений, которые запускаются при старте операционной системы.

Если вы хотите скрыть данные об активности приложений на компьютере пользователя, вы можете ограничить доступ пользователя к инструменту Мониторинг активности приложений.

Как скрыть Мониторинг активности приложений в интерфейсе приложения через Консоль администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Интерфейс**.
4. Используйте флажок **Скрыть раздел Мониторинг активности приложений**, чтобы включить или выключить доступ к инструменту.
5. Сохраните внесенные изменения.

Как скрыть Мониторинг активности приложений в интерфейсе приложения через Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Взаимодействие с пользователем**.
5. Используйте флажок **Скрыть раздел Мониторинг активности приложений**, чтобы включить или выключить доступ к инструменту.
6. Сохраните внесенные изменения.

Правила формирования масок имен файлов или папок

Маска имени файла или папки – это представление имени папки или имени и расширения файла с использованием общих символов.

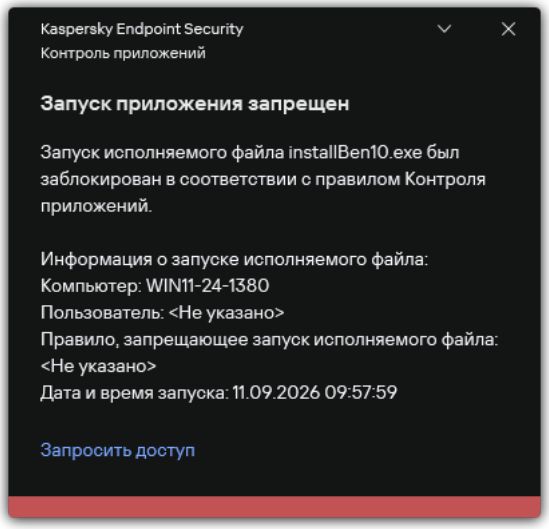
Для формирования маски имени файла или папки вы можете использовать следующие общие символы:

- Символ `*`, который заменяет любой набор символов, в том числе пустой. Например, маска `C:\*.txt` будет включать все пути к файлам с расширением `txt`, расположенным в папках и подпапках на диске (C:).

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Изменение шаблонов сообщений Контроля приложений

Когда пользователь пытается запустить приложение, запрещенное правилом Контроля приложений, Kaspersky Endpoint Security выводит сообщение о блокировке запуска приложения. Специалисты "Лаборатории Касперского" составили шаблон сообщения пользователю, которое описывает причины блокировки приложения (см. рис. ниже). Для работы с шаблонами сообщений предусмотрены специальные переменные (например, `%USER_NAME%`). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров. При формировании сообщения Kaspersky Endpoint Security определяет значение переменной из настроек операционной системы и подставляет это значение в сообщение, соответствующие конкретному компьютеру, пользователю и событию.



Уведомление Контроля приложений

Если блокировка запуска приложения, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить сообщение администратору локальной сети организации. Для этого пользователю нужно нажать на кнопку **Запросить доступ** и отправить администратору сообщение с описанием ситуации. Вы также можете подготовить шаблон сообщения администратору и добавить в текст сообщения данные, которые могут быть вам нужны для принятия решения о разрешении доступа к приложению. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете запуска приложения**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

Как изменить шаблон сообщений Контроля приложения в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Контроль приложений**.
4. В блоке **Настройки шаблонов сообщений** нажмите на кнопку **Шаблоны**.
5. В открывшемся окне настройте шаблоны сообщений Контроля приложений:

   - **Сообщение о блокировке**. Шаблон сообщения, которое появляется при срабатывании правила Контроля приложений, блокирующего запуск приложения.

     Настроить шаблоны сообщения для Контроля приложений в тестовом режиме невозможно. Контроль приложений в тестовом режиме показывает предустановленные уведомления.

   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка приложения, по мнению пользователя, произошла ошибочно.

   Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Переменная** и выберите нужную переменную из списка доступных.

   Также вы можете восстановить текст шаблона по умолчанию с помощью кнопки **По умолчанию**.

6. Сохраните внесенные изменения.

Как изменить шаблон сообщений Контроля приложения в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль приложений**.

5. В блоке **Шаблоны сообщений** перейдите по ссылке **Сообщение о запрете запуска приложения** и настройте шаблоны сообщений Контроля приложений:

   - **Сообщение пользователю**. Шаблон сообщения, которое появляется при срабатывании правила Контроля приложений, блокирующего запуск приложения.

     Настроить шаблоны сообщения для Контроля приложений в тестовом режиме невозможно. Контроль приложений в тестовом режиме показывает предустановленные уведомления.

   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка приложения, по мнению пользователя, произошла ошибочно.

   Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Добавить переменную** и выберите нужную переменную из списка доступных.

   Также вы можете восстановить текст шаблона по умолчанию с помощью кнопки **Восстановить по умолчанию**.

6. Сохраните внесенные изменения.

Как изменить шаблон сообщений Контроля приложения в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль приложений**.

3. В блоке **Шаблоны сообщений о блокировке приложений** настройте шаблоны сообщений Контроля приложений:

   - **Сообщение о блокировке**. Шаблон сообщения, которое появляется при срабатывании правила Контроля приложений, блокирующего запуск приложения.

     Настроить шаблоны сообщения для Контроля приложений в тестовом режиме невозможно. Контроль приложений в тестовом режиме показывает предустановленные уведомления.

   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка приложения, по мнению пользователя, произошла ошибочно.

   Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Добавить переменную** и выберите нужную переменную из списка доступных.

   Также вы можете восстановить текст шаблона по умолчанию с помощью кнопки **Сбросить**.

4. Сохраните внесенные изменения.

Переменные в шаблонах сообщений Контроля приложений

В шаблонах сообщений пользователю или администратору вы можете использовать следующие переменные:

- **Название сработавшего правила** – `%RULE%`.

  Название правила, в соответствии с которым заблокирован запуск исполняемого файла.

- **Текущая дата** – `%DATE%`.

  Дата блокировки запуска исполняемого файла в формате ДД.ММ.ГГГГ.

- **Текущее время** – `%TIME%`.

  Время блокировки запуска исполняемого файла в формате в формате ЧЧ:ММ.

- **Имя пользователя** – `%USER_NAME%`.

  Имя текущей учетной записи компьютера, на котором заблокирован исполняемый файл, в формате `<device name>\<user alias>` (например, `DESKTOP-123\John.Smith`).

- **Название компьютера** – `%COMPUTER_NAME%`.

  Название компьютера, на котором заблокирован запуск исполняемого файла.

- **Название исполняемого файла** – `%FILE_NAME%`.

  Название исполняемого файла заблокированного приложения.

- **KL-категория исполняемого файла** – `%KL_CAT%`.

  KL-категория, к которой относится заблокированное приложение (например, *Браузеры* или другая категория).

- **Путь к исполняемому файлу** – `%FILE_PATH%`.

  Полный путь к исполняемому файлу заблокированного приложения.

- **Версия исполняемого файла** – `%FILE_VERSION%`.

  Версия исполняемого файла заблокированного приложения.

- **Исходное название исполняемого файла** – `%ORIGINAL_FILE_NAME%`.

  Исходное название исполняемого файла заблокированного приложения. Название файла указано в свойствах исполняемого файла приложения.

- **Производитель** – `%FILE_PUBLISHER%`.

  Название производителя заблокированного приложения.

- **Название приложения** – `%FILE_PRODUCT_NAME%`.

  Название заблокированного приложения.

- **Версия приложения** – `%PRODUCT_VERSION%`.

  Версия заблокированного приложения.

- **Хеш исполняемого файла** – `%FILE_HASH%`.

  Хеш исполняемого файла заблокированного приложения.

- **Издатель сертификата** – `%CERT_ISSUER%`.

  Издатель сертификата, которым подписан исполняемый файл.

- **Субъект сертификата** – `%CERT_SUBJECT%`.

  Субъект сертификата, которым подписан исполняемый файл.

- **Отпечаток сертификата** – `%CERT_THUMBPRINT%`.

  Отпечаток сертификата, которым подписан исполняемый файл.

Лучшие практики инвентаризации исполняемых файлов

Задача *Инвентаризация* предназначена для получения данных об исполняемых файлах (EXE, BAT, CMD и т.п.), DLL-модулях и скриптах (PowerShell, JS и другие). Эти данные нужны для формирования категорий Контроля приложений и настройки прав приложений для компонента Предотвращение вторжений. Задачу *Инвентаризация* следует запускать регулярно для поддержания данных в актуальном состоянии. Задача *Инвентаризация*, как и задача *Поиск вредоносного ПО*, требует ресурсов компьютера. Поэтому мы рекомендуем настроить запуск задачи ночью или в выходные дни.

Этапы инвентаризации исполняемых файлов

1. Выберите группу эталонных компьютеров, на которых установлен типовой набор программного обеспечения. Мы рекомендуем свести к минимуму количество компьютеров для инвентаризации исполняемых файлов. Чем меньше задач *Инвентаризация*, тем меньше нагрузка на Сервер администрирования Kaspersky Security Center.

2. Переместите эталонные компьютеры в отдельную группу администрирования к консоли Kaspersky Security Center. Вы можете назвать группу, например, *Эталонные компьютеры*.

3. Создайте задачу *Инвентаризация* для группы администрирования *Эталонные компьютеры*. Мы рекомендует оставить параметры задачи по умолчанию.

Пример инвентаризации исполняемых файлов в организации

Например, в вашей организации 100 компьютеров с установленной операционной системой Windows 11 25H2. На всех компьютерах развернута операционной системы одного выпуска и одной локализации. Также на компьютерах установлен один набор обновлений.

В такой организации нет необходимости запускать задачу *Инвентаризация* на всех компьютерах. Большинство исполняемых файлов на этих компьютерах идентичны. Достаточно создать задачу для одного эталонного компьютера. Вы можете создать дополнительные задачи *Инвентаризация* для компьютеров с нетипичной конфигурацией.

Лучшие практики по внедрению режима списка разрешенных приложений

При планировании внедрения режима списка разрешенных приложений рекомендуется выполнить следующие действия:

1. Произвести следующие виды группировок:

   - Группы пользователей. Группы пользователей, для которых необходимо разрешить использование различных наборов приложений.

   - Группы администрирования. Одна или несколько групп компьютеров, к которым Kaspersky Security Center будет применять режим списка разрешенных приложений. Создание нескольких групп компьютеров необходимо, если для этих групп используются различные параметры режима списка разрешенных.

2. Составить список приложений, запуск которых необходимо разрешить.

   Перед составлением списка рекомендуется выполнить следующие действия:

   a. Запустить задачу инвентаризации.

      Информация о создании, изменении параметров и запуске задачи инвентаризации доступна в разделе Управление задачами.

   b. Просмотреть список исполняемых файлов.

Настройка режима списка разрешенных приложений

При настройке режима списка разрешенных приложений рекомендуется выполнить следующие действия:

1. Создать категории приложений, содержащие те приложения, запуск которых необходимо разрешить.

   Вы можете выбрать один из следующих способов формирования категорий приложений:

   - **Пополняемая вручную категория**. Вы можете вручную пополнять эту категорию, используя следующие условия:

     - Метаданные файла. Kaspersky Security Center добавляет в категорию приложений все исполняемые файлы, сопровождающиеся указанными метаданными.

     - Хеш файла. Kaspersky Security Center добавляет в категорию приложений все исполняемые файлы, имеющие указанный хеш.

       Использование этого условия исключает возможность автоматической установки обновлений, поскольку файлы различных версий будут иметь различный хеш.

     - Сертификат файла. Kaspersky Security Center добавляет в категорию приложений все исполняемые файлы, подписанные указанным сертификатом.

- KL-категория. Kaspersky Security Center добавляет в категорию приложений все приложения, входящие в указанную KL-категорию.

- Папка приложения. Kaspersky Security Center добавляет в категорию приложений все исполняемые файлы из этой папки.

  Использование условия **Папка приложения** небезопасно, поскольку запуск любого приложения из указанной папки будет разрешен. Правила, использующие категории приложений с условием **Папка приложения**, рекомендуется применять только к тем пользователям, для которых необходимо разрешить автоматическую установку обновлений.

- **Категория, в которую входят исполняемые файлы из указанной папки**. Вы можете указать папку, исполняемые файлы из которой будут автоматически попадать в создаваемую категорию приложений.

- **Категория, в которую входят исполняемые файлы с выбранных устройств**. Вы можете указать компьютер, все исполняемые файлы которого будут автоматически попадать в создаваемую категорию приложений.

  При использовании этого способа формирования категорий приложений Kaspersky Security Center получает информацию о приложениях на компьютере из папки **Исполняемые файлы**.

2. Выбрать режим списка разрешенных приложений для компонента Контроль приложений.

3. Создать правила Контроля приложений с использованием созданных категорий приложений.

   Для режима Список разрешенных приложений изначально заданы правила **Приложения ОС** и **Доверенные приложения обновления**. Эти правила Контроля приложений соответствуют KL-категориям. В KL-категорию *Приложения ОС* входят приложения, обеспечивающие нормальную работу операционной системы. В KL-категорию *Доверенные приложения обновления* входят приложения обновления наиболее известных производителей программного обеспечения. Вы не можете удалить эти правила. Параметры этих правил недоступны для изменения. По умолчанию правило **Приложения ОС** включено, а правило **Доверенные приложения обновления** выключено. Запуск приложений, соответствующих условиям срабатывания этих правил, разрешен всем пользователям.

4. Определить те приложения, для которых необходимо разрешить автоматическую установку обновлений.

   Вы можете разрешить автоматическую установку обновлений одним из следующих способов:

   - Указать расширенный список разрешенных приложений, разрешив запуск всех приложений, входящих в любую из KL-категорий.

   - Указать расширенный список разрешенных приложений, разрешив запуск всех приложений, подписанных сертификатами.

     Чтобы разрешить запуск всех приложений, подписанных сертификатами, вы можете создать категорию с условием на основе сертификата, в котором используется только параметр **Субъект** со значением `*`.

- Для правила Контроля приложений установить параметр **Доверенные приложения обновления**. Если этот флажок установлен, то Kaspersky Endpoint Security будет считать приложения, входящие в правило, доверенными приложениями обновления. Kaspersky Endpoint Security разрешает запуск приложений, которые были установлены или обновлены приложениями, входящими в правило. При этом приложения не должны попадать под действие запрещающих правил.

  При миграции параметров Kaspersky Endpoint Security осуществляется также миграция списка исполняемых файлов, созданных доверенными приложениями обновления.

- Создать папку и поместить в нее исполняемые файлы приложений, для которых вы хотите разрешить автоматическую установку обновлений. Далее создать категорию приложений с условием **Папка приложения** и указать путь к этой папке. Далее создать разрешающее правило и выбрать эту категорию.

  Использование условия **Папка приложения** небезопасно, поскольку запуск любого приложения из указанной папки будет разрешен. Правила, использующие категории приложений с условием **Папка приложения**, рекомендуется применять только к тем пользователям, для которых необходимо разрешить автоматическую установку обновлений.

Тестирование режима списка разрешенных приложений

Чтобы убедиться, что правила Контроля приложений не блокируют приложения, необходимые для работы, рекомендуется после создания правил включить тестирование правил Контроля приложений и проанализировать их работу. При включении тестирования Kaspersky Endpoint Security не будет блокировать приложения, запуск которых запрещен правилами Контроля приложений, но будет отправлять уведомления об их запуске на Сервер администрирования.

При тестировании режима списка разрешенных приложений рекомендуется выполнить следующие действия:

1. Определить период тестирования (от нескольких дней до двух месяцев).
2. Включить тестирование правил Контроля приложений.
3. Проанализировать результаты тестирования, используя события по результатам тестовой работы компонента Контроль приложений и отчеты о запрещенных приложениях в тестовом режиме.
4. По результатам анализа внести изменения в параметры режима списка разрешенных приложений.

   В частности, по результатам тестирования вы можете добавить в категорию приложений исполняемые файлы, связанные с событиями.

Поддержка режима списка разрешенных приложений

После выбора блокирующего действия Контроля приложений рекомендуется продолжать поддержку режима списка разрешенных приложений, выполняя следующие действия:

- Анализировать работу правил Контроля приложений, используя события по результатам работы Контроля приложений и отчеты о запрещенных запусках.
- Анализировать запросы доступа к приложениям, получаемые от пользователей.

- Анализировать незнакомые исполняемые файлы, проверяя их репутацию в Kaspersky Security Network.
- Перед установкой обновлений для операционной системы или для программного обеспечения устанавливать эти обновления на тестовой группе компьютеров, чтобы проверить, как они будут обрабатываться правилами Контроля приложений.
- Добавлять необходимые приложения в категории, используемые в правилах Контроля приложений.

Контроль сетевых портов

Во время работы Kaspersky Endpoint Security компоненты Веб-Контроль, Защита от почтовых угроз, Защита от веб-угроз, Анализ поведения, Защита от эксплойтов контролируют потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP- и UDP-порты компьютера пользователя. Например, компонент Защита от почтовых угроз анализирует информацию, передаваемую по SMTP-протоколу, а компонент Защита от веб-угроз анализирует информацию, передаваемую по протоколам HTTP и FTP.

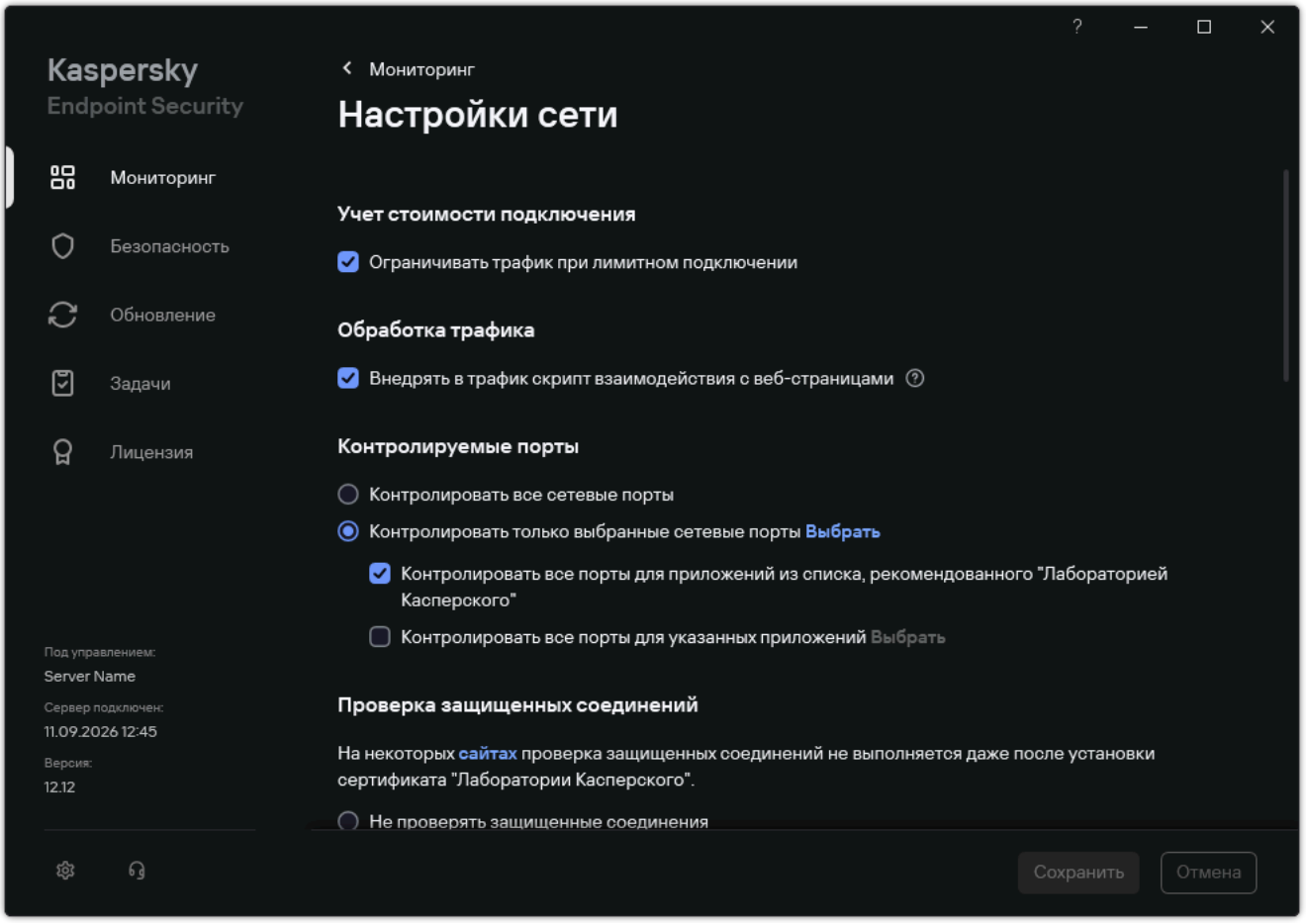
Kaspersky Endpoint Security подразделяет TCP- и UDP-порты компьютера пользователя на несколько групп в соответствии с вероятностью их взлома. Сетевые порты, отведенные для уязвимых служб, рекомендуется контролировать более тщательно, так как эти сетевые порты с большей вероятностью могут являться целью сетевой атаки. Если вы используете нестандартные службы, которым отведены нестандартные сетевые порты, эти сетевые порты также могут являться целью для атакующего компьютера. Вы можете задать список сетевых портов и список приложений, запрашивающих сетевой доступ, на которые компоненты Защита от почтовых угроз и Защита от веб-угроз должны обращать особое внимание во время слежения за сетевым трафиком.

Компоненты Анализ поведения и Защита от эксплойтов также контролируют потоки данных через сетевые порты для обеспечения безопасности компьютера. Компоненты постоянно контролируют сетевой трафик для отдельных процессов, которые могут представлять угрозу.

Включение контроля всех сетевых портов

Чтобы включить контроль всех сетевых портов, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.



Параметры контроля сетевых портов

3. В блоке **Контролируемые порты** выберите вариант **Контролировать все сетевые порты**.
4. Сохраните внесенные изменения.

Формирование списка контролируемых сетевых портов

Чтобы сформировать список контролируемых сетевых портов, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.

4. Нажмите на кнопку **Выбрать**.

   Откроется список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика. Этот список сетевых портов включен в поставку Kaspersky Endpoint Security.

5. Используйте переключатель в графе **Статус**, чтобы включить или выключить контроль сетевых портов.

6. Если сетевой порт отсутствует в списке сетевых портов, добавьте его следующим образом:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне введите номер сетевого порта и короткое описание.

   c. Установите статус контроля сетевого порта **Активно** или **Неактивно**.

7. Сохраните внесенные изменения.

При работе протокола FTP в пассивном режиме соединение может устанавливаться через случайный сетевой порт, который не добавлен в список контролируемых сетевых портов. Чтобы защищать такие соединения, включите контроль всех сетевых портов или настройте контроль сетевых портов для приложений, с помощью которых устанавливается FTP-соединение.

Формирование списка приложений, для которых контролируются все сетевые порты

Вы можете сформировать список приложений, для которых Kaspersky Endpoint Security контролирует все сетевые порты.

В список приложений, для которых Kaspersky Endpoint Security контролирует все сетевые порты, рекомендуется включить приложения, которые принимают или передают данные по протоколу FTP.

Чтобы сформировать список приложений, для которых контролируются все сетевые порты, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки сети**.

3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.

4. Установите флажок **Контролировать все порты для приложений из списка, рекомендованного "Лабораторией Касперского"**.

   Если установлен этот флажок, приложение Kaspersky Endpoint Security контролирует все порты для следующих приложений:

   - Adobe Acrobat Reader.
   - Apple Application Support.
   - Google Chrome.

- Microsoft Edge.
- Mozilla Firefox.
- Internet Explorer.
- Java.
- mIRC.
- Opera.
- Pidgin.
- Safari.
- Агент Mail.ru.
- Яндекс.Браузер.

5. Установите флажок **Контролировать все порты для указанных приложений**.
6. Нажмите на кнопку **Выбрать**.

   Откроется список приложений, сетевые порты которых контролирует Kaspersky Endpoint Security.
7. Используйте переключатель в графе **Статус**, чтобы включить или выключить контроль сетевых портов.
8. Если приложение отсутствует в списке приложений, добавьте ее следующим образом:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне укажите путь к исполняемому файлу приложения и короткое описание.

   c. Установите статус контроля сетевых портов **Активно** или **Неактивно**.
9. Сохраните внесенные изменения.

Экспорт и импорт списков контролируемых портов

Для контроля сетевых портов Kaspersky Endpoint Security использует следующие списки: список сетевых портов и список приложений, порты которых контролирует Kaspersky Endpoint Security. Вы можете экспортировать списки контролируемых портов в файл в формате XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество портов с одинаковым описанием. Также вы можете использовать функцию экспорта / импорта для резервного копирования списков контролируемых портов или для миграции списков на другой сервер.

Как экспортировать / импортировать списки контролируемых портов в Консоли администрирования (MMC)

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки → Настройки сети**.

5. Для экспорта списка сетевых портов выполните следующие действия:

   a. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.

   b. Перейдите по ссылке **Выбрано N портов**.

      Откроется окно **Сетевые порты**. В окне **Сетевые порты** находится список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика. Этот список сетевых портов включен в поставку Kaspersky Endpoint Security.

   c. В списке сетевых портов выберите порты, которые вы хотите экспортировать.

   d. Нажмите на кнопку **Экспорт**.

   e. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список сетевых портов, а также выберите папку, в которой вы хотите сохранить этот файл.

   f. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список сетевых портов в XML-файл.

6. Для экспорта списка приложений, порты которых контролирует Kaspersky Endpoint Security, выполните следующие действия:

   a. В блоке **Контролируемые порты** установите флажок **Контролировать все порты для указанных приложений**.

   b. Перейдите по ссылке **Выбрано N приложений**.

   c. В списке приложений выберите приложения, которые вы хотите экспортировать.

   d. Нажмите на кнопку **Экспорт**.

   e. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список приложений, а также выберите папку, в которой вы хотите сохранить этот файл.

   f. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список приложений в XML-файл.

7. Для импорта списка сетевых портов выполните следующие действия:

   a. В списке сетевых портов нажмите на кнопку **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список сетевых портов.

   b. Откройте файл.

      Если на компьютере уже есть список сетевых портов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

8. Для импорта списка приложений, порты которых контролирует Kaspersky Endpoint Security, выполните следующие действия:

   a. В списке приложений нажмите на кнопку **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список приложений.

   b. Откройте файл.

      Если на компьютере уже есть список приложений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

9. Сохраните внесенные изменения.

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Общие настройки** → **Настройки сети**.

4. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.

5. Нажмите на кнопку **Настройка**.

   Откроется окно **Сетевые порты**. В окне **Сетевые порты** находится список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика. Этот список сетевых портов включен в поставку Kaspersky Endpoint Security.

6. Для экспорта списка сетевых портов выполните следующие действия:

   a. В списке сетевых портов выберите порты, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

      Если вы не выбрали ни одного порта, Kaspersky Endpoint Security экспортирует все порты.

   b. Нажмите на кнопку **Экспортировать**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список сетевых портов, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список сетевых портов в XML-файл.

7. Для экспорта списка приложений, порты которых контролирует Kaspersky Endpoint Security, выполните следующие действия:

   a. Установите флажок **Контролировать все порты для указанных приложений**.

   b. В списке приложений выберите приложения, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

      Если вы не выбрали ни одного приложения, Kaspersky Endpoint Security экспортирует все приложения.

   c. Нажмите на кнопку **Экспортировать**.

   d. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список приложений, а также выберите папку, в которой вы хотите сохранить этот файл.

e. Сохраните файл.

Kaspersky Endpoint Security экспортирует список приложений в XML-файл.

8. Для импорта списка сетевых портов выполните следующие действия:

a. В списке сетевых портов нажмите на кнопку **Импортировать**.

В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список сетевых портов.

b. Откройте файл.

Если на компьютере уже есть список сетевых портов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

9. Для импорта списка приложений, порты которых контролирует Kaspersky Endpoint Security, выполните следующие действия:

a. В списке приложений нажмите на кнопку **Импортировать**.

В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список приложений.

b. Откройте файл.

Если на компьютере уже есть список приложений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

10. Сохраните внесенные изменения.

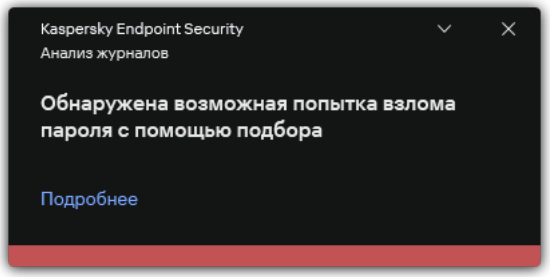
Анализ журналов

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций.

Анализ журналов контролирует целостность защищаемой среды на основе журналов событий Windows. При обнаружении признаков нетипичного поведения в системе приложение информирует администратора, так как это поведение может указывать на попытки кибератак.

Kaspersky Endpoint Security анализирует журналы событий Windows и выявляет нарушения в соответствии с правилами. В компонент включены предустановленные правила. Для работы предустановленных правил приложение использует эвристический анализ. Также вы можете добавить собственные правила (пользовательские правила). При срабатывании правила, приложение создает событие со статусом *Критическое* (см. рис. ниже).

Для работы Анализа журналов убедитесь, что параметры политики аудита безопасности настроены и система регистрирует нужные события (подробнее см. на сайте Службы технической поддержки Microsoft).



Уведомление Анализа журналов

Настройка предустановленных правил

Предустановленные правила включают шаблоны аномальной активности на защищаемом компьютере. Аномальная активность может являться признаком попытки атаки. Для работы предустановленных правил приложение использует эвристический анализ. Для Анализа журналов доступно семь предустановленных правил. Вы можете включать и выключать любые правила. Удалить предустановленные правила невозможно.

Вы можете настроить критерии срабатывания правил, которые контролируют события для следующих операций:

- обработка подбора пароля;
- обработка сетевого входа.

Как настроить предустановленные правила в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Анализ журналов**.
4. Убедитесь, что флажок **Анализ журналов** установлен.
5. В блоке **Предустановленные правила** нажмите на кнопку **Настройка**.
6. Настройте работу предустановленных правил с помощью флажков:
   - **Обнаружена возможная попытка взлома пароля с помощью подбора**.
   - **Обнаружена подозрительная активность во время сетевого сеанса входа**.

- **Обнаружены признаки компрометации журналов Windows**.
- **Обнаружена подозрительная активность со стороны новой установленной службы**.
- **Обнаружена подозрительная аутентификация с явным указанием учетных данных**.
- **Обнаружены признаки атаки Kerberos forged PAC (MS14-068)**.
- **Обнаружены подозрительные изменения привилегированной группы Администраторы**.

7. Если требуется, настройте параметры правила **Обнаружена возможная попытка взлома пароля с помощью подбора**:
   a. Нажмите на кнопку **Настройка** под правилом.
   b. В открывшемся окне укажите количество попыток и промежуток времени, в течение которого выполнялись попытки ввода пароля, для срабатывания правила.
   c. Нажмите на кнопку **OK**.
8. Если вы выбрали правило **Обнаружена подозрительная активность во время сетевого сеанса входа**, вам нужно настроить параметры правила:
   a. Нажмите на кнопку **Настройка** под правилом.
   b. В блоке **Обработка атипичной аутентификации** укажите начало и конец временного интервала.
      Kaspersky Endpoint Security будет считать аномальной активностью выполненные попытки входа в течение заданного интервала.
      По умолчанию интервал не задан и приложение не контролирует попытки входа. Чтобы приложение постоянно контролировало попытки входа, задайте интервал 12:00 AM – 11:59 PM. Начало и конец интервала не должны совпадать. Если они совпадают, приложение не контролирует попытки входа.
   c. Сформируйте списки доверенных пользователей и доверенных IP-адресов компьютеров (IPv4 и IPv6).
      Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно. Kaspersky Endpoint Security не будет контролировать попытки входа для этих пользователей и компьютеров.
   d. Нажмите на кнопку **OK**.
9. Сохраните внесенные изменения.

Как настроить предустановленные правила в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности → Анализ журналов**.
5. Убедитесь, что переключатель **Анализ журналов ВКЛЮЧЕН** включен.

6. В блоке **Предустановленные правила** настройте работу предустановленных правил с помощью переключателей:

   - **Обнаружена возможная попытка взлома пароля с помощью подбора**.
   - **Обнаружена подозрительная активность во время сетевого сеанса входа**.
   - **Обнаружены признаки компрометации журналов Windows**.
   - **Обнаружена подозрительная активность со стороны новой установленной службы**.
   - **Обнаружена подозрительная аутентификация с явным указанием учетных данных**.
   - **Обнаружены признаки атаки Kerberos forged PAC (MS14-068)**.

   a. **Обнаружены подозрительные изменения привилегированной группы Администраторы**.

7. Если требуется, настройте параметры правила **Обнаружена возможная попытка взлома пароля с помощью подбора**:

   a. Нажмите **Настройки** под правилом.

   b. В открывшемся окне укажите количество попыток и промежуток времени, в течение которого выполнялись попытки ввода пароля, для срабатывания правила.

   c. Нажмите на кнопку **OK**.

8. Если вы выбрали правило **Обнаружена подозрительная активность во время сетевого сеанса входа**, вам нужно настроить параметры правила:

   a. Нажмите **Настройки** под правилом.

   b. В блоке **Обнаружение входа в сеть** укажите начало и конец временного интервала.

   Kaspersky Endpoint Security будет считать аномальной активностью выполненные попытки входа в течение заданного интервала.

   По умолчанию интервал не задан и приложение не контролирует попытки входа. Чтобы приложение постоянно контролировало попытки входа, задайте интервал 12:00 AM – 11:59 PM. Начало и конец интервала не должны совпадать. Если они совпадают, приложение не контролирует попытки входа.

   c. В блоке **Исключения** добавьте доверенных пользователей и доверенные IP-адреса компьютеров (IPv4 и IPv6).

   Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно. Kaspersky Endpoint Security не будет контролировать попытки входа для этих пользователей и компьютеров.

   d. Нажмите на кнопку **OK**.

9. Сохраните внесенные изменения.

Как настроить предустановленные правила в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Анализ журналов**.
3. Убедитесь, что переключатель **Анализ журналов** включен.
4. В блоке **Предустановленные правила** нажмите на кнопку **Настроить**.
5. Настройте работу предустановленных правил с помощью флажков:
   - **Обнаружена возможная попытка взлома пароля с помощью подбора**.
   - **Обнаружена подозрительная активность во время сетевого сеанса входа**.
   - **Обнаружены признаки компрометации журналов Windows**.
   - **Обнаружена подозрительная активность со стороны новой установленной службы**.
   - **Обнаружена подозрительная аутентификация с явным указанием учетных данных**.
   - **Обнаружены признаки атаки Kerberos forged PAC (MS14-068)**.

   a. **Обнаружены подозрительные изменения привилегированной группы Администраторы**.
6. Если требуется, настройте параметры правила **Обнаружена возможная попытка взлома пароля с помощью подбора**:
   a. Нажмите **Настройка** под правилом.
   b. В открывшемся окне укажите количество попыток и промежуток времени, в течение которого выполнялись попытки ввода пароля, для срабатывания правила.
7. Если вы выбрали правило **Обнаружена подозрительная активность во время сетевого сеанса входа**, вам нужно настроить параметры правила:
   a. Нажмите **Настройка** под правилом.
   b. В блоке **Обработка атипичной аутентификации** укажите начало и конец временного интервала.

      Kaspersky Endpoint Security будет считать аномальной активностью выполненные попытки входа в течение заданного интервала.

      По умолчанию интервал не задан и приложение не контролирует попытки входа. Чтобы приложение постоянно контролировало попытки входа, задайте интервал 12:00 AM – 11:59 PM. Начало и конец интервала не должны совпадать. Если они совпадают, приложение не контролирует попытки входа.
   c. В блоке **Исключения** добавьте доверенных пользователей и доверенные IP-адреса компьютеров (IPv4 и IPv6).

      Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно. Kaspersky Endpoint Security не будет контролировать попытки входа для этих пользователей и компьютеров.
8. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security при срабатывании правила будет создавать события со статусом *Критическое событие*.

Добавление пользовательских правил

Вы можете задать собственные критерии срабатывания правила Анализа журналов. Для этого вам нужно ввести идентификатор события и выбрать источник событий. Вы можете узнать идентификатор события на сайте Службы технической поддержки Microsoft. Для выбора источника событий доступны стандартные журналы: *Application*, *Security* или *System*. Также вы можете указать журнал стороннего приложения. Название журнала стороннего приложения вы можете узнать с помощью инструмента Просмотр событий. Журналы сторонних приложений расположены в папке Журналы приложений и служб (например, журнал *Windows PowerShell*).

Приложение не выполняет проверок на фактическое наличие заданного журнала в журнале событий Windows. Если название журнала введено с ошибкой, приложение не будет контролировать события из этого журнала.

В список пользовательских правил уже добавлено три правила, которые созданы специалистами "Лаборатории Касперского".

Как добавить пользовательское правило в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Анализ журналов**.
4. Убедитесь, что флажок **Анализ журналов** установлен.
5. В блоке **Пользовательские правила** нажмите на кнопку **Настройка**.
6. В открывшемся окне установите флажки напротив тех пользовательских правил, которые вы хотите включить.
7. Если требуется, создайте собственные пользовательские правила по кнопке **Добавить**.
8. В открывшемся окне настройте параметры пользовательского правила:
   - **Имя правила**.
   - **Имя журнала**. Журналы событий Windows. Доступны следующие журналы: *Application*, *Security*, *System*.
   - **Источник**. Журналы событий сторонних приложений. Название журнала стороннего приложения вы можете узнать с помощью инструмента Просмотр событий. Журналы сторонних приложений расположены в папке Журналы приложений и служб (например, журнал *Windows PowerShell*).
   - **Идентификаторы событий**. Идентификаторы событий в журнале событий Windows. Вы можете узнать идентификатор события в справке Microsoft.
9. Сохраните внесенные изменения.

Как добавить пользовательское правило в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Анализ журналов**.
5. Убедитесь, что переключатель **Анализ журналов ВКЛЮЧЕН** включен.
6. В блоке **Пользовательские правила** выберите пользовательские правила, которые вы хотите включить.
7. Если требуется, создайте собственные пользовательские правила по кнопке **Добавить**.
8. В открывшемся окне настройте параметры пользовательского правила:
   - **Имя правила**.
   - **Имя журнала**. Журналы событий Windows. Доступны следующие журналы: *Application*, *Security*, *System*.
   - **Источник**. Журналы событий сторонних приложений. Название журнала стороннего приложения вы можете узнать с помощью инструмента Просмотр событий. Журналы сторонних приложений расположены в папке Журналы приложений и служб (например, журнал *Windows PowerShell*).
   - **Идентификаторы событий**. Идентификаторы событий в журнале событий Windows. Вы можете узнать идентификатор события в справке Microsoft.
9. Сохраните внесенные изменения.

Как добавить пользовательское правило в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Анализ журналов**.
3. Убедитесь, что переключатель **Анализ журналов** включен.
4. В блоке **Пользовательские правила** нажмите на кнопку **Настроить**.
5. В открывшемся окне установите флажки напротив тех пользовательских правил, которые вы хотите включить.
6. Если требуется, создайте собственные пользовательские правила по кнопке **Добавить**.
7. В открывшемся окне настройте параметры пользовательского правила:
   - **Название правила**.
   - **Имя журнала**. Журналы событий Windows. Доступны следующие журналы: *Application*, *Security*, *System*.

- **Источник**. Журналы событий сторонних приложений. Название журнала стороннего приложения вы можете узнать с помощью инструмента Просмотр событий. Журналы сторонних приложений расположены в папке Журналы приложений и служб (например, журнал *Windows PowerShell*).

- **Идентификатор событий**. Идентификаторы событий в журнале событий Windows. Вы можете узнать идентификатор события в справке Microsoft.

8. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security при срабатывании правила будет создавать события со статусом *Критическое*.

Контроль целостности системы

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций.

Начиная с версии Kaspersky Endpoint Security для Windows 12.6 вместо компонента Мониторинг файловых операций добавлен компонент Контроль целостности системы. Контроль целостности системы включает в себя все функции Мониторинга файловых операций, а также позволяет контролировать изменения в реестре и подключение внешних устройств.

Контроль целостности системы отслеживает изменения в операционной системе, которые могут указывать на нарушения безопасности компьютера. Обнаружив такие изменения, Kaspersky Endpoint Security формирует соответствующие события и предупреждает администратора. Контроль целостности системы может работать в режиме реального времени, а также выполнять проверку целостности системы по запросу.

Контроль целостности системы в режиме реального времени

При работе в режиме реального времени Контроль целостности системы отслеживает изменения в объектах, которые вы включили в область действия компонента (*область мониторинга*). Также Контроль целостности системы позволяет блокировать несанкционированный доступ к этим объектам в режиме реального времени.

Проверка целостности системы по запросу

Проверка целостности системы по запросу представляет собой задачу, которую вы можете запускать вручную или по расписанию. Для выполнения задачи *Проверка целостности системы* требуется настроить область действия компонента (*область мониторинга*) и создать снимок состояния системы. *Снимок состояния системы* – зафиксированное состояние объектов системы, с которым приложение сравнивает текущее состояние.

Миграция параметров Мониторинга файловых операций

При обновлении Kaspersky Endpoint Security до версии 12.6 миграция параметров Мониторинга файловых операций будет выполнена автоматически. Во время миграции приложение переносит правила мониторинга в Контроль целостности системы. Также при миграции с KSWS на KES правила компонента Мониторинг файловых операций будут перенесены в Контроль целостности системы.

Для корректной работы Контроля целостности системы нужно обновить приложение Kaspersky Endpoint Security и плагин управления до версии 12.6. Если у вас установлен плагин управления более ранней версии, настроить параметры Контроля целостности системы невозможно, так как в плагине управления отсутствует раздел **Контроль целостности системы**.

О правилах Контроля целостности системы

Для работы Контроля целостности системы требуется добавить хотя бы одно правило. *Правило Контроля целостности системы* – набор критериев, которые определяют доступ пользователей к файлам и реестру. Контроль целостности системы обнаруживает изменения в файлах и реестре в заданной *области мониторинга*. Область мониторинга является одним из критериев правила Контроля целостности системы.

Контроль целостности системы позволяет контролировать следующие объекты:

- файлы;
- реестр;
- внешние устройства.

Особенности мониторинга файлов

Контроль целостности системы осуществляет мониторинг изменений в файлах и папках, а также добавление и удаление файлов в области мониторинга. Эти изменения могут указывать на нарушение безопасности компьютера. Рекомендуется добавлять в область мониторинга объекты, изменения в которых происходят редко, или, доступ к которым имеет только администратор. Это позволит уменьшить количество событий Контроля целостности системы.

Контроль целостности системы не осуществляет мониторинг изменений в файлах в общих папках сервера. Контроль целостности системы предназначен только для локального использования.

Kaspersky Endpoint Security отслеживает изменения файлов и папок только на тех дисках, которые подключены в момент начала работы Контроля целостности системы в режиме реального времени. Если диск отключен в момент начала работы Контроля целостности системы в режиме реального времени, приложение не отслеживает изменения файлов и папок на этом диске, даже если эти файлы и папки добавлены в область мониторинга.

Особенности мониторинга реестра

Контроль целостности системы осуществляет мониторинг реестра. Эти изменения могут указывать на нарушение безопасности компьютера.

Контроль целостности системы осуществляет мониторинг следующих корневых разделов реестра:

- HKCR;
- HKLM;
- HKU;
- HKCC;
- HKEY_CLASSES_ROOT;
- HKEY_LOCAL_MACHINE;
- HKEY_USERS;
- HKEY_CURRENT_CONFIG (только для Контроля целостности системы в режиме реального времени);
- HKEY_CURRENT_USER (только для Контроля целостности системы в режиме реального времени).

> Задача *Проверка целостности системы* не поддерживает ключ HKEY_CURRENT_USER. Вы можете указывать путь к ключу в реестре через раздел HKEY_USERS в виде HKEY_USERS\<user profile ID>\<key>.

Особенности мониторинга внешних устройств

Контроль целостности системы осуществляет мониторинг подключения и отключения внешних устройств. Это нужно для защиты компьютера от угроз безопасности, которые могут возникнуть во время файлового обмена с этими устройствами. Контроль целостности системы не контролирует доступ к внешним устройствам и не запрещает обмен файлами. Вы можете настроить доступ к устройствам с помощью другого компонента приложения – Контроль устройств.

> При выполнении задачи *Мониторинг целостности системы на основе эталона* приложение пропускает переключение внешних устройств, если устройства имеют одинаковую букву диска в операционной системе. Для регистрации переключения внешних устройств необходимо, чтобы эти устройства имели разные буквы диска.

Контроль целостности системы осуществляет мониторинг подключения следующих типов внешних устройств:

- Съемный диск (включая USB-флешки).
- Жесткий диск.
- Внешний сетевой адаптер.
- Привод CD/DVD/Blu-ray.
- Сканер / камера.

Контроль целостности системы в режиме реального времени

Контроль целостности системы позволяет отслеживать изменения в операционной системе в режиме реального времени. Вы можете отслеживать изменения, которые могут указывать на нарушения безопасности на компьютере. Компонент позволяет или блокировать эти изменения, или только регистрировать события об изменениях.

Для работы Контроля целостности системы требуется добавить хотя бы одно правило. *Правило Контроля целостности системы* – набор критериев, которые определяют доступ пользователей к файлам и реестру. Контроль целостности системы обнаруживает изменения в файлах и реестре в заданной *области мониторинга*. Область мониторинга является одним из критериев правила Контроля целостности системы.

Режимы работы Контроля целостности системы в режиме реального времени

Чтобы убедиться, что правила Контроля целостности системы не блокируют действия с ресурсами, необходимые для работы операционной системы или других сервисов, рекомендуется после создания правил включить Тестовый режим и проанализировать работу компонента. При включении Тестового режима Kaspersky Endpoint Security не будет блокировать действия пользователя, запрещенные в правилах, но будет формировать события со статусом *Предупреждение* ⚠.

Компонент Контроль целостности системы в режиме реального времени работает в двух режимах:

- Блокировать.

  В этом режиме Контроль целостности системы отслеживает изменения в системе и выполняет действие согласно правилам: **Разрешать** или **Запрещать**. Также Контроль целостности системы формирует соответствующее событие и меняет статус устройства в консоли Kaspersky Security Center.

- Информировать.

  В этом режиме Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга. Если действие с файлами или реестром запрещено, приложение формирует событие *Запрещенное действие разрешено в тестовом режиме*. Для анализа работы правил предназначены отчеты.

Включение Контроля целостности системы в режиме реального времени

Как включить Контроль целостности системы в режиме реального времени в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Контроль целостности системы**.
4. Установите флажок **Контроль целостности системы**.
5. В блоке **Режим работы для блокирующих правил** выберите режим работы Контроля целостности системы в режиме реального времени:
   - **Блокировать**. В этом режиме Контроль целостности системы блокирует действия с файлами и реестром в области мониторинга и формирует соответствующее событие.
   - **Информировать**. В этом режиме Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга и формирует соответствующее событие.
6. В блоке **Контролировать целостность системы в режиме реального времени** установите флажок **Контролировать целостность системы в режиме реального времени**.
7. Настройте мониторинг внешних устройств:
   a. Установите флажок **Следить за устройствами**.
   b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационное*, *Предупреждение*, *Критическое*.

   Контроль целостности системы фиксирует текущее подключение внешних устройств. Приложение начинает контролировать подключение и отключение внешних устройств после включения компонента в параметрах приложения. Далее при подключении или отключении внешних устройств приложение формирует соответствующее событие.
8. Настройте мониторинг файлов и реестра:
   a. Установите флажок **Следить за файлами и реестром**.
   b. Нажмите на кнопку **Настройка**.

      Откроется список правил Контроля целостности системы.
   c. Нажмите на кнопку **Добавить**.

      Вы также можете импортировать правила из другого источника.
   d. Настройте правило Контроля целостности системы (см. таблицу ниже).
9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить Контроль целостности системы в режиме реального времени в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль целостности системы**.
5. Включите переключатель **Контроль целостности системы ВКЛЮЧЕН**.
6. Выберите вкладку **Windows**.
7. В блоке **Контроль целостности системы в режиме реального времени** выберите режим работы Контроля целостности системы в режиме реального времени:

   - **Применять правила**. В этом режиме Контроль целостности системы блокирует действия с файлами и реестром в области мониторинга и формирует соответствующее событие.
   - **Тестировать правила (Информировать)**. В этом режиме Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга и формирует соответствующее событие.
8. Настройте мониторинг файлов и реестра:

   a. Установите флажок **Следить за файлами и реестром**.

   b. Нажмите на кнопку **Правила**.

   Откроется список правил Контроля целостности системы.

   c. Нажмите на кнопку **Добавить**.

   Вы также можете импортировать правила из другого источника.

   d. Настройте правило Контроля целостности системы (см. таблицу ниже).
9. Настройте мониторинг внешних устройств:

   a. Установите флажок **Следить за устройствами**.

   b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационное*, *Предупреждение*, *Критическое*.

   Контроль целостности системы фиксирует текущее подключение внешних устройств. Приложение начинает контролировать подключение и отключение внешних устройств после включения компонента в параметрах приложения. Далее при подключении или отключении внешних устройств приложение формирует соответствующее событие.
10. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить Контроль целостности системы в режиме реального времени в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль целостности системы**.

3. Включить переключатель **Контроль целостности системы**.

4. В блоке **Режим работы для блокирующих правил** выберите режим работы Контроля целостности системы в режиме реального времени:

   - **Блокировать**. В этом режиме Контроль целостности системы блокирует действия с файлами и реестром в области мониторинга и формирует соответствующее событие.

   - **Информировать**. В этом режиме Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга и формирует соответствующее событие.

5. В блоке **Контроль целостности системы в режиме реального времени** установите флажок **Контроль целостности системы в режиме реального времени**.

6. Настройте мониторинг внешних устройств:

   a. Установите флажок **Следить за устройствами**.

   b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационные* ⓘ, *Предупреждение* ⚠, *Критические* ⓘ.

   Контроль целостности системы фиксирует текущее подключение внешних устройств. Приложение начинает контролировать подключение и отключение внешних устройств после включения компонента в параметрах приложения. Далее при подключении или отключении внешних устройств приложение формирует соответствующее событие.

7. Настройте мониторинг файлов и реестра:

   a. Установите флажок **Следить за файлами и реестром**.

   b. Нажмите на кнопку **Настроить**.

      Откроется список правил Контроля целостности системы.

   c. Нажмите на кнопку **Добавить**.

      Вы также можете импортировать правила из другого источника.

8. Настройте правило Контроля целостности системы (см. таблицу ниже).

9. Сохраните внесенные изменения.

Параметры правила Контроля целостности системы в режиме реального времени

Параметр	Описание
Имя правила	Название правила Контроля целостности системы в режиме реального времени.
Действия с файлами и реестром	• **Разрешать**. Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга. • **Запрещать**. Поведение Контроля целостности системы отличается в зависимости от выбранного режима работы. Если вы выбрали *Режим защиты системы*, Контроль целостности системы блокирует действия с файлами и реестром из области мониторинга, формирует соответствующее событие и меняет статус устройства в консоли Kaspersky Security Center. Если вы выбрали *Тестовый режим*, Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга.
Уровень важности событий	Kaspersky Endpoint Security регистрирует события изменения файлов и реестра в области мониторинга. Доступны следующие уровни важности событий: *Информационные*, *Предупреждение*, *Критические*.

Область мониторинга	• **Файл**. Список файлов и папок, которые контролирует компонент. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
	Используйте маски:
	  • Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.
	  • Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.
	  • Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.
	• **Реестр**. Список ключей реестра и значений ключей, которые контролирует компонент. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

Исключения	• **Файл**. Список исключений из области мониторинга. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. Например, `C:\Folder\Application\*.log`. Записи исключений имеют более высокий приоритет, чем записи в области мониторинга.
	Используйте маски:
	  • Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.
	  • Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.
	  • Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.
	• **Реестр**. Список исключений из области мониторинга. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски. Записи исключений имеют более высокий приоритет, чем записи в области мониторинга.

Доверенные пользователи и / или группы пользователей	*Доверенный пользователь* – пользователь, которому разрешено выполнение действий с файлами и реестром в области мониторинга. Если Kaspersky Endpoint Security обнаруживает действие, выполненное доверенным пользователем, Контроль целостности системы формирует событие с уровнем важности *Информационные*. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.
Маркеры файловых операций / Контролируемые действия	Маркеры, характеризующие действие над файлами или реестром, которые будет контролировать приложение.
Хеширование	Вычисление хеша файла при изменении. Kaspersky Endpoint Security добавляет информацию о хеше файла при формировании события.

Проверка целостности системы по запросу

Проверка целостности системы по запросу представляет собой задачу, которую вы можете запускать вручную или по расписанию. Во время выполнения задачи *Проверка целостности системы* приложение сравнивает текущее состояние объектов, включенных в область мониторинга, с состоянием этих объектов, зафиксированных в *снимке состояния системы*. В отличие от Контроля целостности системы в режиме реального времени задача *Проверка целостности системы* позволяет уменьшить количество событий и сформировать общий отчет об изменениях в операционной системе.

Для работы Контроля целостности системы требуется добавить хотя бы одно правило. *Правило Контроля целостности системы* – набор критериев, которые определяют доступ пользователей к файлам и реестру. Контроль целостности системы обнаруживает изменения в файлах и реестре в заданной *области мониторинга*. Область мониторинга является одним из критериев правила Контроля целостности системы. Вы можете настроить общие правила для Контроля целостности системы в режиме реального времени и задачи *Проверка целостности системы* или создать отдельные правила для задачи. Kaspersky Endpoint Security применяет область мониторинга из задачи *Проверка целостности системы* к задаче *Обновление снимка состояния системы* для создания снимка состояния системы.

Создание и обновление снимка состояния системы

Для работы задачи *Проверка целостности системы* вам нужно создать снимок состояния системы. *Снимок состояния системы* – зафиксированное состояние объектов системы, с которым приложение сравнивает текущее состояние. Если текущее состояние системы отличается от состояния системы, зафиксированного в снимке состояния системы, Kaspersky Endpoint Security формирует соответствующее событие. Вы можете создать и обновить снимок состояния системы с помощью задачи *Обновление снимка состояния системы*.

Вы можете обновлять список состояния системы в следующих режимах:

- Полное обновление.

  Приложение обновляет все объекты из области мониторинга.

- Инкрементальное обновление.

  Приложение обнаруживает и обновляет только измененные или новые объекты.

Как создать и обновить снимок состояния системы в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Обновление снимка состояния системы**.

Шаг 2. Выбор режима обновления снимка состояния системы

Выберите режим обновления снимка состояния системы:

- **Полное обновление**. Приложение обновляет все объекты из области мониторинга.
- **Инкрементальное обновление**. Приложение обнаруживает и обновляет только измененные или новые объекты.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Определение названия задачи

Введите название задачи, например, *Снимок состояния системы 2024*.

Шаг 5. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как создать и обновить снимок состояния системы в Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Обновление снимка состояния системы**.

c. В поле **Название задачи** введите короткое описание, например, *Снимок состояния системы 2024*.

d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

5. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.

6. Завершите работу мастера.

   В списке задач отобразится новая задача.

7. Нажмите на новую задачу.

   Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. Выберите режим обновления снимка состояния системы:

   - **Полное обновление**. Приложение обновляет все объекты из области мониторинга.
   - **Инкрементальное обновление**. Приложение обнаруживает и обновляет только измененные или новые объекты.

10. Сохраните внесенные изменения.

11. Установите флажок напротив задачи.

12. Нажмите на кнопку **Запустить**.

Настройка области мониторинга для задачи Проверка целостности системы

По умолчанию область мониторинга для задачи *Проверка целостности системы* совпадает с областью мониторинга Контроля целостности системы в режиме реального времени. Вы можете задать отдельную область мониторинга для задачи.

> Контроль целостности системы не поддерживает импорт ключей `HKEY_CURRENT_USER` и `HKEY_CURRENT_CONFIG` для задачи *Проверка целостности системы*. Если область мониторинга задачи содержит эти ключи, приложение формирует событие *Область мониторинга содержит некорректные объекты*.

Как задать отдельную область мониторинга для задачи Проверка целостности системы в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Контроль безопасности** → **Контроль целостности системы**.

4. Установите флажок **Контроль целостности системы**.

5. В блоке **Проверка целостности системы** выберите режим настройки задачи **Настройки пользователя**.

6. Настройте мониторинг внешних устройств:

   a. Установите флажок **Следить за устройствами**.

   b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационное*, *Предупреждение*, *Критическое*.

   Контроль целостности системы фиксирует подключенные внешние устройства на момент создания снимка состояния системы. Далее при подключении внешних устройств приложение формирует соответствующее событие. При выполнении задачи *Проверка целостности системы* приложение не отслеживает отключение внешних устройств.

7. Настройте мониторинг файлов и реестра:

   a. Установите флажок **Следить за файлами и реестром**.

   b. Нажмите на кнопку **Настройка**.

   Откроется список правил Контроля целостности системы.

   c. Нажмите на кнопку **Добавить**.

   Вы также можете импортировать правила из другого источника.

   d. Настройте правило Контроля целостности системы (см. таблицу ниже).

8. Сохраните внесенные изменения.

Как задать отдельную область мониторинга для задачи Проверка целостности системы в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности** → **Контроль целостности системы**.

5. Выберите вкладку **Windows**.

6. Включите переключатель **Контроль целостности системы ВКЛЮЧЕН**.

7. В блоке **Проверка целостности системы** выберите режим настройки задачи **Настройки пользователя**.

8. Настройте мониторинг внешних устройств:

   a. Установите флажок **Следить за устройствами**.

   b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационное*, *Предупреждение*, *Критическое*.

Контроль целостности системы фиксирует подключенные внешние устройства на момент создания снимка состояния системы. Далее при подключении внешних устройств приложение формирует соответствующее событие. При выполнении задачи *Проверка целостности системы* приложение не отслеживает отключение внешних устройств.

9. Настройте мониторинг файлов и реестра:

   a. Установите флажок **Следить за файлами и реестром**.

   b. Нажмите на кнопку **Правила**.

      Откроется список правил Контроля целостности системы.

   c. Нажмите на кнопку **Добавить**.

      Вы также можете импортировать правила из другого источника.

   d. Настройте правило Контроля целостности системы (см. таблицу ниже).

10. Сохраните внесенные изменения.

Как задать отдельную область мониторинга для задачи Проверка целостности системы в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Контроль безопасности** и нажмите на плитку **Контроль целостности системы**.

3. Включить переключатель **Контроль целостности системы**.

4. В блоке **Проверка целостности системы** выберите режим настройки задачи **Настройки пользователя**.

5. Настройте мониторинг внешних устройств:

   a. Установите флажок **Следить за устройствами**.

   b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационные* ⓘ, *Предупреждение* ⚠, *Критические* ⓘ.

Контроль целостности системы фиксирует подключенные внешние устройства на момент создания снимка состояния системы. Далее при подключении внешних устройств приложение формирует соответствующее событие. При выполнении задачи *Проверка целостности системы* приложение не отслеживает отключение внешних устройств.

6. Настройте мониторинг файлов и реестра:

   a. Установите флажок **Следить за файлами и реестром**.

   b. Нажмите на кнопку **Настроить**.

      Откроется список правил Контроля целостности системы.

c. Нажмите на кнопку **Добавить**.

Вы также можете импортировать правила из другого источника.

d. Настройте правило Контроля целостности системы (см. таблицу ниже).

7. Сохраните внесенные изменения.

Параметры правила задачи Проверка целостности системы

Параметр	Описание
Имя правила	Название правила задачи *Проверка целостности системы*.
Уровень важности событий	Kaspersky Endpoint Security регистрирует события изменения файлов и реестра в области мониторинга. Доступны следующие уровни важности событий: *Информационные*, *Предупреждение*, *Критические*.

Область мониторинга	• **Файл**. Список файлов и папок, которые контролирует компонент. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
	Используйте маски:
	  • Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.
	  • Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.
	  • Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.
	• **Реестр**. Список ключей реестра и значений ключей, которые контролирует компонент. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

Исключения	• **Файл**. Список исключений из области мониторинга. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. Например, `C:\Folder\Application\*.log`. Записи исключений имеют более высокий приоритет, чем записи в области мониторинга.
	Используйте маски:
	  • Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.
	  • Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.
	  • Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.
	• **Реестр**. Список исключений из области мониторинга. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски. Записи исключений имеют более высокий приоритет, чем записи в области мониторинга.

Запуск задачи Проверка целостности системы

Задача *Проверка целостности системы* позволяет проверять изменения в файлах, реестре, а также контролировать подключение внешних устройств. Для контроля изменений файлов вы можете запустить задачу *Проверка целостности системы* в следующих режимах:

- Быстрая проверка.

  При проверке изменений в файлах приложение проверяет только атрибуты файлов. Изменения в содержании файлов приложение не проверяет.

- Полная проверка.

  При проверке изменений в файлах приложение проверяет все атрибуты и содержание файлов.

Режим запуска задачи не влияет на контроль приложением реестра или внешних устройств.

Как запустить задачу Проверка целостности системы в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.

   Откроется список задач.
3. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи. Следуйте его указаниям.
4. Выберите **Kaspersky Endpoint Security → Мониторинг целостности системы на основе эталона**. Выберите режим мониторинга целостности системы:

   - **Полная проверка**. В этом режиме приложение проверяет все атрибуты и хеши файлов.
   - **Быстрая проверка**. В этом режиме приложение проверяет только атрибуты файлов.
5. Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

   - Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
   - Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
   - Задать выборку устройств, для которой требуется запускать задачу.
   - Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
6. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.
7. Настройте расписание запуска задачи, например, вручную или в определенный день недели.
8. Введите название задачи.
9. Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как запустить задачу Проверка целостности системы в Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

    a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

    b. В раскрывающемся списке **Тип задачи** выберите **Проверка целостности системы**.

    c. В поле **Название задачи** введите короткое описание, например, *Еженедельная проверка целостности системы*.

    d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

5. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.

6. Завершите работу мастера.

    В списке задач отобразится новая задача.

7. Нажмите на новую задачу.

    Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. Выберите режим проверки целостности системы:

    - **Быстрая проверка**. Приложение проверяет только атрибуты файлов. Изменения в содержании файлов приложение не проверяет.

    - **Полная проверка**. Приложение проверяет все атрибуты и содержание файлов.

10. Сохраните внесенные изменения.

11. Установите флажок напротив задачи.

12. Нажмите на кнопку **Запустить**.

Для успешного выполнения задачи *Проверка целостности системы* требуется, чтобы снимок состояния системы полностью соответствовал области мониторинга задачи *Проверка целостности системы*. Если область мониторинга отличается, задача завершается с ошибкой. Для синхронизации областей мониторинга запустите задачу *Обновление снимка состояния системы* с новой областью мониторинга.

Экспорт и импорт правил Контроля целостности системы

Вы можете экспортировать список правил Контроля целостности системы в файл в формате XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных записей. Вы можете использовать функцию экспорта / импорта для резервного копирования списка правил Контроля целостности системы или для миграции списка на другой сервер.

Контроль целостности системы не поддерживает импорт ключей `HKEY_CURRENT_USER` и `HKEY_CURRENT_CONFIG` для задачи *Проверка целостности системы*. Если область мониторинга задачи содержит эти ключи, приложение формирует событие *Область мониторинга содержит некорректные объекты*.

Как экспортировать / импортировать список правил Контроля целостности системы в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль безопасности** → **Контроль целостности системы**.
4. Для экспорта / импорта правил *Контроля целостности системы в режиме реального времени* выполните следующие действия:
   a. В блоке **Контролировать целостность системы в режиме реального времени** нажмите на кнопку **Настройка**.
   b. Для экспорта списка правил Контроля целостности системы в режиме реального времени выполните следующие действия:
      1. Выберите правила, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

         Если вы не выбрали ни одного правила, Kaspersky Endpoint Security экспортирует все правила.
      2. Нажмите на ссылку **Экспортировать**.
      3. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список правил, а также выберите папку, в которой вы хотите сохранить этот файл.
      4. Сохраните файл.

         Kaspersky Endpoint Security экспортирует список правил в XML-файл.
   c. Для импорта списка правил Контроля целостности системы в режиме реального времени выполните следующие действия:
      1. Нажмите на ссылку **Импортировать**.

         В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

2. Откройте файл.

   Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

5. Для экспорта / импорта правил *Проверки целостности системы* выполните следующие действия:

   a. В блоке **Проверка целостности системы** выберите вариант **Настройки пользователя**.

   b. Нажмите на кнопку **Настройка**.

   c. Для экспорта списка правил Проверки целостности системы выполните следующие действия:

      1. Выберите правила, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

         Если вы не выбрали ни одного правила, Kaspersky Endpoint Security экспортирует все правила.

      2. Нажмите на ссылку **Экспортировать**.

      3. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список правил, а также выберите папку, в которой вы хотите сохранить этот файл.

      4. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл.

   d. Для импорта списка правил Проверки целостности системы выполните следующие действия:

      1. Нажмите на ссылку **Импортировать**.

         В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

      2. Откройте файл.

      Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

6. Сохраните внесенные изменения.

Как экспортировать / импортировать список правил Контроля целостности системы в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности → Контроль целостности системы**.

5. Выберите вкладку **Windows**.

6. Для экспорта / импорта правил *Контроля целостности системы в режиме реального времени* выполните следующие действия:

   a. В блоке **Контроль целостности системы в режиме реального времени** перейдите по ссылке **Правила**.

   b. Для экспорта списка правил Контроля целостности системы в режиме реального времени выполните следующие действия:

      1. Выберите правила, которые вы хотите экспортировать.

      2. Нажмите на кнопку → **Экспортировать**.

         Kaspersky Endpoint Security экспортирует список правил в JSON-файл в папку для загрузки по умолчанию.

   c. Для импорта списка правил Контроля целостности системы в режиме реального времени выполните следующие действия:

      1. Нажмите на кнопку → **Импортировать**.

         В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список доверенных адресов.

      2. Откройте файл.

         Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.

7. Для экспорта / импорта правил *Проверки целостности системы* выполните следующие действия:

   a. В блоке **Проверка целостности системы по запросу** выберите вариант **Настройки пользователя**.

   b. Перейдите по ссылке **Правила**.

   c. Для экспорта списка правил Проверки целостности системы выполните следующие действия:

      1. Выберите правила, которые вы хотите экспортировать.

      2. Нажмите на кнопку → **Экспортировать**.

         Kaspersky Endpoint Security экспортирует список правил в JSON-файл в папку для загрузки по умолчанию.

   d. Для импорта списка правил Проверки целостности системы выполните следующие действия:

      1. Нажмите на кнопку → **Импортировать**.

         В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список доверенных адресов.

      2. Откройте файл.

         Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.

8. Сохраните внесенные изменения.

Просмотр отчетов о работе Контроля целостности системы

Для анализа работы правил Контроля целостности системы вы можете изучать отчеты, а также просматривать события, сформированные приложением. Kaspersky Endpoint Security формирует следующие отчеты о работе компонента:

- В интерфейсе приложения:
  - Отчет Контроль целостности системы.
  - Отчет Проверка целостности системы.
  - Отчет Обновление снимка состояния системы.

  Отчеты содержат события о работе Контроля целостности системы.
- В консоли Kaspersky Security Center:
  - Отчет о компьютерах, на которых произошло максимальное количество срабатываний правил мониторинга.
  - Отчет о наиболее часто срабатывающих правилах мониторинга.

  По умолчанию отчет создается за последние 30 дней, включая дату создания отчета.

  Как просмотреть отчеты о работе Контроля целостности системы в Консоли администрирования (MMC)

  1. Откройте Консоль администрирования Kaspersky Security Center.
  2. В узле **Сервер администрирования** дерева Консоли администрирования выберите вкладку **Отчеты**.
  3. Нажмите на кнопку **Новый шаблон отчета**.

     Запустится мастер создания шаблона отчета.
  4. Следуйте указаниям мастера создания шаблона отчета. На шаге **Выбор типа шаблона отчета** выберите отчет о работе Контроля целостности системы (раздел **Другое**):
     - **Топ 10 устройств с правилами Мониторинга файловых операций / Контроля целостности системы, срабатывающими чаще всего**.
     - **Топ 10 правил Мониторинга файловых операций / Контроля целостности системы, наиболее часто срабатывающие на устройствах**.

     После завершения работы мастера создания шаблона отчета в таблице на вкладке **Отчеты** появится новый шаблон отчета.
  5. Откройте отчет двойным щелчком мыши.

  Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Как просмотреть отчеты о работе Контроля целостности системы в Web Console

1. В главном окне Web Console выберите **Мониторинг → Отчеты**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания шаблона отчета.
3. В блоке **Тип шаблона** в разделе **Другое** выберите отчет о работе Контроля целостности системы:

   - **Топ 10 устройств с правилами Мониторинга файловых операций / Контроля целостности системы, срабатывающими чаще всего**.
   - **Топ 10 правил Мониторинга файловых операций / Контроля целостности системы, наиболее часто срабатывающие на устройствах**.

   После завершения работы мастера создания шаблона отчета в таблице появится новый шаблон отчета.
4. Выберите и запустите отчет.

   Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Также вы можете просматривать события, сформированные приложением, в консоли Kaspersky Security Center с помощью выборок событий.

Сброс статуса целостности системы

Компьютеры в консоли Kaspersky Security Center имеют статус: *OK*, *Предупреждение* или *Критический*. Если Контроль целостности системы обнаруживает изменения файлов или реестра в области мониторинга, компьютер меняет статус на *Предупреждение* или *Критический*. Статус, назначенный Контролем целостности системы, называется *статусом целостности системы*. Вы можете сбросить статус целостности системы, если, например, после анализа вы убедились в том, что обнаруженные изменения объектов не влияют на безопасность компьютера.

Как сбросить статус целостности системы в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.
2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3) → Сброс статуса целостности системы**.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 3. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную.

Шаг 4. Определение названия задачи

Введите название задачи, например, *Сброс статуса после изменения области мониторинга*.

Шаг 5. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как сбросить статус целостности системы в Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Сброс статуса целостности системы**.

   c. В поле **Название задачи** введите короткое описание, например, *Сброс статуса после изменения области мониторинга*.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

5. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Endpoint Security запускает задачу с правами учетной записи локального пользователя.

6. Завершите работу мастера.

   В списке задач отобразится новая задача.

7. Установите флажок напротив задачи.

8. Нажмите на кнопку **Запустить**.

В результате, если причиной изменения статуса компьютера на *Предупреждение* или *Критический* были события Контроля целостности системы, статус компьютера будет изменен на *ОК*. Если статус компьютера был изменен также по причине других событий, статус компьютера останется прежним.

Cloud Discovery

Cloud Discovery управляет доступом пользователей к облачным сервисам. К облачным сервисам относятся, например, Microsoft Teams, Salesforce, Microsoft Office 365. Облачные сервисы сгруппированы в категории, например, категории *Файловые обменники*, *Мессенджеры*, *Электронная почта*. Специалисты "Лаборатории Касперского" регулярно обновляют набор категорий Cloud Discovery и входящие в их состав облачные сервисы. Kaspersky Endpoint Security обновляет набор категорий и облачные сервисы с базами приложения. То есть Cloud Discovery не использует Kaspersky Security Network для категоризации облачных сервисов.

Cloud Discovery выполняет следующие функции:

- мониторинг использования облачных сервисов;
- блокировка доступа пользователей к облачным сервисам.

Требования к системе

Cloud Discovery доступен при выполнении следующих условий:

- Приложение установлено на компьютере под управлением операционной системы Windows для рабочих станций.

  Компонент недоступен для серверов.

- Kaspersky Security Center версии 15.1 и выше.

  Компонент недоступен в Консоли администрирования (MMC). Вы можете настроить Cloud Discovery в Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console.

- Лицензия Kaspersky Next.

Включите функции приложения, необходимые для работы компонента Cloud Discovery:

1. **Проверять защищенные соединения**. Это нужно для контроля HTTPS-трафика. Управление функцией доступно в разделе **Настройки сети**.

2. **Внедрять в трафик скрипт взаимодействия с веб-страницами**. Скрипт позволяет регистрировать события работы Cloud Discovery. Также скрипт обеспечивает полнофункциональную блокировку доступа к облачным сервисам. Без скрипта приложение блокирует доступ только по доменам облачных сервисов. Управление функцией доступно в разделе **Настройки сети**.

Также вы можете включить функцию **Записывать данные о посещении разрешенных страниц в журнал**. Функция включает группировку событий при посещении пользователем веб-страниц, которые относятся к одному домену. Таким образом, при использовании пользователем облачного сервиса Cloud Discovery регистрирует только одно событие, а не несколько для каждой веб-страницы. Управление функцией доступно в разделе **Веб-Контроль**.

Мониторинг облачных сервисов

Когда пользователь начинает использование облачного сервиса, Kaspersky Endpoint Security регистрирует это событие и делает запись в отчете. Cloud Discovery контролирует использование облачных сервисов как в браузере, так и в соответствующих приложениях. Cloud Discovery контролирует использование облачных сервисов по протоколам HTTP и HTTPS.

Как включить мониторинг облачных сервисов в Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Cloud Discovery**.

5. Включите переключатель **Cloud Discovery ВКЛЮЧЕН**.

6. Сохраните внесенные изменения.

В результате приложение передает в Kaspersky Security Center информацию об используемых облачных сервисах. Вы можете просмотреть информацию об использовании облачных сервисов в отчетах. Если требуется, вы можете заблокировать доступ к облачным сервисам.

Блокировка доступа к облачным сервисам

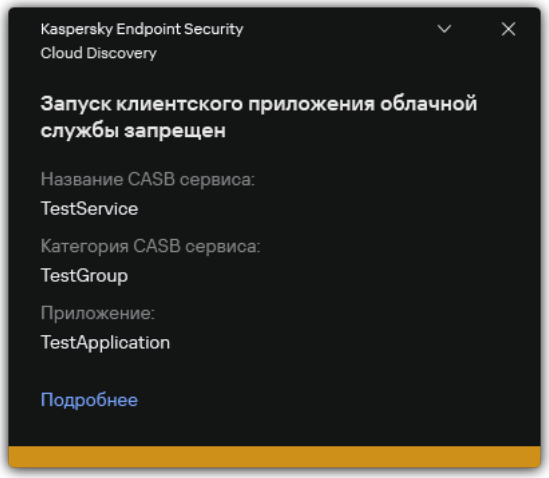
Блокировка доступа к облачным сервисам доступна только для лицензии Kaspersky Next EDR Optimum и XDR Expert. Для лицензии Kaspersky Next EDR Foundations эта функция недоступна. Сравнение функций приложения для вариантов лицензий Kaspersky Next см. в справке Kaspersky Next.

Администратор может ограничить доступ пользователей к категориям Cloud Discovery или отдельным облачным сервисам. Таким образом, администратор может разрешить использование только надежных облачных сервисов и избежать утечки информации. Для каждого облачного сервиса в Cloud Discovery отображаются данные об *уровне риска*. Уровень риска позволяет выявить сервисы, не соответствующие требованиям безопасности организации.

Уровень риска является оценочным показателем и ничего не говорит о качестве облачного сервиса и о его поставщике. Уровень риска – это просто рекомендация экспертов "Лаборатории Касперского".

Уровни риска облачных сервисов отображаются в политике в разделе **Cloud Discovery** в списке всех контролируемых облачных сервисов.

Защиту от угроз и отслеживание подозрительных действий пользователя при использовании облачных сервисов выполняют другие компоненты Kaspersky Endpoint Security.



Уведомление Cloud Discovery

Cloud Discovery не блокирует облачные приложения, которые были запущены раньше чем Kaspersky Endpoint Security.

Как заблокировать доступ к облачным сервисам в Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Cloud Discovery**.
5. Включите переключатель **Cloud Discovery ВКЛЮЧЕН**.

   Откроется список всех облачных сервисов. Облачные сервисы сгруппированы в категории, например, категории *Файловые обменники*, *Мессенджеры*, *Электронная почта*. Специалисты "Лаборатории Касперского" регулярно обновляют набор категорий Cloud Discovery и входящие в их состав облачные сервисы. Kaspersky Endpoint Security обновляет набор категорий и облачные сервисы с базами приложения.

6. Настройте доступ к облачным сервисам с помощью переключателя в графе **Доступ**.

7. Сохраните внесенные изменения.

В результате приложение будет контролировать использование облачных сервисов как в браузере, так и в соответствующих приложениях.

Удаленный доступ VPN

Данная функция находится на этапе бета-тестирования и доступна только участникам программы бета-тестирования решений "Лаборатории Касперского". Работа функции может быть нестабильной.

В Kaspersky Endpoint Security 14.3 добавлен компонент VPN-агент, который обеспечивает защищенное подключение к корпоративной сети через общедоступные сети. Для этого Kaspersky Endpoint Security использует инфраструктуру Kaspersky NGFW.

Kaspersky Endpoint Security в составе Kaspersky NGWF выполняет следующие функции:

- Установление защищенного соединения с удаленным сервером по протоколу WireGuard.
- Аутентификация пользователя с помощью сертификата на токене.
- Поддержка функции раздельного туннелирования (англ. split tunneling). Функция позволяет модифицировать таблицу маршрутизации компьютера пользователя при установлении VPN-соединения в соответствии с параметрами, заданными администратором на удаленном сервере.
- Централизованное управление сетевыми параметрами и политиками безопасности на компьютере пользователя в Kaspersky Security Center.

Управление Защитой доступа сети выполняется в политике Kaspersky Endpoint Security и политике Kaspersky NGFW. Для работы с политиками Kaspersky NGFW требуется установить плагин Kaspersky NGFW, который входит в комплект поставки.

Лицензирование

Для интеграции Kaspersky Endpoint Security с Kaspersky NGFW отдельный ключ не требуется.

Интеграция с Kaspersky NGFW

Kaspersky NGFW при работе с конечными устройствами с установленным приложением Kaspersky Endpoint Security выполняет функции VPN-сервера, сервера контроля сетевого доступа и межсетевого экрана. После установления VPN-соединения конечные устройства автоматически регистрируются в Kaspersky NGFW. Взаимодействие конечных устройств с Kaspersky NGFW производится с использованием протокола REST over mTLS. После регистрации в Kaspersky NGFW каждому новому конечному устройству присваивается уникальный идентификатор, который хранится в базе Kaspersky NGFW.

Установка VPN-агента для удаленного доступа

Данная функция находится на этапе бета-тестирования и доступна только участникам программы бета-тестирования решений "Лаборатории Касперского". Работа функции может быть нестабильной.

VPN-агент для удаленного доступа входит в состав Kaspersky Endpoint Security для Windows. Вы можете установить VPN-агент для удаленного доступа во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*. По умолчанию VPN-агент исключен из установки приложения.

Для завершения обновления приложения с новым компонентов нужно перезагрузить компьютер.

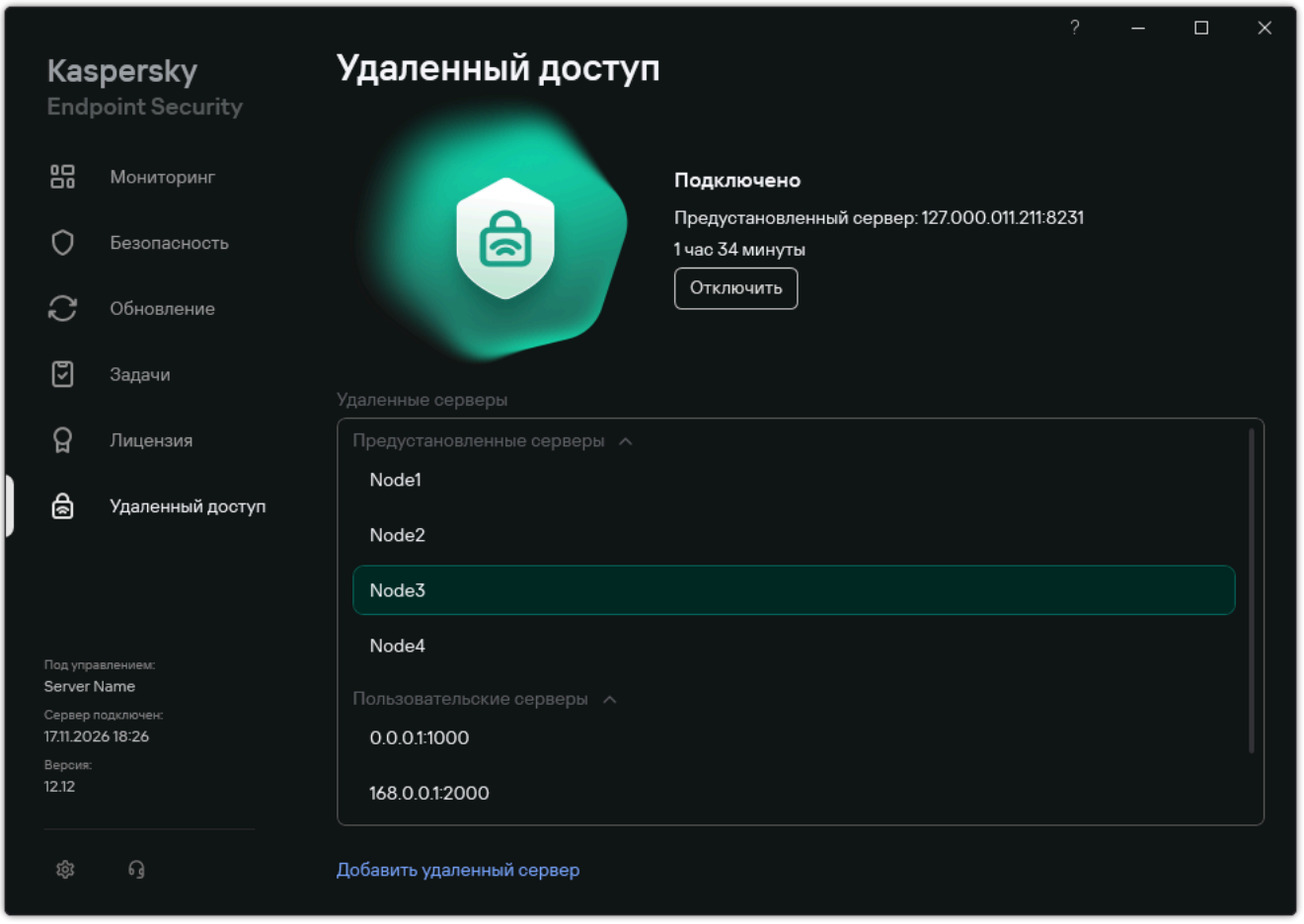
Минимальные системные требования

Минимальные системные требования для агента соответствуют требованиям к Kaspersky Endpoint Security.

Минимальные системные требование к Kaspersky NGFW приведены в справке к Kaspersky NGFW.

Интерфейс VPN-агента

После установки VPN-агента для удаленного доступа в интерфейс Kaspersky Endpoint Security будет добавлен новый раздел – **Удаленный доступ**. В этом разделе вы можете выбрать предустановленный сервер для установки VPN-соединения или добавить сервера вручную.



Интерфейс VPN-агента

Добавление удаленного сервера

Данная функция находится на этапе бета-тестирования и доступна только участникам программы бета-тестирования решений "Лаборатории Касперского". Работа функции может быть нестабильной.

Kaspersky Endpoint Security позволяет использовать предустановленные и пользовательские серверы. Чтобы упростить пользователям подключение к удаленному серверу, вы можете добавить адреса предустановленных серверов в политику. Пользователь не может изменить адрес предустановленного сервера, заданный в политике. Приложение выполняет подключение к предустановленному серверу автоматически. Администратор может добавить несколько серверов для повышения отказоустойчивости. Если установить соединение с одним сервером не удалось, пользователь может попробовать подключиться к другому серверу.

У пользователя есть возможность настроить параметры подключения к удаленному серверу вручную. Для этого администратору нужно разрешить использование пользовательских серверов (см. инструкцию ниже).

Требования к удаленному серверу

- Сервер доступа должен использовать сертификат, которому доверяют устройства пользователей. Kaspersky Endpoint Security выполняет проверку сертификата, размещенного на токене.
- Пользователь должен обладать учётными данными, необходимыми для аутентификации на удаленном сервере.
- На компьютере пользователя должен быть установлен VPN-агент для удаленного доступа.

Добавление предустановленного сервера

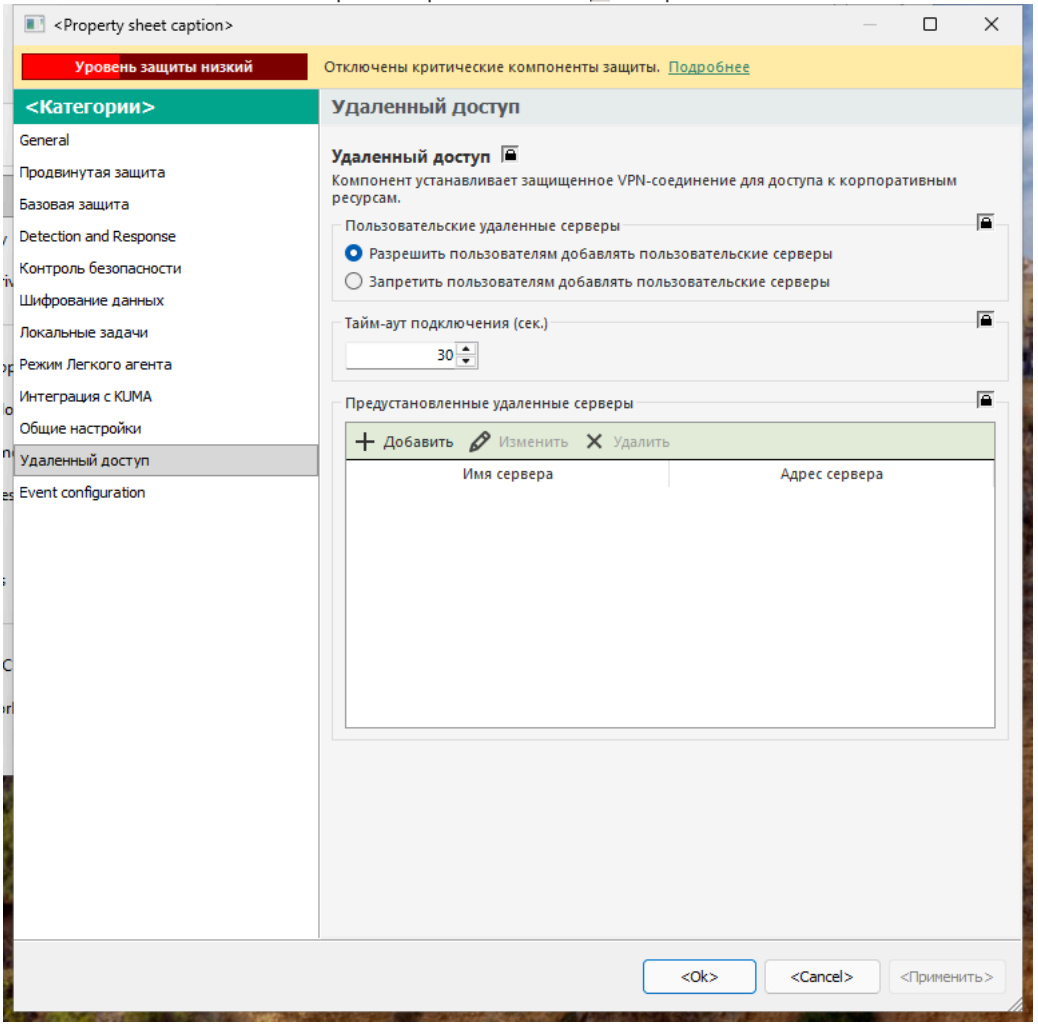
Как добавить удаленный сервер в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Удаленный доступ**.
5. В блоке **Предустановленные удаленные серверы** нажмите на кнопку **Добавить**.

   Откроется форма добавления сервера.
6. Введите имя удаленного сервера.
7. Введите адрес сервера (IPv4, IPv6, FQDN), а также порт подключения к серверу (по умолчанию 443).

   Вы можете добавить несколько адресов удаленных серверов. Пользователь выберет удаленный сервер и, если установить соединение не удалось, пользователь может выбрать другой сервер.
8. Задайте значение параметра **Тайм-аут подключения (сек.)**. Максимальное время ожидания ответа от удаленного сервера. Если в течение заданного периода установить соединение с удаленным сервером не удалось, приложение отображает сообщение об ошибке.

9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.



Раздел политики Удаленный доступ

Как добавить удаленный сервер в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Удаленный доступ**.
5. В блоке **Предустановленные удаленные серверы** нажмите на кнопку **Добавить**.

   Откроется форма добавления сервера.
6. Введите имя удаленного сервера.
7. Введите адрес сервера (IPv4, IPv6, FQDN), а также порт подключения к серверу (по умолчанию 443).

   Вы можете добавить несколько адресов удаленных серверов. Пользователь выберет удаленный сервер и, если установить соединение не удалось, пользователь может выбрать другой сервер.

8. Задайте значение параметра **Время ожидания (сек.)**. Максимальное время ожидания ответа от удаленного сервера. Если в течение заданного периода установить соединение с удаленным сервером не удалось, приложение отображает сообщение об ошибке.

9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Добавление пользовательского сервера

Как разрешить добавлять пользовательские серверы в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите папку **Политики**.

3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

4. В окне политики выберите **Удаленный доступ**.

5. В блоке **Пользовательские удаленные серверы** выберите вариант **Разрешить пользователям добавлять пользовательские серверы**.

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как разрешить добавлять пользовательские серверы в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Удаленный доступ**.

5. В блоке **Пользовательские удаленные серверы** выберите вариант **Разрешить пользователям добавлять пользовательские серверы**.

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Чтобы добавить пользовательский сервер, выполните следующие действия.

1. В главном окне приложения перейдите в раздел **Удаленный доступ**.

2. Откроется окно со списком удаленных серверов.

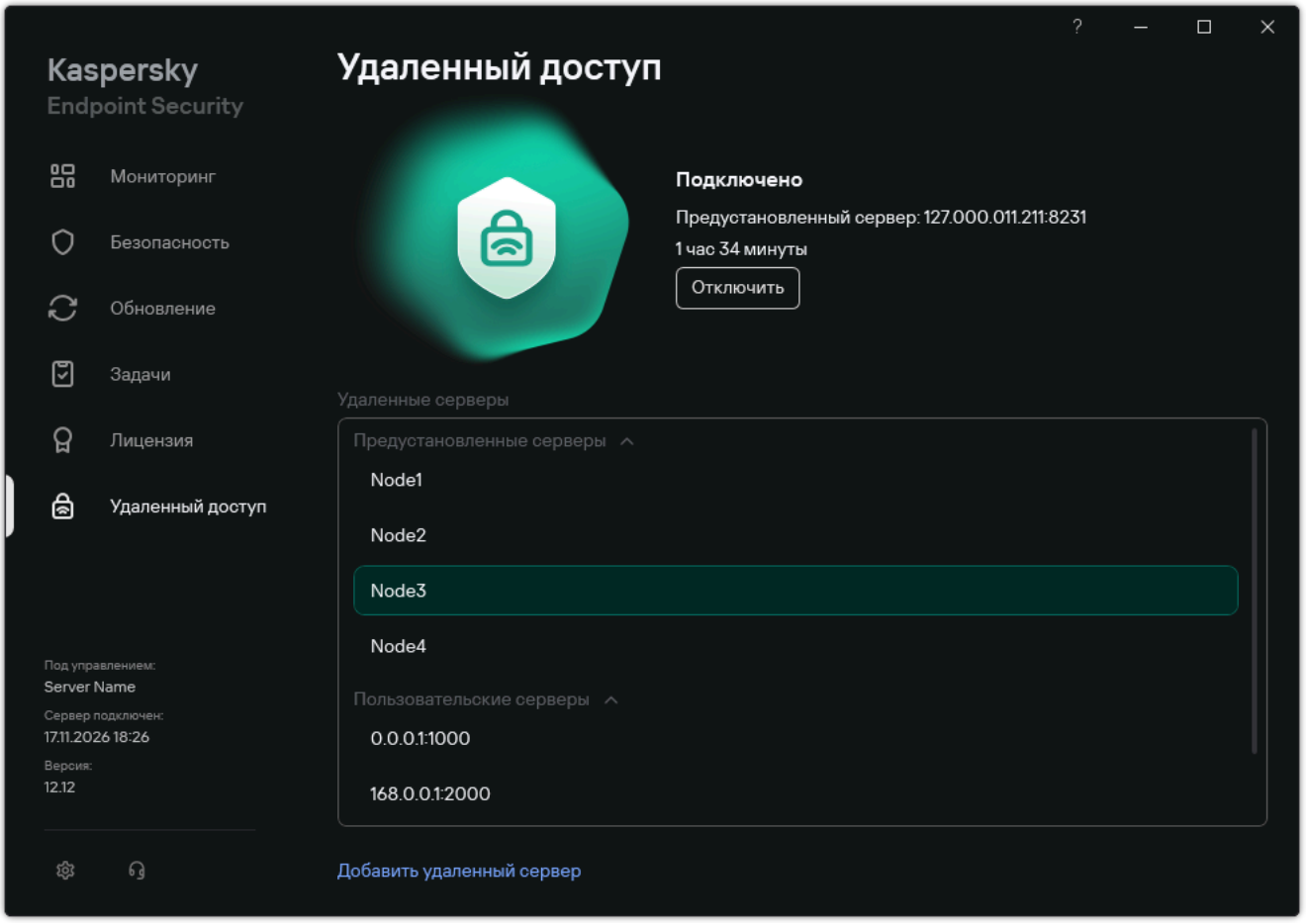
3. Внизу окна нажмите на кнопку **Добавить удаленный сервер**.

   Откроется форма добавления сервера.

4. Введите адрес сервера (IPv4, IPv6, FQDN), а также порт подключения к серверу (по умолчанию 443).

5. Нажмите на кнопку **Подключить**.

Kaspersky Endpoint Security попытается подключиться к корпоративной сети.



Раздел клиента для удаленного доступа VPN

Установка VPN-соединения

Данная функция находится на этапе бета-тестирования и доступна только участникам программы бета-тестирования решений "Лаборатории Касперского". Работа функции может быть нестабильной.

При работе с Kaspersky Security Center параметры VPN-соединения централизованно задает администратор сети. Но вы можете добавить сервер вручную.

Чтобы установить VPN-соединение, выполните следующие действия:

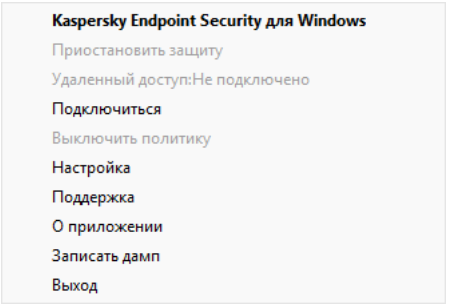
1. Установите токен для установки VPN-соединения, выданный вашим администратором.

2. По правой клавише мыши откройте контекстное меню значка приложения, который расположен в области уведомлений панели задач.

3. В контекстном меню выберите пункт **Подключиться**.

   Этот пункт доступен, если VPN-агент для удаленного доступа установлен.

Приложение Безопасность Windows предложит выбрать сертификат для аутентификации.

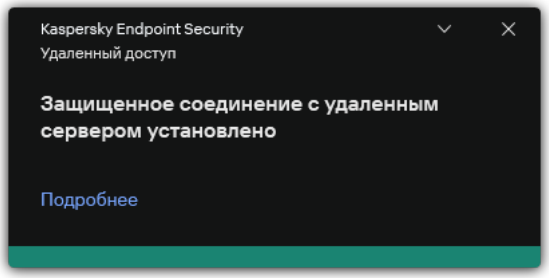


Контекстное меню приложения

4. Выберите сертификат токена и, если требуется, введите учетные данные пользователя.

   Kaspersky Endpoint Security попытается установить VPN-соединение с первым удаленным сервером. Если установить соединение не удалось, агент переключится на следующий сервер и так далее. Список серверов доступен в интерфейсе приложения.

5. При успешном установлении соединения Kaspersky Endpoint Security покажет уведомление.



Уведомление об установленном VPN-соединении

6. Чтобы разорвать VPN-соединение, выберите пункт **Отключиться от удаленного сервера**.

Доверенная зона

Доверенная зона – это сформированный администратором системы список объектов и приложений, которые Kaspersky Endpoint Security не контролирует в процессе работы.

Доверенную зону администратор системы формирует самостоятельно в зависимости от особенностей объектов, с которыми требуется работать, а также от приложений, установленных на компьютере. Включение объектов и приложений в доверенную зону может потребоваться, например, если Kaspersky Endpoint Security блокирует доступ к какому-либо объекту или приложению, в то время как вы уверены, что этот объект или приложение безвредны. Также администратор может разрешить пользователю формировать собственную локальную доверенную зону для отдельного компьютера. Таким образом, кроме общей доверенной зоны, сформированной в политике, пользователь может создавать собственные локальные списки исключений и доверенных приложений.

Начиная с версии Kaspersky Endpoint Security для Windows 12.5 вы можете добавить EDR-телеметрию в доверенную зону. Это позволяет оптимизировать данные, которые приложение отправляет на Сервер сбора телеметрии для решения Kaspersky Anti Targeted Attack Platform (EDR).

Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах.

Начиная с версии Kaspersky Endpoint Security для Windows 12.8 добавлена установка приложения в режиме Легкого агента для защиты виртуальных сред. Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в виртуальных средах Citrix и VMware.

Создание исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Endpoint Security не проверяет объект на вирусы и другие приложения, представляющие угрозу. Исключения из проверки позволяют работать с легальными приложениями, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие приложения не имеют вредоносных функций, но могут быть использованы злоумышленниками. Подробную информацию о легальных приложениях, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского".

В результате работы Kaspersky Endpoint Security такие приложения могут быть заблокированы. Чтобы избежать блокирования, для используемых приложений вы можете настроить исключения из проверки. Для этого нужно добавить в доверенную зону название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского". Например, вы часто используете в своей работе приложение Radmin, предназначенное для удаленного управления компьютерами. Такая активность приложения рассматривается Kaspersky Endpoint Security как подозрительная и может быть заблокирована. Чтобы исключить блокировку приложения, нужно сформировать исключение из проверки, где указать название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского".

Если у вас на компьютере установлено приложение, выполняющее сбор и отправку информации на обработку, приложение Kaspersky Endpoint Security может классифицировать такое приложение как вредоносное. Чтобы избежать этого, вы можете исключить приложение из проверки, настроив приложение Kaspersky Endpoint Security способом, описанным в этом документе.

Исключения из проверки могут использоваться в ходе работы следующих компонентов и задач приложения, заданных администратором системы:

- Анализ поведения.
- Защита от эксплойтов.
- Предотвращение вторжений.
- Защита от файловых угроз.
- Защита от веб-угроз.
- Защита от почтовых угроз.
- Задача *Поиск вредоносного ПО*.

Kaspersky Endpoint Security не проверяет объект, если при запуске одной из задач проверки в область проверки включен диск, на котором находится объект, или папка, в которой находится объект. Однако при запуске задачи выборочной проверки именно для этого объекта исключение из проверки не применяется.

Как создать исключение из проверки в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Общие настройки** → **Исключения и типы объектов**.
5. В блоке **Исключения из проверки и доверенные приложения** → **Исключения из проверки** нажмите на кнопку **Настройка**.

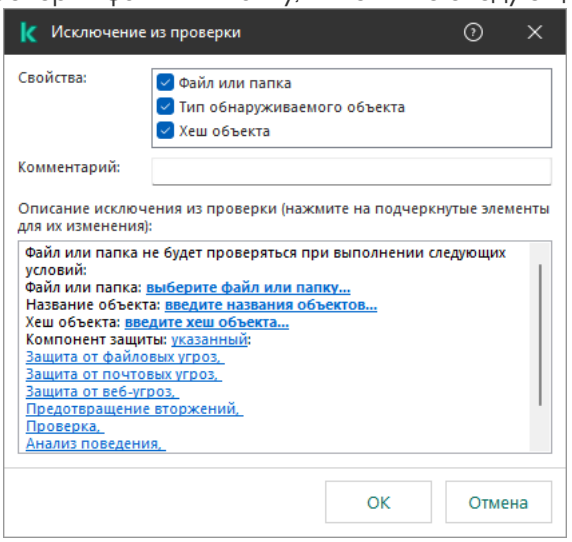
   Откроется окно со списком исключений.
6. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список исключений для всех компьютеров организации. Списки исключений родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Исключения родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление исключений родительской политики невозможно.
7. Установите флажок **Разрешить использование локальных исключений**, если вы хотите чтобы у пользователя была возможность создать локальный список исключений. Таким образом, кроме общего списка исключений, сформированного в политике, пользователь может создавать собственный локальный список исключений. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера.

   Если флажок снят, пользователю доступен только общий список исключений, сформированный в политике. Также, если флажок снят, Kaspersky Endpoint Security скрывает для просмотра общий список исключений из проверки в интерфейсе приложения.

8. Нажмите на кнопку **Добавить** и выберите нужное действие:

- **Категорию**. Вы можете группировать исключения из проверки в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно исключение из проверки.
- **Новое исключение**. Kaspersky Endpoint Security добавляет новое исключение из проверки в корень списка.
- **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные исключения из проверки*. Также в приложение добавлены предустановленные исключения из проверки для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные исключения из проверки.
- **Новое исключение в выбранную категорию**. Для добавления нового исключения из проверки в отдельную категорию выберите категорию.

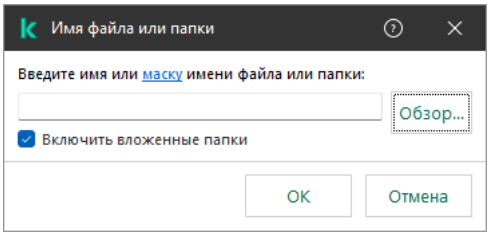
9. Если вы хотите исключить из проверки файл или папку, выполните следующие действия:



Параметры исключения

a. В блоке **Свойства** установите флажок **Файл или папка**.

b. По ссылке, расположенной в блоке ниже, откройте окно **Имя файла или папки**.



Выбор файла или папки

a. Введите имя файла или папки, маску имени файла или папки или выберите файл или папку в дереве папок, нажав на кнопку **Обзор**.

Используйте маски:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `?:\Users\*\Folder\`.

Kaspersky Endpoint Security поддерживает переменные среды.

Вы можете исключать сетевые папки. Для этого введите путь к сетевой папке вручную (например, `\\Network Share\*`).

> Kaspersky Endpoint Security не поддерживает переменную среды `%userprofile%` при формировании списка исключений через консоль Kaspersky Security Center. Чтобы применить запись ко всем учетным записям, вы можете использовать символ `*` (например, `C:\Users\*\Documents\File.exe`). При добавлении новой переменной среды нужно перезапустить приложение.

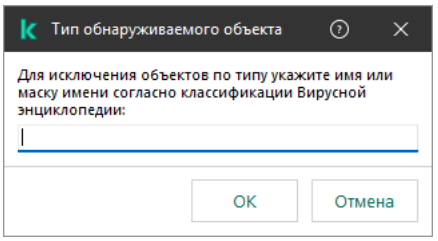
b. При необходимости выключите функцию **Включить вложенные папки**. Если функция включена, приложение не будет проверять файлы во всех вложенных папках. Если функция выключена, приложение исключит из области проверки только указанную папку. По умолчанию функция включена.

c. Сохраните внесенные изменения.

10. Если вы хотите исключить из проверки объекты с определенным названием, выполните следующие действия:

    a. В блоке **Свойства** установите флажок **Тип обнаруживаемого объекта**.

    b. По ссылке, расположенной в блоке ниже, откройте окно **Тип обнаруживаемого объекта**.



Выбор объекта

    a. Введите название типа объекта по классификации Энциклопедии "Лаборатории Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

    Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, Kaspersky Endpoint Security исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

    b. Сохраните внесенные изменения.

11. Если вы хотите исключить из проверки отдельный файл, выполните следующие действия:

    a. В блоке **Свойства** установите флажок **Хеш объекта**.

    b. По ссылке, расположенной в блоке ниже, откройте окно **Хеш объекта**.



Выбор файла

    a. Введите хеш файла или выберите файл, нажав на кнопку **Обзор**.

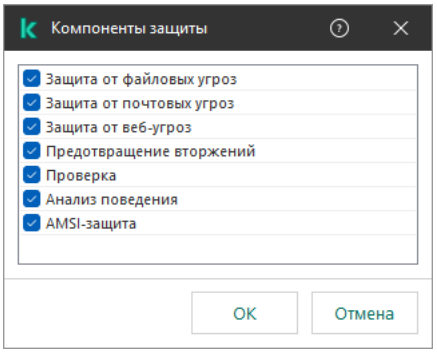
    Если файл изменится, хеш файла тоже будет изменен. В результате измененный файл не будет добавлен в исключения.

    b. Сохраните внесенные изменения.

12. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

13. Определите компоненты Kaspersky Endpoint Security, в работе которых должно быть использовано исключение из проверки:

    a. По ссылке, расположенной в блоке ниже, откройте окно **Компоненты защиты**.



Выбор компонентов защиты

    a. Установите флажки напротив тех компонентов, на работу которых должно распространяться исключение из проверки.

    Если компоненты указаны в параметрах исключения из проверки, то исключение применяется при проверке только этими компонентами Kaspersky Endpoint Security.

    Если компоненты не указаны в параметрах исключения из проверки, то исключение применяется при проверке всеми компонентами Kaspersky Endpoint Security.

14. Нажмите на кнопку **OK**.

    Новое исключение будет добавлено в список. Вы можете в любое время остановить работу исключения с помощью флажка напротив объекта.

15. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как создать исключение из проверки в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Доверенная зона**.

5. В открывшемся окне перейдите по ссылке **Исключения из Поиска вредоносного ПО**.

6. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список исключений для всех компьютеров организации. Списки исключений родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Исключения родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление исключений родительской политики невозможно.

7. Установите флажок **Разрешить использование локальных исключений**, если вы хотите чтобы у пользователя была возможность создать локальный список исключений. Таким образом, кроме общего списка исключений, сформированного в политике, пользователь может создавать собственный локальный список исключений. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера.

   Если флажок снят, пользователю доступен только общий список исключений, сформированный в политике. Также, если флажок снят, Kaspersky Endpoint Security скрывает для просмотра общий список исключений из проверки в интерфейсе приложения.

8. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категория**. Вы можете группировать исключения из проверки в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно исключение из проверки.

   - **Новое исключение**. Kaspersky Endpoint Security добавляет новое исключение из проверки в корень списка.

   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные исключения из проверки*. Также в приложение добавлены предустановленные исключения из проверки для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные исключения из проверки.

   Для добавления нового исключения из проверки в отдельную категорию установите флажок рядом с этой категорией и выберите вариант **Новое исключение**.

9. Выберите способ добавления исключения: **Путь к файлу или папке**, **Тип объекта** или **Хеш объекта**.

10. Если вы хотите исключить из проверки файл или папку, введите путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски:

    - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

    - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

    - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

      Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `?:\Users\*\Folder\`.

      Вы можете исключать сетевые папки. Для этого введите путь к сетевой папке вручную (например, `\\Network Share\*`).

11. Если вы хотите исключить из проверки тип объектов, в поле **Тип объекта** введите название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

    Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, Kaspersky Endpoint Security исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

12. Если вы хотите исключить из проверки отдельный файл, в поле **Хеш объекта** введите хеш файла.

    Если файл изменится, хеш файла тоже будет изменен. В результате измененный файл не будет добавлен в исключения.

13. В блоке **Применить исключение к** выберите компоненты, на работу которых должно распространяться исключение из проверки.

14. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

15. Нажмите на кнопку **ОК**.

    Новое исключение будет добавлено в список. Вы можете в любое время остановить работу исключения с помощью переключателя.

16. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

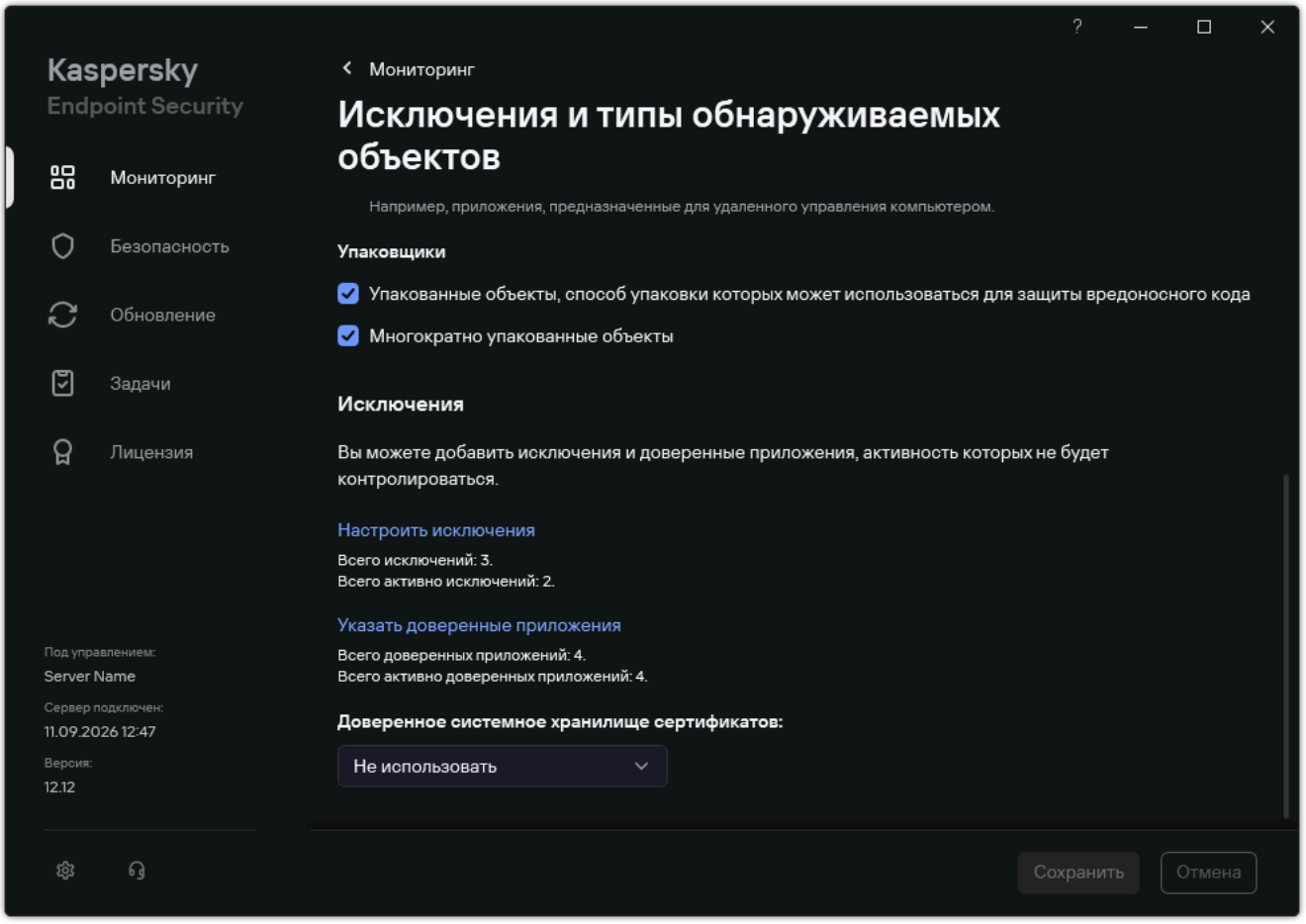
Как создать исключение из проверки в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.

3. В блоке **Исключения** перейдите по ссылке **Настроить исключения**.

Kaspersky Endpoint Security скрывает для просмотра список исключений из проверки в интерфейсе приложения, если администратор в консоли запретил настройку исключений из проверки ("замок" закрыт) и запретил использование локальных исключений из проверки (флажок **Разрешить использование локальных исключений** снят).



Параметры исключений

4. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категорию**. Вы можете группировать исключения из проверки в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно исключение из проверки.

   - **Новое исключение**. Kaspersky Endpoint Security добавляет новое исключение из проверки в корень списка.

   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные исключения из проверки*. Также в приложение добавлены предустановленные исключения из проверки для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные исключения из проверки.

   Для добавления нового исключения из проверки в отдельную категорию установите флажок рядом с этой категорией и выберите вариант **Новое исключение**.

5. Если вы хотите исключить из проверки файл или папку, выберите файл или папку, нажав на кнопку **Обзор**.

Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

  Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `?:\Users\*\Folder\`.

  Вы можете исключать сетевые папки. Для этого введите путь к сетевой папке вручную (например, `\\Network Share\*`).

6. Если вы хотите исключить из проверки тип объектов, в поле **Тип обнаруживаемого объекта** введите название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

   Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, Kaspersky Endpoint Security исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

7. Если вы хотите исключить из проверки отдельный файл, в поле **Хеш объекта** введите хеш файла.

   Если файл изменится, хеш файла тоже будет изменен. В результате измененный файл не будет добавлен в исключения.

8. В блоке **Компоненты защиты** выберите компоненты, на работу которых должно распространяться исключение из проверки.

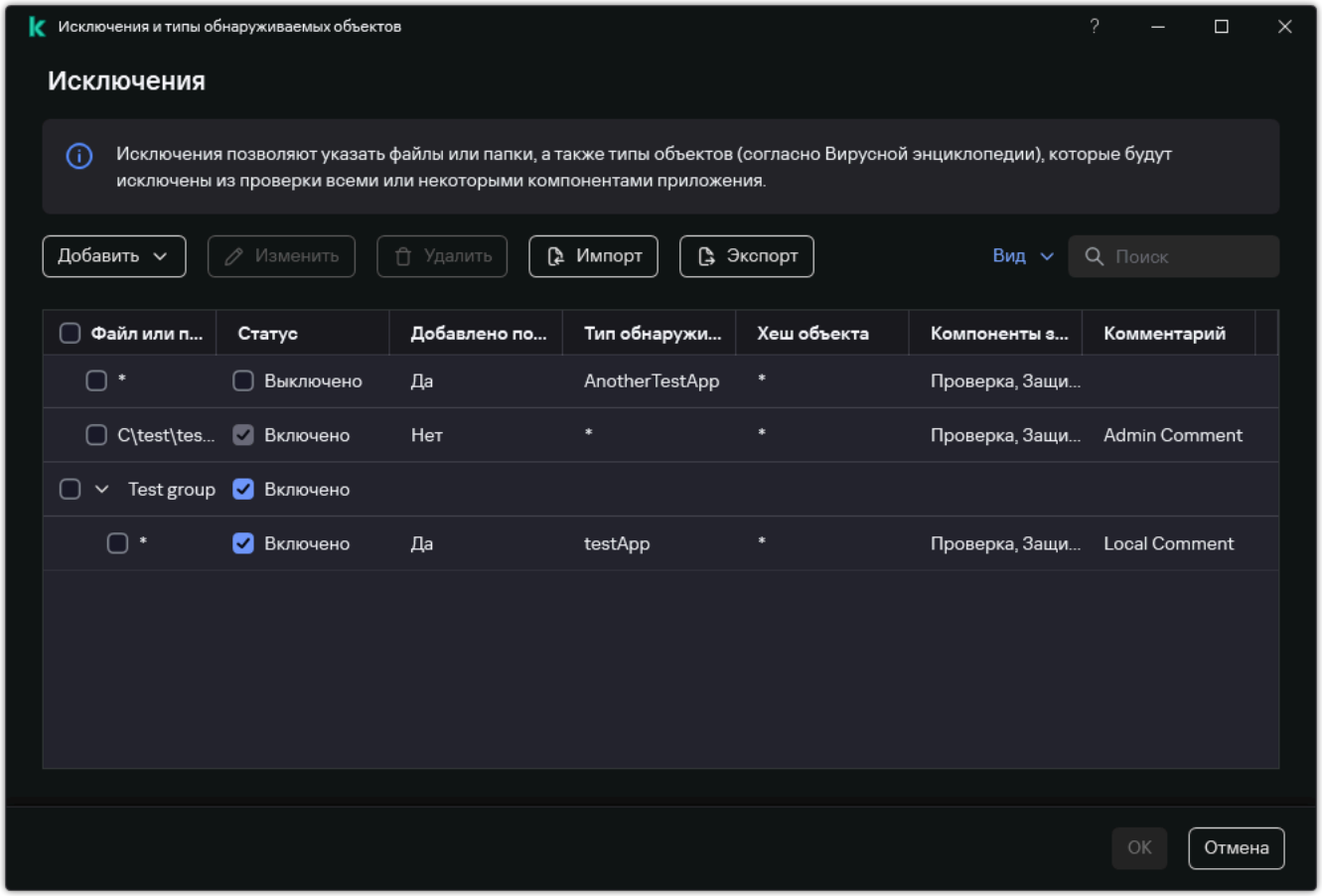
9. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

10. Установите статус для исключения **Активно**.

11. Нажмите на кнопку **Добавить**.

    Новое исключение будет добавлено в список. Вы можете в любое время остановить работу исключения с помощью флажка в графе **Статус**.

12. Сохраните внесенные изменения.



Список исключений

Примеры масок пути:

Рекомендуется указывать относительные пути вместо абсолютных. Это позволяет исключить из проверки не только объекты файловой системы, но и бесфайловые объекты. Например, `*\Program Files (x86)\Folder\Subfolder`.

Пути к файлам, расположенным в любой из папок:

- Маска `*.exe` будет включать все пути к файлам с расширением exe.
- Маска `example*` будет включать все пути к файлам с именем EXAMPLE.

Пути к файлам, расположенным в указанной папке:

- маска `C:\dir\*.*` будет включать все пути к файлам в папке `C:\dir\`, но не в подпапках папки `C:\dir\`;
- маска `C:\dir\*` будет включать все пути к файлам в папке `C:\dir\`, включая подпапки;
- маска `C:\dir\` будет включать все пути к файлам в папке `C:\dir\`, включая подпапки;
- маска `C:\dir\*.exe` будет включать все пути к файлам с расширением exe в папке `C:\dir\`, но не в подпапках папки `C:\dir\`;
- маска `C:\dir\test` будет включать все пути к файлам с именем test в папке `C:\dir\`, но не в подпапках папки `C:\dir\`;
- маска `C:\dir\*\test` будет включать все пути к файлам с именем test в папке `C:\dir\` и в подпапках папки `C:\dir\`;
- маска `C:\dir1\*\dir3\` будет включать все пути к файлам в подпапках dir3 в папке `C:\dir1\` через один уровень;
- маска `C:\dir1\**\dirN\` будет включать все пути к файлам в подпапках dirN в папке `C:\dir1\` на любом уровне.

Пути к файлам, расположенным во всех папках с указанным именем:

- маска `dir\*.*` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\*` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\*.exe` будет включать все пути к файлам с расширением exe в папках с именем dir, но не в подпапках этих папок;
- маска `dir\test` будет включать все пути к файлам с именем test в папках с именем dir, но не в подпапках этих папок.

Создание исключения по типу обнаруживаемых объектов

Kaspersky Endpoint Security классифицирует обнаруживаемые объекты следующим образом:

- **Вирусы и черви**

  Подкатегория: вирусы и черви (Viruses_and_Worms)

  Уровень опасности: высокий

  Классические вирусы и черви выполняют на компьютере действия, не разрешенные пользователем. Они могут создавать свои копии, которые обладают способностью дальнейшего самовоспроизведения.

  Классический вирус

  Попав в систему, классический вирус заражает какой-либо файл, активизируется в нем, выполняет свое вредоносное действие, а затем добавляет свои копии в другие файлы.

Классический вирус размножается только на локальных ресурсах компьютера и не может самостоятельно проникать на другие компьютеры. Он может попасть на другой компьютер только в том случае, если добавит свою копию в файл, который хранится в папке общего доступа или на установленном компакт-диске, или если пользователь сам перешлет сообщение электронной почты с вложенным в него зараженным файлом.

Код классического вируса может внедряться в различные области компьютера, операционной системы или приложения. В зависимости от среды обитания вирусы подразделяют на *файловые*, *загрузочные*, *скриптовые* и *макро-вирусы*.

Вирусы могут заражать файлы различными способами. *Перезаписывающие* (Overwriting) вирусы записывают свой код вместо кода заражаемого файла, уничтожая его содержимое. Зараженный файл перестает работать, и его нельзя восстановить. *Паразитические* (Parasitic) вирусы изменяют файлы, оставляя их полностью или частично работоспособными. *Вирусы-компаньоны* (Companion) не изменяют файлы, но создают их двойники. При открытии зараженного файла запускается его двойник, то есть вирус. Среди вирусов встречаются также *вирусы-ссылки* (Link), вирусы, *заражающие объектные модули* (OBJ), вирусы, *заражающие библиотеки компиляторов* (LIB), вирусы, *заражающие исходные тексты программ*, и другие.

Червь

Код червя, как и код классического вируса, попав в систему, активизируется и выполняет свое вредоносное действие. Свое название червь получил благодаря способности "переползать" с компьютера на компьютер – без разрешения пользователя распространять свои копии через различные информационные каналы.

Основной признак, по которому черви различаются между собой, – способ их распространения. Описание типов червей по способу распространения приводится в следующей таблице.

Способы распространения червей

Тип	Название	Описание
Email-Worm	Почтовые черви	Распространяются через электронную почту. Зараженное сообщение электронной почты содержит прикрепленный файл с копией червя или ссылку на такой файл на веб-сайте, например, взломанном или специально созданном. Когда вы запускаете прикрепленный файл, червь активизируется; когда вы щелкаете на ссылке, загружаете, а затем открываете файл, червь также начинает выполнять свое вредоносное действие. После этого он продолжает распространять свои копии, разыскивая другие адреса электронной почты и отправляя по ним зараженные сообщения.
IM-Worm	Черви IM-клиентов	Распространяются через IM-клиенты. Обычно такой червь рассылает по контакт-листам сообщения, содержащие ссылку на файл с его копией на веб-сайте. Когда пользователь загружает файл и открывает его, червь активизируется.
IRC-Worm	Черви интернет-чатов	Распространяются через ретранслируемые интернет-чаты (Internet Relay Chats) – сервисные системы, с помощью которых можно общаться через интернет с другими людьми в реальном времени. Такой червь публикует в интернет-чате файл со своей копией или ссылку на файл. Когда пользователь загружает файл и открывает его, червь активизируется.
Net-Worm	Сетевые черви (черви компьютерных сетей)	Распространяются через компьютерные сети. В отличие от червей других типов, сетевой червь распространяется без участия пользователя. Он ищет в локальной сети компьютеры, на которых используются программы, содержащие уязвимости. Для этого он посылает специально сформированный сетевой пакет (эксплойт), который содержит код червя или его часть. Если в сети находится "уязвимый" компьютер, он принимает такой сетевой пакет. Полностью проникнув на компьютер, червь активизируется.

Тип	Название	Описание
P2P-Worm	Черви файлообменных сетей	Распространяются через файлообменные пиринговые сети. Чтобы внедриться в файлообменную сеть, червь копирует себя в каталог обмена файлами, обычно расположенный на компьютере пользователя. Файлообменная сеть отображает информацию об этом файле, и пользователь может "найти" зараженный файл в сети так же, как и любой другой, загрузить его и открыть. Более сложные черви имитируют сетевой протокол конкретной файлообменной сети: они положительно отвечают на поисковые запросы и предлагают для загрузки свои копии.
Worm	Прочие черви	К прочим сетевым червям относятся: • Черви, которые распространяют свои копии через сетевые ресурсы. Используя функции операционной системы, они перебирают доступные сетевые папки, подключаются к компьютерам в глобальной сети и пытаются открыть их диски на полный доступ. В отличие от описанных выше разновидностей червей, прочие черви активизируются не самостоятельно, а как только пользователь открывает файл с копией червя. • Черви, которые не относятся ни к одному из описанных в этой таблице способов распространения (например, те, которые распространяются через мобильные телефоны).

- **Троянские приложения (в том числе приложения-вымогатели)**

  Подкатегория: троянские программы (Trojan_programs)

  Уровень опасности: высокий

  В отличие от червей и вирусов, троянские программы не создают свои копии. Они проникают на компьютер, например, через электронную почту или через браузер, когда пользователь посещает зараженную веб-страницу. Троянские программы запускаются при участии пользователя. Они начинают выполнять свое вредоносное действие сразу после запуска.

  Разные троянские программы ведут себя на зараженном компьютере по-разному. Основные функции троянских программ – блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей. Кроме этого, троянские программы могут принимать или отправлять файлы, выполнять их, выводить на экран сообщения, обращаться к веб-страницам, загружать и устанавливать программы, перезагружать компьютер.

  Злоумышленники часто используют "наборы" из разных троянских программ.

  Типы поведения троянских программ описаны в следующей таблице.

  Типы поведения троянских программ на зараженном компьютере

Тип	Название	Описание
Trojan-ArcBomb	Троянские программы – "архивные бомбы"	Архивы; при распаковке увеличиваются до таких размеров, что нарушают работу компьютера. Когда пользователь пытается распаковать такой архив, компьютер может начать работать медленно или "зависнуть", диск может заполниться "пустыми" данными. "Архивные бомбы" особенно опасны для файловых и почтовых серверов. Если на сервере используется система автоматической обработки входящей информации, такая "архивная бомба" может остановить сервер.
Backdoor	Троянские программы удаленного администрирования	Считаются наиболее опасными среди троянских программ. По своим функциям напоминают устанавливаемые на компьютеры программы удаленного администрирования. Эти программы устанавливают себя в компьютере незаметно для пользователя и позволяют злоумышленнику удаленно управлять компьютером.
Trojan	Троянские программы	Включают следующие вредоносные программы: • **Классические троянские программы**. Эти программы выполняют только основные функции троянских программ: блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей. Они не имеют дополнительных функций, свойственных другим типам троянских программ, описанным в этой таблице. • **"Многоцелевые" троянские программы**. Эти программы имеют дополнительные функции, присущие сразу нескольким типам троянских программ.

Тип	Название	Описание
Trojan-Ransom	Троянские программы, требующие выкупа	"Берут в заложники" информацию на компьютере пользователя, изменяя или блокируя ее, или нарушают работу компьютера таким образом, чтобы пользователь не мог воспользоваться информацией. Злоумышленник требует от пользователя выкуп за обещание выслать программу, которая восстановит работоспособность компьютера и данные на нем.
Trojan-Clicker	Троянские программы-кликеры	С компьютера пользователя обращаются к веб-страницам: они или сами посылают команды браузеру, или заменяют хранящиеся в системных файлах веб-адреса. С помощью этих программ злоумышленники организовывают сетевые атаки, повышают посещаемость сайтов, чтобы увеличить количество показов рекламных баннеров.
Trojan-Downloader	Троянские программы-загрузчики	Обращаются к веб-странице злоумышленника, загружают с нее другие вредоносные программы и устанавливают их на компьютере пользователя; могут хранить имя файла загружаемой вредоносной программы в себе или получать его с веб-страницы, к которой обращаются.
Trojan-Dropper	Троянские программы-установщики	Сохраняют на диске компьютера, а затем устанавливают другие троянские программы, которые хранятся в теле этих программ. Злоумышленники могут использовать троянские программы-установщики, чтобы достичь следующих целей: • установить вредоносную программу незаметно для пользователя: троянские программы-установщики не отображают никаких сообщений или выводят на экран ложные сообщения, например, об ошибке в архиве или неверной версии операционной системы; • защитить от обнаружения другую известную вредоносную программу: не все антивирусы могут распознать вредоносную программу внутри троянской программы-установщика.
Trojan-Notifier	Троянские программы-уведомители	Сообщают злоумышленнику о том, что зараженный компьютер находится "на связи"; передают ему информацию о компьютере: IP-адрес, номер открытого порта или адрес электронной почты. Они связываются со злоумышленником по электронной почте, через FTP, обращаясь к его веб-странице или другим способом. Троянские программы-уведомители часто используются в наборах из разных троянских программ. Они извещают злоумышленника о том, что другие троянские программы успешно установлены на компьютере пользователя.
Trojan-Proxy	Троянские программы-прокси	Позволяют злоумышленнику анонимно обращаться через компьютер пользователя к веб-страницам; часто используются для рассылки спама.
Trojan-PSW	Троянские программы, крадущие пароли	Троянские программы, крадущие пароли (Password Stealing Ware); крадут учетные записи пользователей, например, регистрационную информацию к программному обеспечению. Они отыскивают конфиденциальные данные в системных файлах и реестре и пересылают ее "хозяину" по электронной почте, через FTP, обращаясь к веб-странице злоумышленника или другим способом. Некоторые из этих троянских программ выделены в отдельные типы, описанные в этой таблице. Это троянские программы, крадущие банковские счета (Trojan-Banker), троянские программы, крадущие данные пользователей IM-клиентов (Trojan-IM) и троянские программы, крадущие данные пользователей сетевых игр (Trojan-GameThief).
Trojan-Spy	Троянские программы-шпионы	Ведут электронный шпионаж за пользователем: собирают информацию о его действиях на компьютере, например, перехватывают данные, которые пользователь вводит с клавиатуры, делают снимки экрана или собирают списки активных приложений. Получив эту информацию, они передают ее злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Trojan-DDoS	Троянские программы – сетевые атаки	Отправляют с компьютера пользователя многочисленные запросы на удаленный сервер. У сервера не хватает ресурсов для обработки запросов, и он перестает работать (Denial-of-Service (DoS) – отказ в обслуживании). Такими программами часто заражают многие компьютеры, чтобы с них одновременно атаковать один сервер. DoS-программы реализуют атаку с одного компьютера с ведома пользователя. DDoS-программы (Distributed DoS) реализуют распределенные атаки с разных компьютеров, причем без ведома пользователя зараженного компьютера.
Trojan-IM	Троянские программы, крадущие данные пользователей IM-клиентов	Крадут номера и пароли пользователей IM-клиентов. Передают данные злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Rootkit	Руткиты	Скрывают другие вредоносные программы и их активность и таким образом продлевают пребывание этих программ в системе; могут скрывать файлы, процессы в памяти зараженного компьютера или ключи реестра, которые запускают вредоносные программы; могут скрывать обмен данными между приложениями на компьютере пользователя и других компьютерах в сети.
Trojan-SMS	Троянские программы – SMS-сообщения	Заражают мобильные телефоны и с них отправляют SMS-сообщения на платные номера.

Тип	Название	Описание
Trojan-GameThief	Троянские программы, крадущие данные пользователей сетевых игр	Крадут учетные данные пользователей сетевых компьютерных игр; передают их злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Trojan-Banker	Троянские программы, крадущие банковские счета	Крадут данные банковских счетов или счетов в системах электронных денег; передают данные злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Trojan-Mailfinder	Троянские программы – сборщики адресов электронной почты	Собирают адреса электронной почты на компьютере и передают их злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом. По собранным адресам злоумышленники могут рассылать спам.

- **Вредоносные утилиты**

  Подкатегория: вредоносные утилиты (Malicious_tools)

  Уровень опасности: средний

  Вредоносные утилиты, в отличие от других вредоносных программ, не выполняют своих действий сразу при запуске и могут безопасно храниться и запускаться на компьютере пользователя. Злоумышленники используют функции этих программ для создания вирусов, червей и троянских программ, организации сетевых атак на удаленные серверы, "взлома" компьютеров или других вредоносных действий.

  Разнообразные функции вредоносных утилит делятся на типы, которые описаны в следующей таблице.

  Функции вредоносных утилит

Тип	Название	Описание
Constructor	Конструкторы	Позволяют создавать новые вирусы, черви и троянские программы. Некоторые конструкторы имеют стандартный оконный интерфейс, в котором с помощью меню можно выбирать тип создаваемой вредоносной программы, способ ее противодействия отладчику и другие свойства.
Dos	Сетевые атаки	Отправляют с компьютера пользователя многочисленные запросы на удаленный сервер. У сервера не хватает ресурсов для обработки запросов, и он перестает работать (Denial-of-Service (DoS) – отказ в обслуживании).
Exploit	Эксплойты	*Эксплойт* – это набор данных или программный код, использующий уязвимости приложения, в котором он обрабатывается, чтобы выполнить на компьютере вредоносное действие. Например, эксплойт может записывать или считывать файлы либо обращаться к "зараженным" веб-страницам. Разные эксплойты используют уязвимости разных приложений или сетевых служб. Эксплойт в виде сетевого пакета передается по сети на многие компьютеры, выискивая компьютеры с уязвимыми сетевыми службами. Эксплойт в файле DOC использует уязвимости текстового редактора. Он может начать выполнять заложенные в него злоумышленником функции, когда пользователь откроет зараженный файл. Эксплойт, внедренный в сообщение электронной почты, ищет уязвимости в каком-либо почтовом клиенте. Он может начать выполнять вредоносное действие, как только пользователь откроет зараженное сообщение в этом почтовом клиенте. С помощью эксплойтов распространяются сетевые черви (Net-Worm). Эксплойты-ньюкеры (Nuker) представляют собой сетевые пакеты, которые выводят компьютеры из строя.
FileCryptor	Шифровальщики	Шифруют другие вредоносные программы, чтобы скрыть их от антивирусного приложения.
Flooder	Программы для "замусоривания" сетей	Рассылают многочисленные сообщения по сетевым каналам. К этому типу относятся, например, программы для замусоривания ретранслируемых интернет-чатов (Internet Relay Chats). К типу Flooder не относятся программы, "забивающие мусором" каналы электронной почты, IM-клиентов и мобильных систем. Эти программы выделяют в отдельные типы, описанные в этой таблице (Email-Flooder, IM-Flooder и SMS-Flooder).
HackTool	Инструменты хакера	Позволяют взламывать компьютер, на котором они установлены, или атаковать другой компьютер (например, без разрешения пользователя добавлять других пользователей системы; очищать системные журналы, чтобы скрыть следы присутствия в системе). К этому типу относят некоторые снифферы, которые обладают вредоносными функциями, например перехватывают пароли. Снифферы (Sniffers) – это программы, которые позволяют просматривать сетевой трафик.

Тип	Название	Описание
Hoax	Злые шутки	Пугают пользователя вирусоподобными сообщениями: могут "обнаружить" вирус в незараженном файле или объявить о форматировании диска, которого на самом деле не происходит.
Spoofer	Утилиты-имитаторы	Отправляют сообщения и сетевые запросы с поддельным адресом отправителя. Злоумышленники используют утилиты-имитаторы, чтобы, например, выдать себя за отправителя.
VirTool	Инструменты для модификации вредоносных программ	Позволяют модифицировать другие вредоносные программы так, чтобы скрыть их от антивирусных приложений.
Email-Flooder	Программы для "замусоривания" адресов электронной почты	Отправляют многочисленные сообщения по адресам электронной почты ("забивают их мусором"). Большой поток сообщений не дает пользователям просматривать полезную входящую почту.
IM-Flooder	Программы для "замусоривания" IM-клиентов	Отправляют многочисленные сообщения пользователям IM-клиентов. Большой поток сообщений не дает пользователям просматривать полезные входящие сообщения.
SMS-Flooder	Программы для "замусоривания" SMS-сообщениями	Отправляют многочисленные SMS-сообщения на мобильные телефоны.

- **Рекламные приложения**

  Подкатегория: рекламные программы (Adware)

  Уровень опасности: средний

  Рекламные программы связаны с показом пользователю рекламной информации. Они отображают в интерфейсе других программ рекламные баннеры, перенаправляют поисковые запросы на рекламные веб-страницы. Некоторые из них собирают и переправляют своему разработчику маркетинговую информацию о пользователе: например, сведения о том, какие тематические веб-сайты он посещает, какие поисковые запросы делает. В отличие от троянских программ-шпионов, рекламные программы передают эту информацию разработчику с разрешения пользователя.

- **Приложения автодозвона**

  Подкатегория: Приложения автодозвона (Dialer).

  Уровень опасности: средний

  Приложения автодозвона могут устанавливать телефонные соединения через модем в скрытом режиме.

- **Легальные приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя**

  Подкатегория: легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

  Уровень опасности: средний

  Большинство этих программ являются полезными, и многие пользователи применяют их. Среди таких программ – IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

  Однако если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать некоторые их функции для нарушения безопасности.

Подобные программы различают по функциям, типы которых описаны в таблице ниже.

Тип	Название	Описание
Client-IRC	Клиенты интернет-чатов	Пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.
Downloader	Программы-загрузчики	Могут загружать файлы с веб-страниц в скрытом режиме.
Monitor	Программы-мониторы	Позволяют наблюдать за активностью на компьютере, на котором установлены (видеть, какие приложения работают и как они обмениваются данными с приложениями на других компьютерах).
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры пользователей злоумышленники.
RemoteAdmin	Программы удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры пользователей для наблюдения за удаленными компьютерами и управления ими. Легальные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные программы этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на локальном компьютере	Дают пользователю дополнительные возможности при работе на своем компьютере (позволяют скрывать на своем компьютере файлы или окна активных приложений, закрывать активные процессы).
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

- **Упакованные объекты, способ упаковки которых может использоваться для защиты вредоносного кода**

  Подкатегория: Упакованные файлы, которые могут нанести вред.

  Уровень опасности: средний.

  Файл упакован специальным упаковщиком, который используется для упаковки вредоносных программ: вирусов, червей, троянских программ. Kaspersky Endpoint Security проверяет модуль-распаковщик в составе самораспаковывающихся архивов SFX (self-extracting archive).

Чтобы скрыть вредоносные программы от обнаружения антивирусом, злоумышленники упаковывают их с помощью специальных упаковщиков. Специалисты "Лаборатории Касперского" выделили упаковщики, которые злоумышленники используют чаще всего.

- **Многократно упакованные объекты**

  Подкатегория: Многократно упакованные файлы.

  Уровень опасности: средний.

  Файл упакован одним или несколькими упаковщиками три или более раз.

  Чтобы скрыть вредоносные программы от обнаружения антивирусом, злоумышленники многократно упаковывают один файл. Kaspersky Endpoint Security проверяет упакованные файлы.

По умолчанию Kaspersky Endpoint Security обнаруживает все типы объектов. Рекомендуется оставить обнаружение всех типов объектов для обеспечения безопасности компьютера. Если вы используете собственные утилиты, которые приложение обнаруживает как вредоносные, добавьте эти утилиты в список исключений, но не выключайте обнаружение этого типа объектов.

Как выбрать типы обнаруживаемых объектов в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Общие настройки** → **Исключения и типы объектов**.
5. В блоке **Типы обнаруживаемых объектов** нажмите на кнопку **Настройка**.
6. В открывшемся окне установите флажки для типов объектов, которые должен обнаруживать Kaspersky Endpoint Security.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

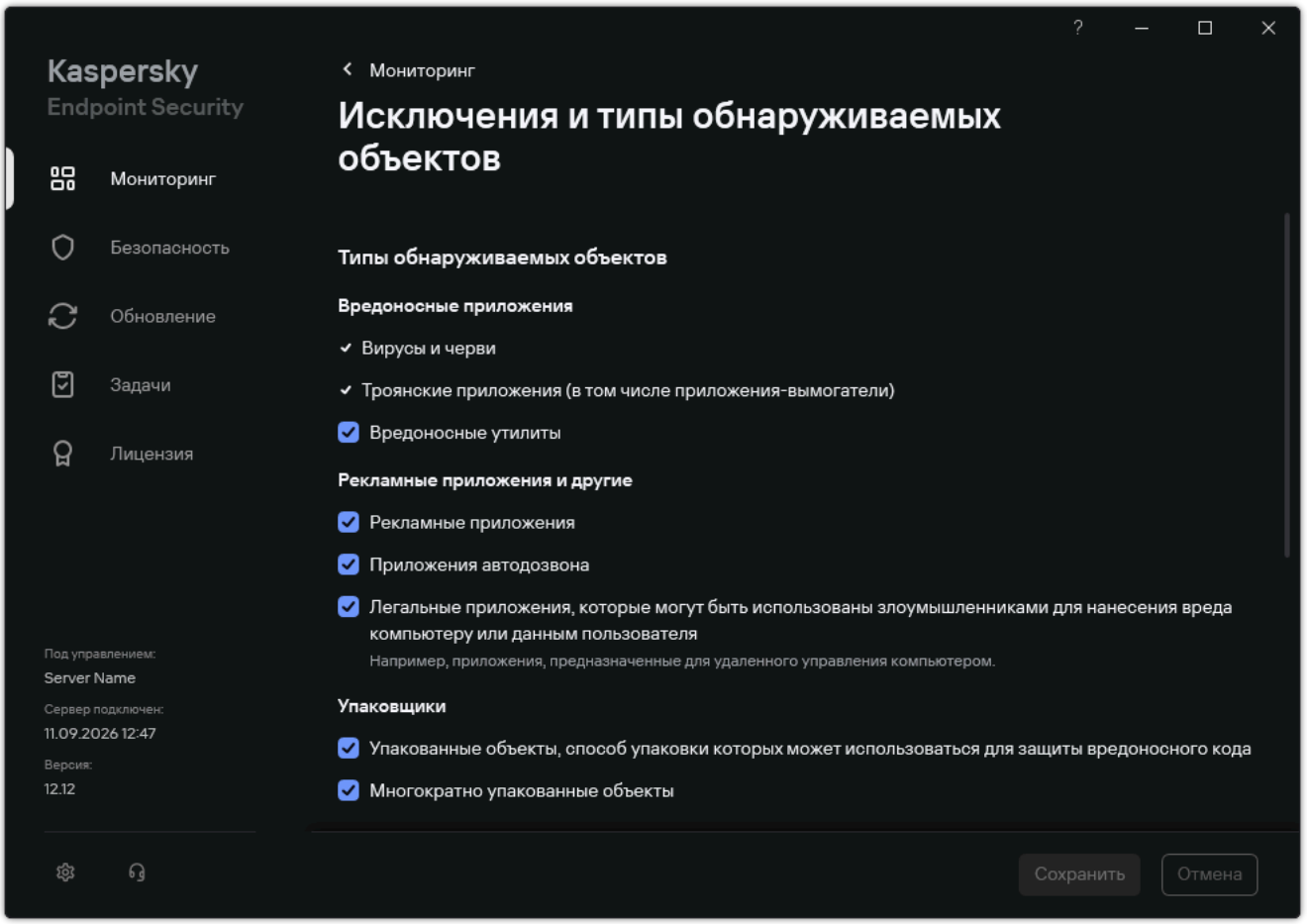
Как выбрать типы обнаруживаемых объектов в Web Console и Cloud Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки обнаружения**.
5. В блоке **Обнаружение других типов объектов** установите флажки для типов объектов, которые должен обнаруживать Kaspersky Endpoint Security.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как выбрать типы обнаруживаемых объектов в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.
3. В блоке **Типы обнаруживаемых объектов** установите флажки для типов объектов, которые должен обнаруживать Kaspersky Endpoint Security.
4. Сохраните внесенные изменения.



Типы обнаруживаемых объектов

Формирование списка доверенных приложений

Список доверенных приложений – это список приложений, у которых Kaspersky Endpoint Security не контролирует файловую и сетевую активности (в том числе и вредоносную), а также обращения этих приложений к системному реестру. По умолчанию Kaspersky Endpoint Security контролирует объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех приложений и создаваемый ими сетевой трафик. После добавления приложения в список доверенных приложений Kaspersky Endpoint Security перестает контролировать активность приложения.

Отличие исключений из проверки от доверенных приложений заключается в том, что для исключений Kaspersky Endpoint Security не проверяет файлы, а для доверенных приложений инициируемые процессы. То есть, если доверенное приложение создаст вредоносный файл в папке, которая не включена в исключения, Kaspersky Endpoint Security обнаружит этот файл и устранит угрозу. Если папка добавлена в исключения, Kaspersky Endpoint Security пропустит этот файл.

Например, если вы считаете объекты, используемые приложением Microsoft Windows Блокнот, безопасными, то есть доверяете этому приложению, вам следует добавить приложение Microsoft Windows Блокнот в список доверенных приложений, чтобы не контролировать объекты, используемые этим приложением. Это позволит увеличить производительность компьютера, что особенно важно при использовании серверных приложений.

Кроме того, некоторые действия, которые Kaspersky Endpoint Security классифицирует как подозрительные, могут быть безопасны в рамках функциональности ряда приложений. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием приложения автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких приложений и отключить контроль их активности, рекомендуется добавить их в список доверенных приложений.

Доверенные приложения позволяют избежать проблемы совместимости Kaspersky Endpoint Security с другими приложениями (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky Endpoint Security и другого антивирусного приложения).

В то же время исполняемый файл и процесс доверенного приложения по-прежнему проверяются на наличие в них вирусов и других приложений, представляющих угрозу. Для полного исключения приложения из проверки Kaspersky Endpoint Security следует пользоваться исключениями из проверки.

Как добавить приложение в список доверенных в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Общие настройки** → **Исключения и типы объектов**.
5. В блоке **Исключения из проверки и доверенные приложения** → **Доверенные приложения** нажмите на кнопку **Настройка**.

   Откроется окно со списком доверенных приложений.
6. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных приложений для всех компьютеров организации. Списки доверенных приложений родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные приложения родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных приложений родительской политики невозможно.
7. Установите флажок **Разрешить использование локальных доверенных приложений**, если вы хотите чтобы у пользователя была возможность создать локальный список доверенных приложений. Таким образом, кроме общего списка доверенных приложений, сформированного в политике, пользователь может создавать собственный локальный список доверенных приложений. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера.

   Если флажок снят, пользователю доступен только общий список доверенных приложений, сформированный в политике. Также, если флажок снят, Kaspersky Endpoint Security скрывает для просмотра общий список доверенных приложений в интерфейсе приложения.

8. Нажмите на кнопку **Добавить** и выберите нужное действие:

- **Категорию**. Вы можете группировать доверенные приложения в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно доверенное приложение.
- **Новое исключение**. Kaspersky Endpoint Security добавляет новое доверенное приложение в корень списка.
- **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные доверенные приложения*. Также в приложение добавлены предустановленные доверенные приложения для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные доверенные приложения.
- **Новое исключение в выбранную категорию**. Для добавления нового доверенного приложения в отдельную категорию выберите категорию.

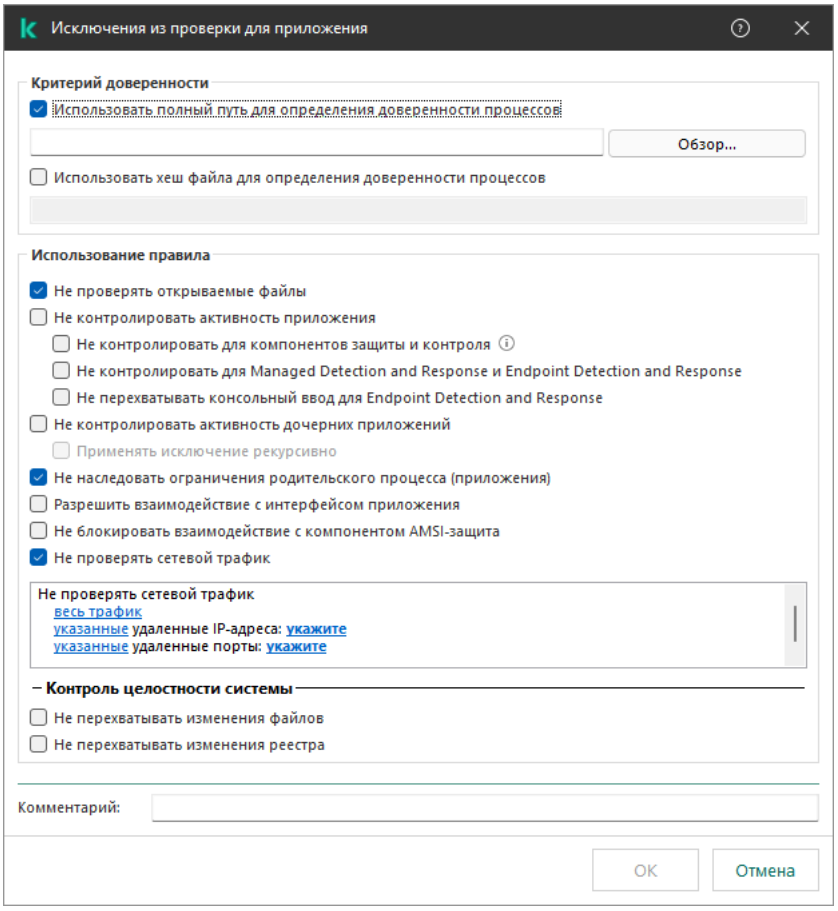
9. Выберите критерий доверенности:

- **Использовать полный путь для определения доверенности процессов**. Введите путь к исполняемому файлу доверенного приложения.

  Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

  Kaspersky Endpoint Security учитывает регистр имени файла доверенного приложения. Если вы ввели имя файла в неверном регистре, Kaspersky Endpoint Security не распознает доверенное приложение.
- **Использовать хеш файла для определения доверенности процессов**.

Kaspersky Endpoint Security не поддерживает переменную среды `%userprofile%` при формировании списка доверенных приложений через консоль Kaspersky Security Center. Чтобы применить запись ко всем учетным записям, вы можете использовать символ * (например, `C:\Users\*\Documents\File.exe`). При добавлении новой переменной среды нужно перезапустить приложение.

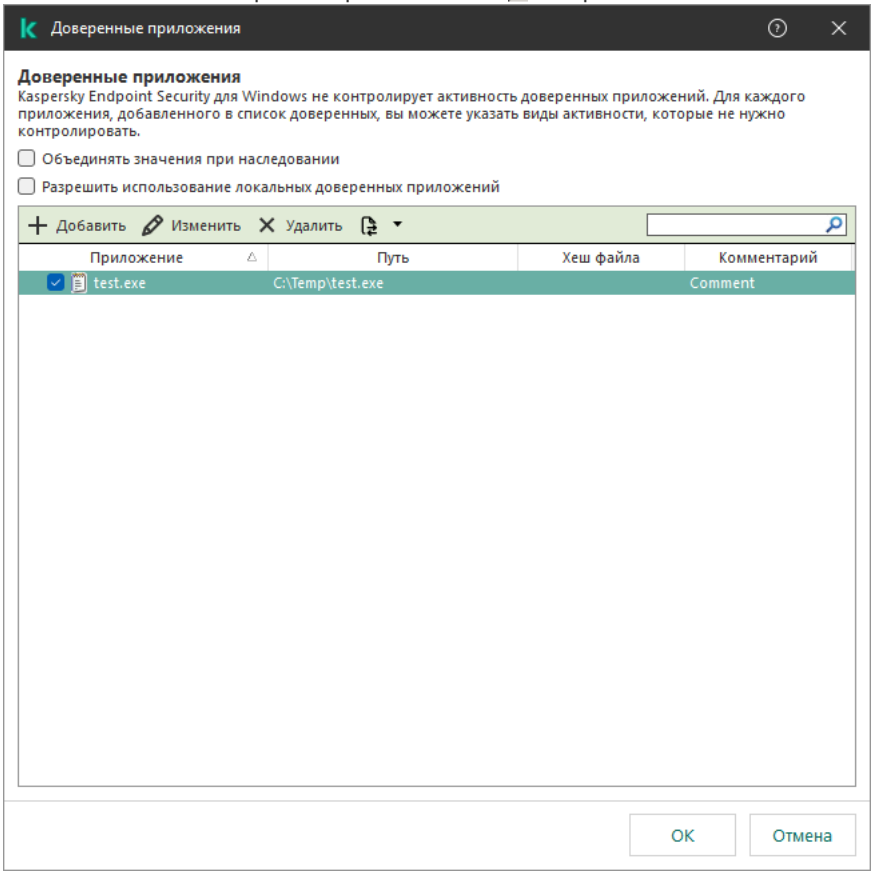


Параметры доверенного приложения

10. Настройте дополнительные параметры доверенного приложения (см. таблицу ниже).
11. Нажмите на кнопку **OK**.

    Новое доверенное приложение будет добавлено в список. Вы можете в любое время исключить приложение из доверенной зоны с помощью флажка напротив объекта.

12. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.



Список доверенных приложений

Как добавить приложение в список доверенных в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона**.
5. В открывшемся окне перейдите по ссылке **Приложения**.

   Откроется окно со списком доверенных приложений.
6. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных приложений для всех компьютеров организации. Списки доверенных приложений родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные приложения родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных приложений родительской политики невозможно.

7. Установите флажок **Разрешить использование локальных исключений**, если вы хотите чтобы у пользователя была возможность создать локальный список доверенных приложений. Таким образом, кроме общего списка доверенных приложений, сформированного в политике, пользователь может создавать собственный локальный список доверенных приложений. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера.

   Если флажок снят, пользователю доступен только общий список доверенных приложений, сформированный в политике. Также, если флажок снят, Kaspersky Endpoint Security скрывает для просмотра общий список доверенных приложений в интерфейсе приложения.

8. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категория**. Вы можете группировать доверенные приложения в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно доверенное приложение.
   - **Новое исключение**. Kaspersky Endpoint Security добавляет новое доверенное приложение в корень списка.
   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные доверенные приложения*. Также в приложение добавлены предустановленные доверенные приложения для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные доверенные приложения.

   Для добавления нового доверенного приложения в отдельную категорию установите флажок рядом с этой категорией и выберите вариант **Новое исключение**.

9. Выберите критерий доверенности:

   - **Путь к файлу или папке**. Введите путь к исполняемому файлу доверенного приложения.

     Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

     Kaspersky Endpoint Security учитывает регистр имени файла доверенного приложения. Если вы ввели имя файла в неверном регистре, Kaspersky Endpoint Security не распознает доверенное приложение.

   - **Хеш приложения**.

   Kaspersky Endpoint Security не поддерживает переменную среды %userprofile% при формировании списка доверенных приложений через консоль Kaspersky Security Center. Чтобы применить запись ко всем учетным записям, вы можете использовать символ `*` (например, `C:\Users\*\Documents\File.exe`). При добавлении новой переменной среды нужно перезапустить приложение.

10. Настройте дополнительные параметры доверенного приложения (см. таблицу ниже).

11. Нажмите на кнопку **OK**.

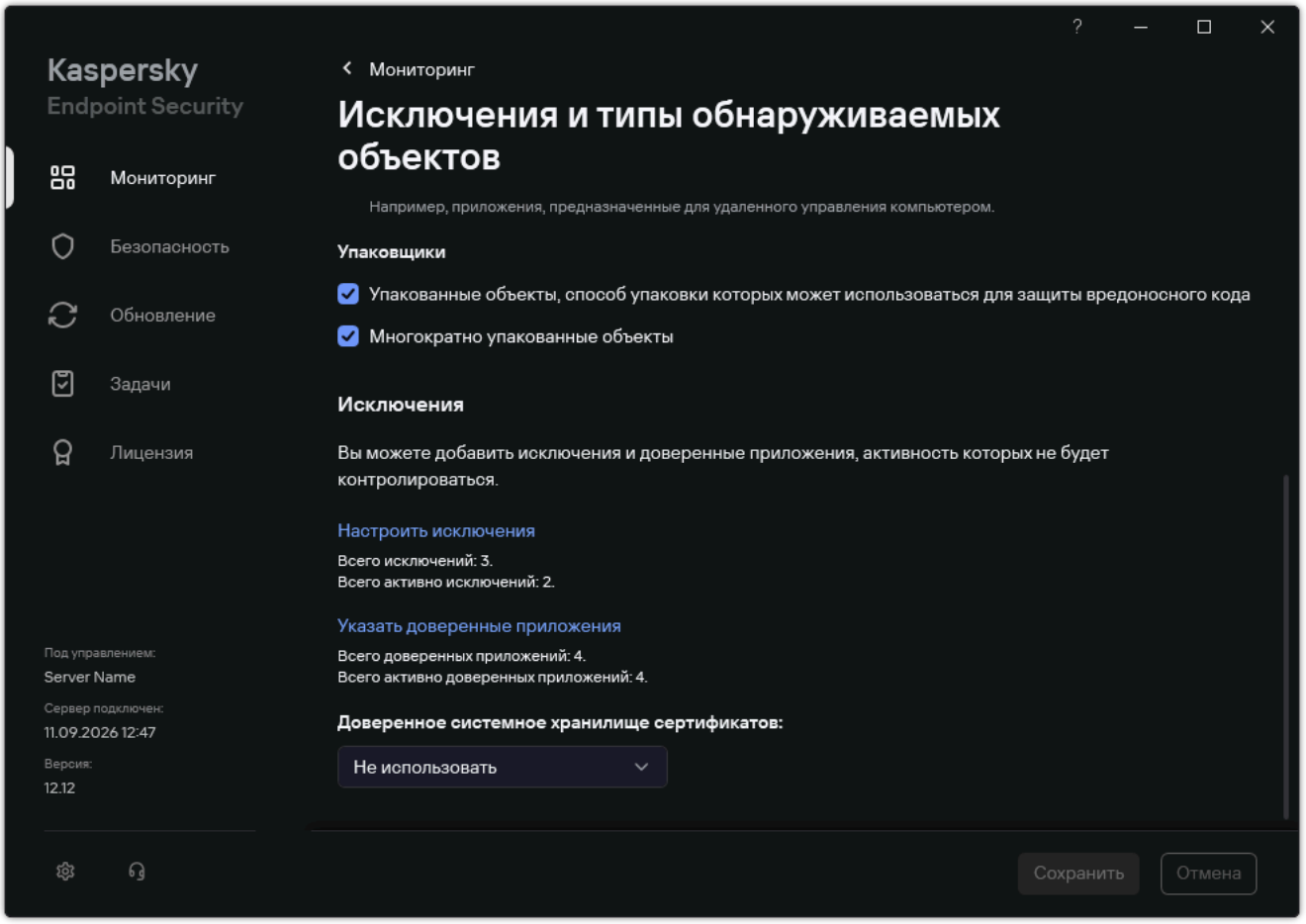
    Новое доверенное приложение будет добавлено в список. Вы можете в любое время исключить приложение из доверенной зоны с помощью флажка в графе **Статус**.

12. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как добавить приложение в список доверенных в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.
3. В блоке **Исключения** перейдите по ссылке **Указать доверенные приложения**.

Kaspersky Endpoint Security скрывает для просмотра список доверенных приложений в интерфейсе приложения, если администратор в консоли запретил настройку доверенных приложений ("замок" закрыт) и запретил использование локальных доверенных приложений (флажок **Разрешить использование локальных доверенных приложений** снят).



Параметры исключений

4. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категорию**. Вы можете группировать доверенные приложения в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно доверенное приложение.

   - **Новое исключение**. Kaspersky Endpoint Security добавляет новое доверенное приложение в корень списка.

   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные доверенные приложения*. Также в приложение добавлены предустановленные доверенные приложения для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные доверенные приложения.

   Для добавления нового доверенного приложения в отдельную категорию установите флажок рядом с этой категорией и выберите вариант **Новое исключение**.

5. Выберите критерий доверенности:

   - **Использовать полный путь для определения доверенности процессов**. Введите путь к исполняемому файлу доверенного приложения.

     Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

     Kaspersky Endpoint Security учитывает регистр имени файла доверенного приложения. Если вы ввели имя файла в неверном регистре, Kaspersky Endpoint Security не распознает доверенное приложение.

   - **Использовать хеш файла для определения доверенности процессов**.

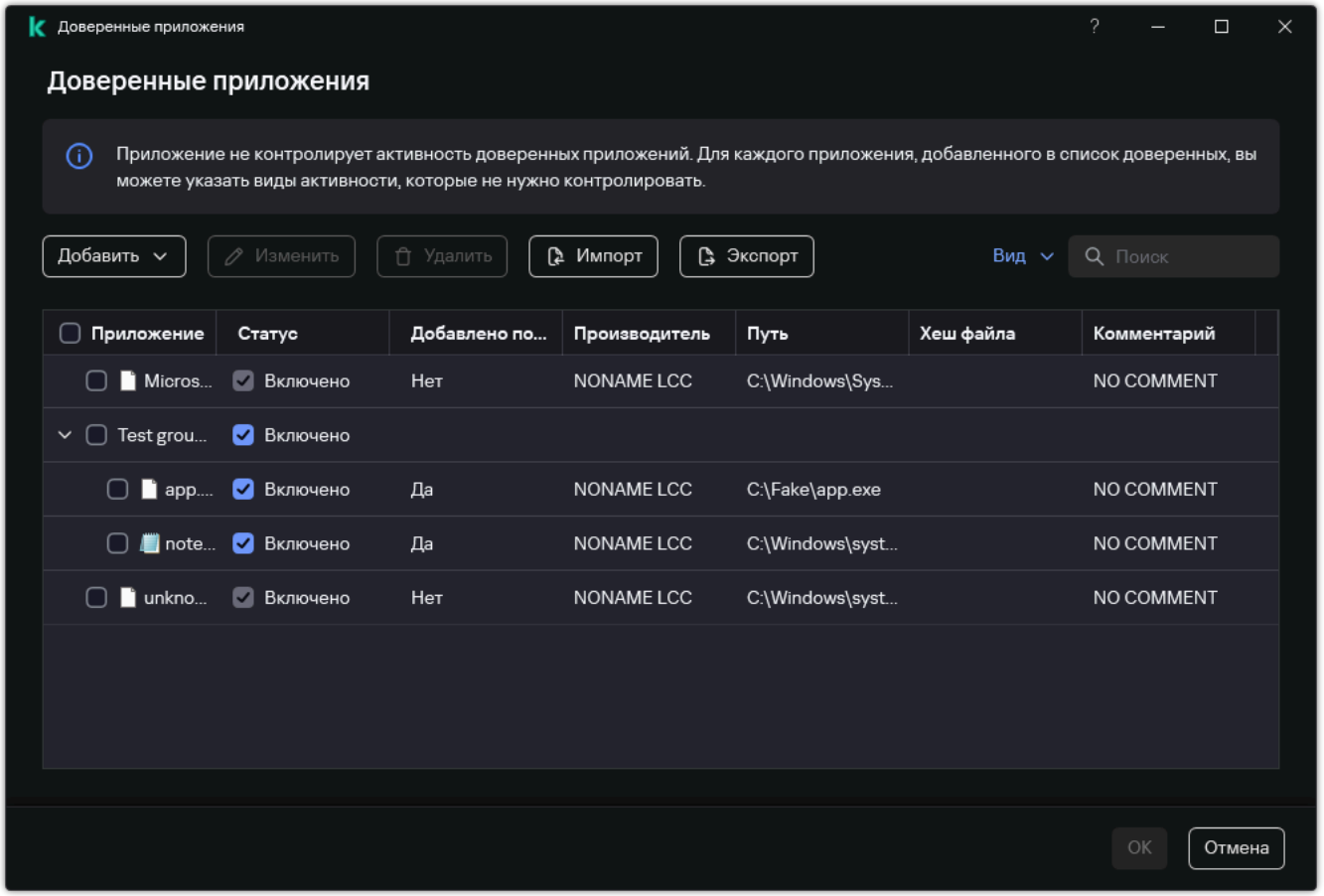
   Kaspersky Endpoint Security поддерживает переменные среды. При этом Kaspersky Endpoint Security конвертирует путь в локальном интерфейсе приложения. То есть, если вы ввели путь к файлу `%userprofile%\Documents\File.exe`, в локальном интерфейсе приложения для пользователя Fred123 будет добавлена запись `C:\Users\Fred123\Documents\File.exe`. Соответственно, Kaspersky Endpoint Security игнорирует доверенное приложение `File.exe` для других пользователей. Чтобы применить запись ко всем учетным записям, вы можете использовать символ `*` (например, `C:\Users\*\Documents\File.exe`). При добавлении новой переменной среды нужно перезапустить приложение.

6. В окне свойств доверенного приложения настройте дополнительные параметры.

7. Нажмите на кнопку **OK**.

   Новое доверенное приложение будет добавлено в список. Вы можете в любое время исключить приложение из доверенной зоны с помощью флажка в графе **Статус**.

8. Сохраните внесенные изменения.



Список доверенных приложений

Параметры доверенного приложения

Параметр	Описание
Не проверять открываемые файлы	Kaspersky Endpoint Security исключает из проверки все файлы, открываемые с помощью приложения. Например, если вы используете приложения резервного копирования файлов, функция позволит снизить потребление ресурсов компьютера Kaspersky Endpoint Security.
Не контролировать активность приложения	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложения в операционной системе. Вы можете настроить контроль активности приложения для разных компонентов Kaspersky Endpoint Security: • **Не контролировать для компонентов защиты и контроля**. Контроль за активностью приложения выполняют следующие компоненты: Анализ поведения, Защита от эксплойтов, Предотвращение вторжений, Откат вредоносных действий и Сетевой экран. • **Не контролировать для Managed Detection and Response и Endpoint Detection and Response**. Контроль за активностью приложения выполняют встроенный агент MDR и встроенный агент EDR (KATA). • **Не перехватывать консольный ввод для Endpoint Detection and Response**. Kaspersky Endpoint Security не отправляет данные телеметрии об управлении приложением через консоль. Данные телеметрии использует Kaspersky Anti Targeted Attack Platform (EDR).
Не контролировать активность дочерних приложений	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложений, которые запускает приложение. Вы можете применить исключение рекурсивно. То есть приложение не контролирует активность всей цепочки дочерних приложений.
Не наследовать ограничения родительского процесса (приложения)	Kaspersky Endpoint Security не применяет ограничения к процессу, которые настроены для родительского процесса. Родительский процесс запускает приложение, для которой настроены права приложения (Предотвращение вторжений) и сетевые правила приложения (Сетевой экран).
Не контролировать активность дочерних приложений	Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложений, которые запускает приложение. Вы можете применить исключение рекурсивно. То есть приложение не контролирует активность всей цепочки дочерних приложений.
Разрешить взаимодействие с интерфейсом приложения	Самозащита Kaspersky Endpoint Security блокирует все попытки управления службами приложения с удаленного компьютера. Если флажок установлен, то приложению удаленного доступа к компьютеру разрешено управлять параметрами Kaspersky Endpoint Security через интерфейс Kaspersky Endpoint Security.

Параметр	Описание
Не блокировать взаимодействие с компонентом AMSI-защита	Kaspersky Endpoint Security не контролирует запросы доверенного приложения на проверку объектов компонентом AMSI-защита.
Не проверять сетевой трафик	Kaspersky Endpoint Security исключает из проверки сетевой трафик, инициируемый приложением. Вы можете исключить из проверки весь трафик или только зашифрованный трафик. Также вы можете исключить из проверки отдельные IP-адреса или номера портов. Kaspersky Endpoint Security версии 14.0 и ниже не поддерживает исключение сетевого трафика, если для доверенного приложения указан хеш, а не путь.
Не перехватывать изменения файлов *(доступен только в консоли Kaspersky Security Center)*	Kaspersky Endpoint Security не контролирует изменения в файлах из области мониторинга Контроля целостности системы. Приложение применяет исключение для всех режимов работы Контроля целостности системы: режим реального времени и проверка целостности системы по запросу.
Не перехватывать изменения реестра *(доступен только в консоли Kaspersky Security Center)*	Kaspersky Endpoint Security не контролирует изменения ключей реестра из области мониторинга Контроля целостности системы. Приложение применяет исключение для всех режимов работы Контроля целостности системы: режим реального времени и проверка целостности системы по запросу.
Комментарий	Если необходимо, вы можете ввести краткий комментарий к доверенному приложению. Комментарий позволяет упростить поиск и сортировку доверенных приложений.
Статус	Статус доверенного приложения: • **Активно** – приложение в доверенной зоне. • **Неактивно** – приложение исключено из доверенной зоны.

Создание локальной доверенной зоны

У пользователя есть возможность формировать собственную локальную доверенную зону для отдельного компьютера. Таким образом, кроме общей доверенной зоны, сформированной в политике, пользователь может создавать собственные локальные списки исключений из проверки и доверенных приложений. Администратор может разрешить или запретить использование локальных исключений или локальных доверенных приложений в параметрах политики. Для этого предназначены флажки **Разрешить использование локальных исключений** и **Разрешить использование локальных доверенных приложений** в разделе политики **Исключения**.

Если администратор разрешил формировать локальную доверенную зону, пользователь может добавлять собственные исключения из проверки и доверенные приложения в интерфейсе приложения. При этом у пользователя нет прав на изменение или удаление объектов из доверенной зоны, заданной в политике. Также администратор может просматривать, добавлять, изменять или удалять элементы списка в консоли Kaspersky Security Center, если необходимо добавить исключения для отдельного компьютера.

Kaspersky Endpoint Security скрывает для просмотра списки исключений из проверки и доверенных приложений в интерфейсе приложения, если администратор в консоли запретил настройку доверенной зоны ("замок" закрыт) и запретил использование локальных исключений из проверки и доверенных приложений.

Как добавить объект в локальную доверенную зону в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите вкладку **Устройства**.

4. Откройте свойства компьютера двойным щелчком мыши.

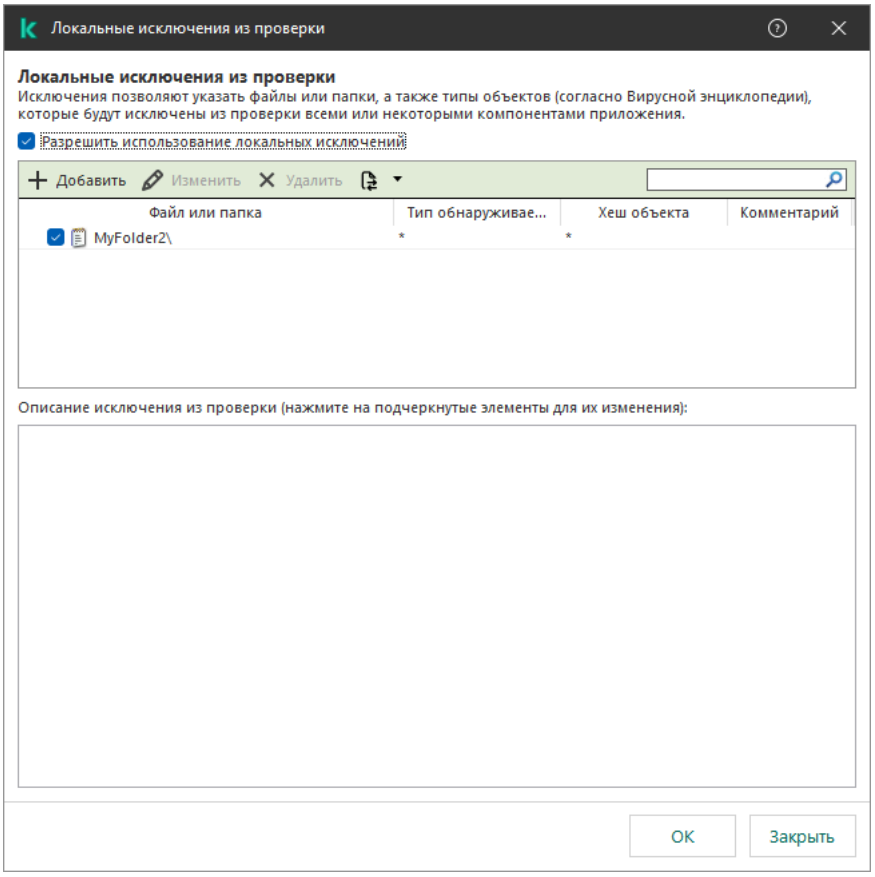
5. В окне свойств компьютера выберите раздел **Приложения**.

6. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows (14.3)** и откройте свойства приложения двойным щелчком мыши.

7. В окне параметров приложения выберите раздел **Общие настройки → Исключения и типы объектов**.

8. В блоке **Исключения из проверки и доверенные приложения → Локальные исключения из проверки** нажмите на кнопку **Настройка**.

   Откроется окно со списком локальных исключений.



Параметры доверенной зоны

9. Сформируйте список локальных исключений из проверки.

   Правила создания локальных исключений из проверки не отличаются от правил создания общих исключений. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

10. В блоке **Исключения из проверки и доверенные приложения → Локальные доверенные приложения** нажмите на кнопку **Настройка**.

    Откроется окно со списком локальных доверенных приложений.

11. Сформируйте список локальных доверенных приложений.

    Правила добавления приложений в список локальных доверенных приложений не отличаются от правил добавления в общий список. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.

12. Сохраните внесенные изменения.

Как добавить объект в локальную доверенную зону в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите предоставить пользователю разрешение на выполнение запрещенного действия.
3. Выберите вкладку **Приложения**.
4. Нажмите на **Kaspersky Endpoint Security для Windows**.

   Откроются локальные параметры приложения.

5. Выберите вкладку **Параметры приложения**.
6. В окне параметров приложения выберите раздел **Общие настройки** → **Исключения и типы обнаруживаемых объектов**.
7. В блоке **Исключения из проверки и доверенные приложения** перейдите по ссылке **Локальные исключения из проверки**.
8. Сформируйте список локальных исключений из проверки.

   Правила создания локальных исключений не отличаются от правил создания общих исключений. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.

9. В блоке **Исключения из проверки и доверенные приложения** перейдите по ссылке **Локальные доверенные приложения**.
10. Сформируйте список локальных доверенных приложений.

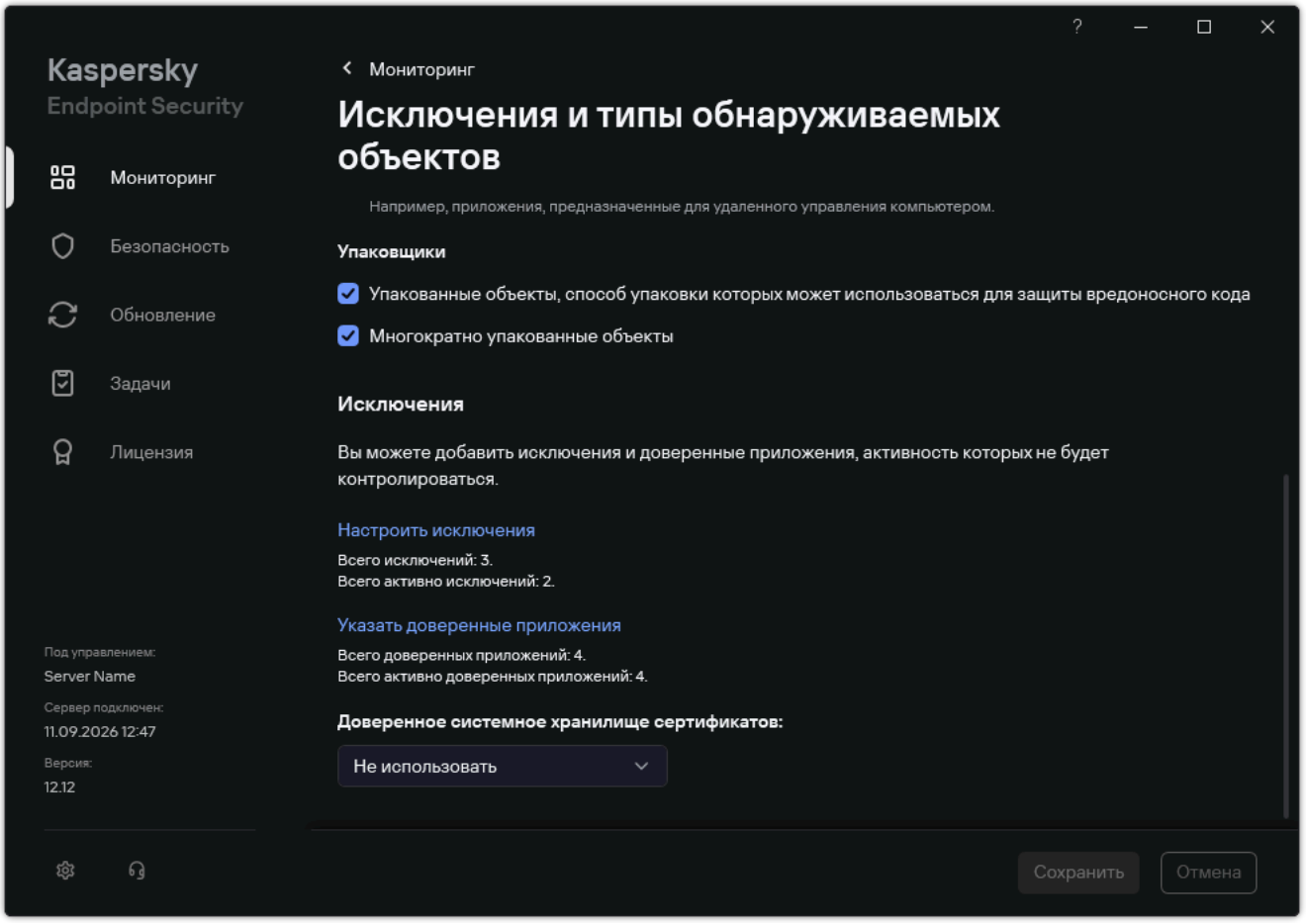
    Правила добавления приложений в список локальных доверенных приложений не отличаются от правил добавления в общий список. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.

11. Сохраните внесенные изменения.

Как создать локальное исключение из проверки в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.
3. В блоке **Исключения** перейдите по ссылке **Настроить исключения**.

Kaspersky Endpoint Security скрывает для просмотра список исключений из проверки в интерфейсе приложения, если администратор в консоли запретил настройку исключений из проверки ("замок" закрыт) и запретил использование локальных исключений из проверки (флажок **Разрешить использование локальных исключений** снят).



Параметры исключений

4. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категорию**. Вы можете группировать исключения из проверки в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно исключение из проверки.

   - **Новое исключение**. Kaspersky Endpoint Security добавляет новое исключение из проверки в корень списка.

   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные исключения из проверки*. Также в приложение добавлены предустановленные исключения из проверки для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные исключения из проверки.

   Для добавления нового исключения из проверки в отдельную категорию установите флажок рядом с этой категорией и выберите вариант **Новое исключение**.

5. Если вы хотите исключить из проверки файл или папку, выберите файл или папку, нажав на кнопку **Обзор**.

Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

  Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `?:\Users\*\Folder\`.

  Вы можете исключать сетевые папки. Для этого введите путь к сетевой папке вручную (например, `\\Network Share\*`).

6. Если вы хотите исключить из проверки тип объектов, в поле **Тип обнаруживаемого объекта** введите название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

   Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, Kaspersky Endpoint Security исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

7. Если вы хотите исключить из проверки отдельный файл, в поле **Хеш объекта** введите хеш файла.

   Если файл изменится, хеш файла тоже будет изменен. В результате измененный файл не будет добавлен в исключения.

8. В блоке **Компоненты защиты** выберите компоненты, на работу которых должно распространяться исключение из проверки.

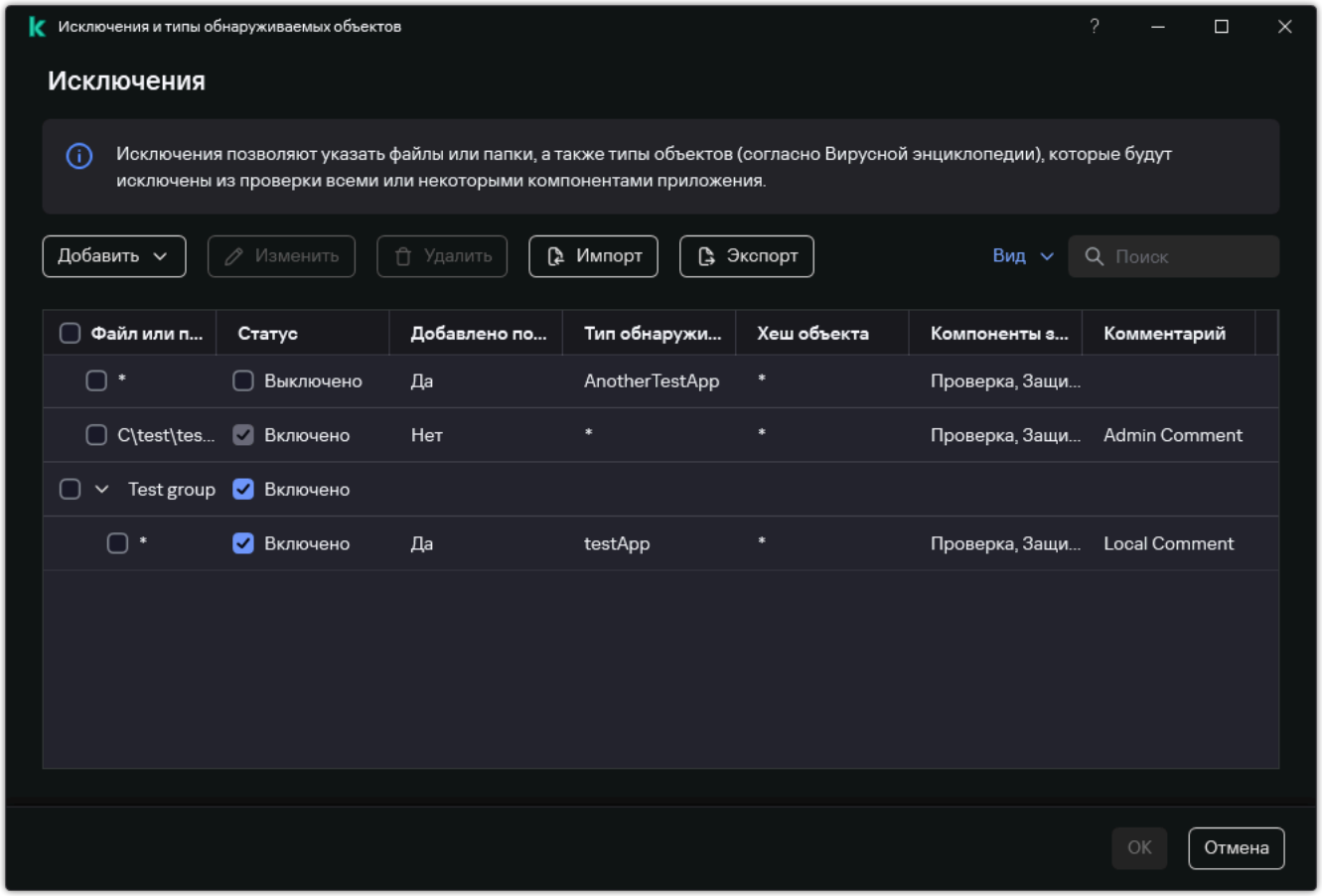
9. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

10. Установите статус для исключения **Активно**.

11. Нажмите на кнопку **Добавить**.

    Новое исключение будет добавлено в список. Вы можете в любое время остановить работу исключения с помощью флажка в графе **Статус**.

12. Сохраните внесенные изменения.



Список исключений

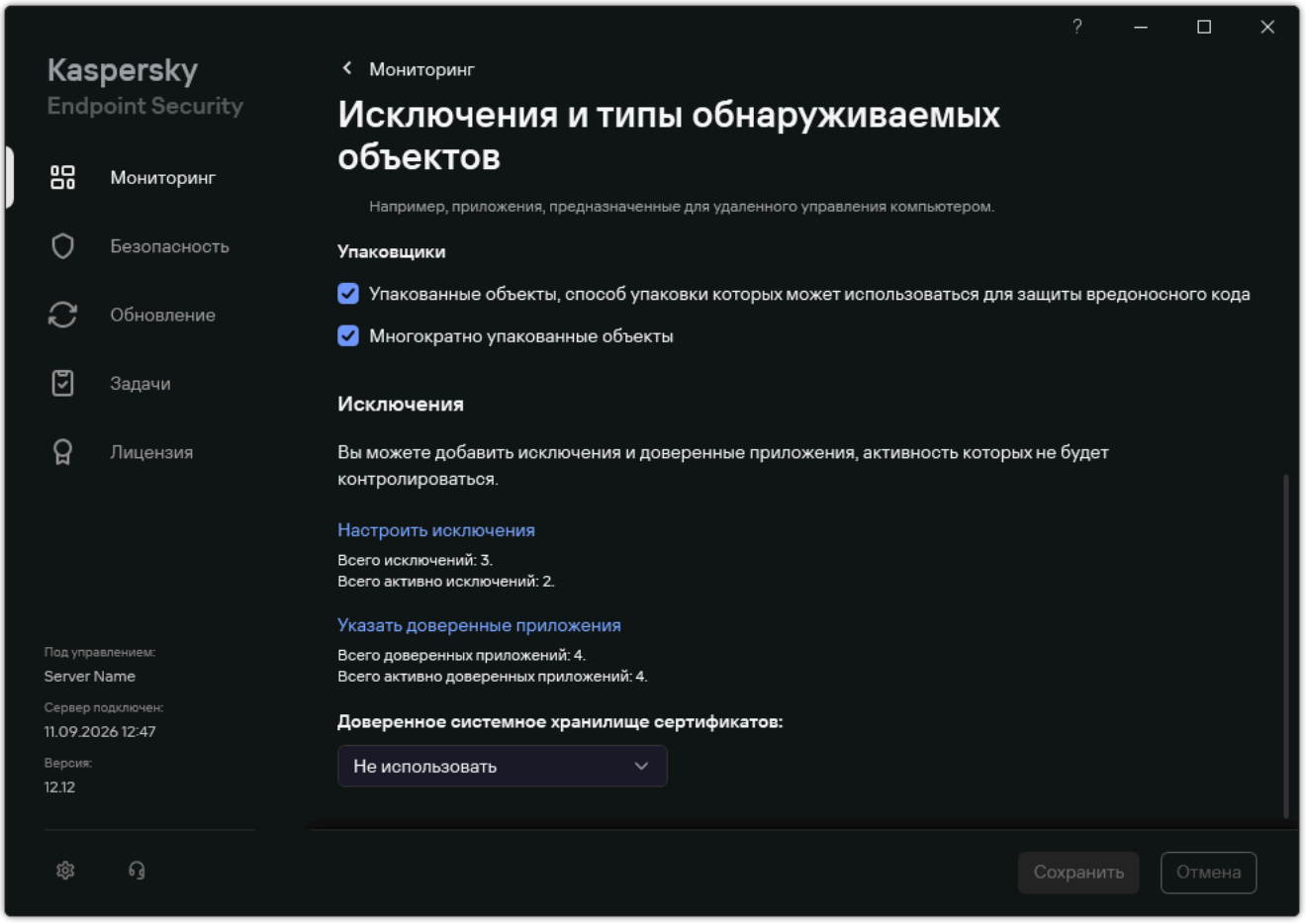
Как добавить приложение в список локальных доверенных приложений в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.

3. В блоке **Исключения** перейдите по ссылке **Указать доверенные приложения**.

Kaspersky Endpoint Security скрывает для просмотра список доверенных приложений в интерфейсе приложения, если администратор в консоли запретил настройку доверенных приложений ("замок" закрыт) и запретил использование локальных доверенных приложений (флажок **Разрешить использование локальных доверенных приложений** снят).



Параметры исключений

4. Нажмите на кнопку **Добавить** и выберите нужное действие:

- **Категорию**. Вы можете группировать доверенные приложения в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно доверенное приложение.
- **Новое исключение**. Kaspersky Endpoint Security добавляет новое доверенное приложение в корень списка.
- **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager в приложение добавлены *предустановленные доверенные приложения*. Также в приложение добавлены предустановленные доверенные приложения для настройки приложения в виртуальных средах Citrix и VMware. В зависимости от назначения защищаемого сервера вам нужно выбрать предустановленные доверенные приложения.

Для добавления нового доверенного приложения в отдельную категорию установите флажок рядом с этой категорией и выберите вариант **Новое исключение**.

5. Выберите критерий доверенности:

- **Использовать полный путь для определения доверенности процессов**. Введите путь к исполняемому файлу доверенного приложения.

  Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

  Kaspersky Endpoint Security учитывает регистр имени файла доверенного приложения. Если вы ввели имя файла в неверном регистре, Kaspersky Endpoint Security не распознает доверенное приложение.

- **Использовать хеш файла для определения доверенности процессов**.

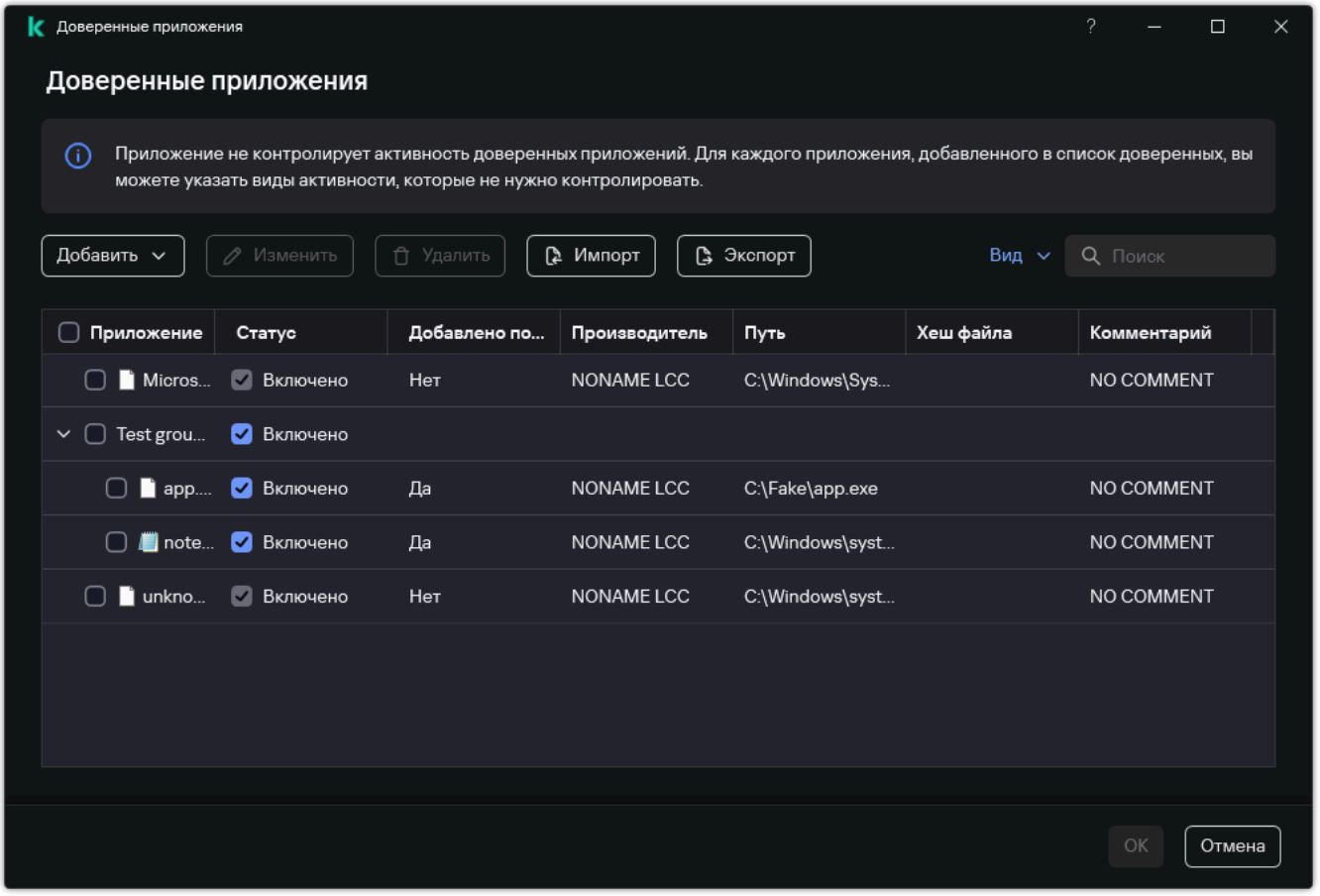
Kaspersky Endpoint Security поддерживает переменные среды. При этом Kaspersky Endpoint Security конвертирует путь в локальном интерфейсе приложения. То есть, если вы ввели путь к файлу `%userprofile%\Documents\File.exe`, в локальном интерфейсе приложения для пользователя Fred123 будет добавлена запись `C:\Users\Fred123\Documents\File.exe`. Соответственно, Kaspersky Endpoint Security игнорирует доверенное приложение `File.exe` для других пользователей. Чтобы применить запись ко всем учетным записям, вы можете использовать символ `*` (например, `C:\Users\*\Documents\File.exe`). При добавлении новой переменной среды нужно перезапустить приложение.

6. В окне свойств доверенного приложения настройте дополнительные параметры.

7. Нажмите на кнопку **OK**.

   Новое доверенное приложение будет добавлено в список. Вы можете в любое время исключить приложение из доверенной зоны с помощью флажка в графе **Статус**.

8. Сохраните внесенные изменения.



Список доверенных приложений

Экспорт и импорт доверенной зоны

Доверенная зона – это сформированный администратором системы список объектов и приложений, которые Kaspersky Endpoint Security не контролирует в процессе работы. Доверенная зона состоит из следующих списков: *исключения из проверки* и *доверенные приложения*. Вы можете экспортировать эти списки в файлы в формате XML и другие форматы. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных исключений. Также вы можете использовать функцию экспорта / импорта для резервного копирования списков исключений и доверенных приложений или для миграции списков на другой сервер.

Для работы функции экспорта / импорта *списка исключений* приложение использует следующие форматы:

- XML – доступен в Консоли администрирования (MMC), Web Console и Cloud Console.
- DAT – доступен только для импорта в Консоли администрирования (MMC). Этот формат предназначен для поддержки совместимости с предыдущими версиями приложения. Вы можете конвертировать DAT-файл в XML в Консоли администрирования (MMC), чтобы перенести списки исключений в Web Console.
- CSV – доступен только в локальном интерфейсе приложения.

Kaspersky Endpoint Security использует формат XML для работы функции экспорта / импорта *списка доверенных приложений*.

Как экспортировать / импортировать доверенную зону в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Исключения и типы объектов**.
4. В блоке **Исключения из проверки и доверенные приложения** выберите компонент доверенной зоны, которую вы хотите экспортировать или импортировать: **Исключения из проверки** или **Доверенные приложения**.
5. Нажмите на кнопку **Настройка**.
6. Для экспорта списка исключений выполните следующие действия:
   a. Выберите исключения, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

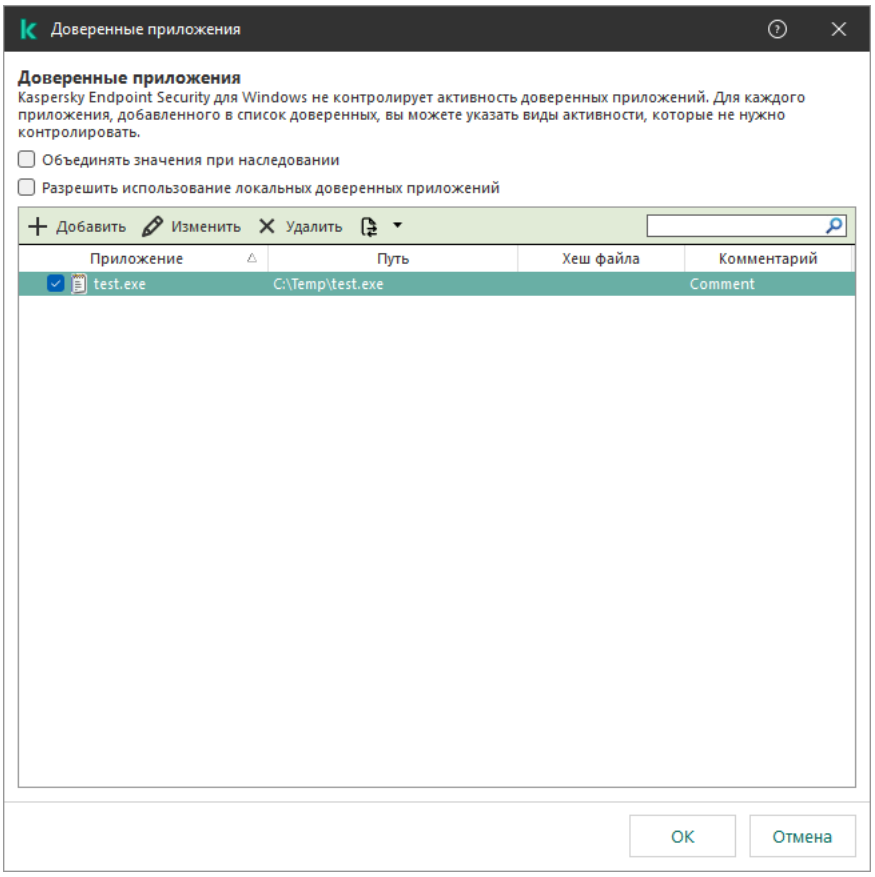
      Если вы не выбрали ни одного исключения, Kaspersky Endpoint Security экспортирует все исключения.

   b. Нажмите на кнопку → **Экспортировать**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список исключений, а также выберите папку, в которой вы хотите сохранить этот файл.

d. Сохраните файл.

Kaspersky Endpoint Security экспортирует список исключений в XML-файл. Kaspersky Endpoint Security также поддерживает экспорт списка исключений в файл формата DAT.



Список доверенных приложений

7. Для импорта списка исключений выполните следующие действия:

a. Нажмите на кнопку → **Импортировать**.

b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

c. Откройте файл.

Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла. Kaspersky Endpoint Security также поддерживает импорт списка исключений из файла формата DAT.

8. Сохраните внесенные изменения.

Как экспортировать /импортировать доверенную зону в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Доверенная зона**.

5. Для экспорта списка исключений выполните следующие действия:

   a. Перейдите по ссылке **Исключения из Поиска вредоносного ПО**.

   b. Выберите исключения, которые вы хотите экспортировать.

   c. Нажмите на кнопку → **Экспортировать**.

      Kaspersky Endpoint Security экспортирует список исключений в JSON-файл в папку для загрузки по умолчанию.

6. Для экспорта списка доверенных приложений выполните следующие действия:

   a. Выберите доверенные приложения, которые вы хотите экспортировать.

   b. Нажмите на кнопку → **Экспортировать**.

      Kaspersky Endpoint Security экспортирует список доверенных приложений в JSON-файл в папку для загрузки по умолчанию.

7. Для импорта списка исключений выполните следующие действия:

   a. Перейдите по ссылке **Исключения из Поиска вредоносного ПО**.

   b. Нажмите на кнопку → **Импортировать**.

      В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список исключений.

   c. Откройте файл.

      Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.

8. Для импорта списка доверенных приложений выполните следующие действия:

   a. Перейдите по ссылке **Приложения**.

   b. Нажмите на кнопку → **Импортировать**.

      В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список доверенных приложений.

   c. Откройте файл.

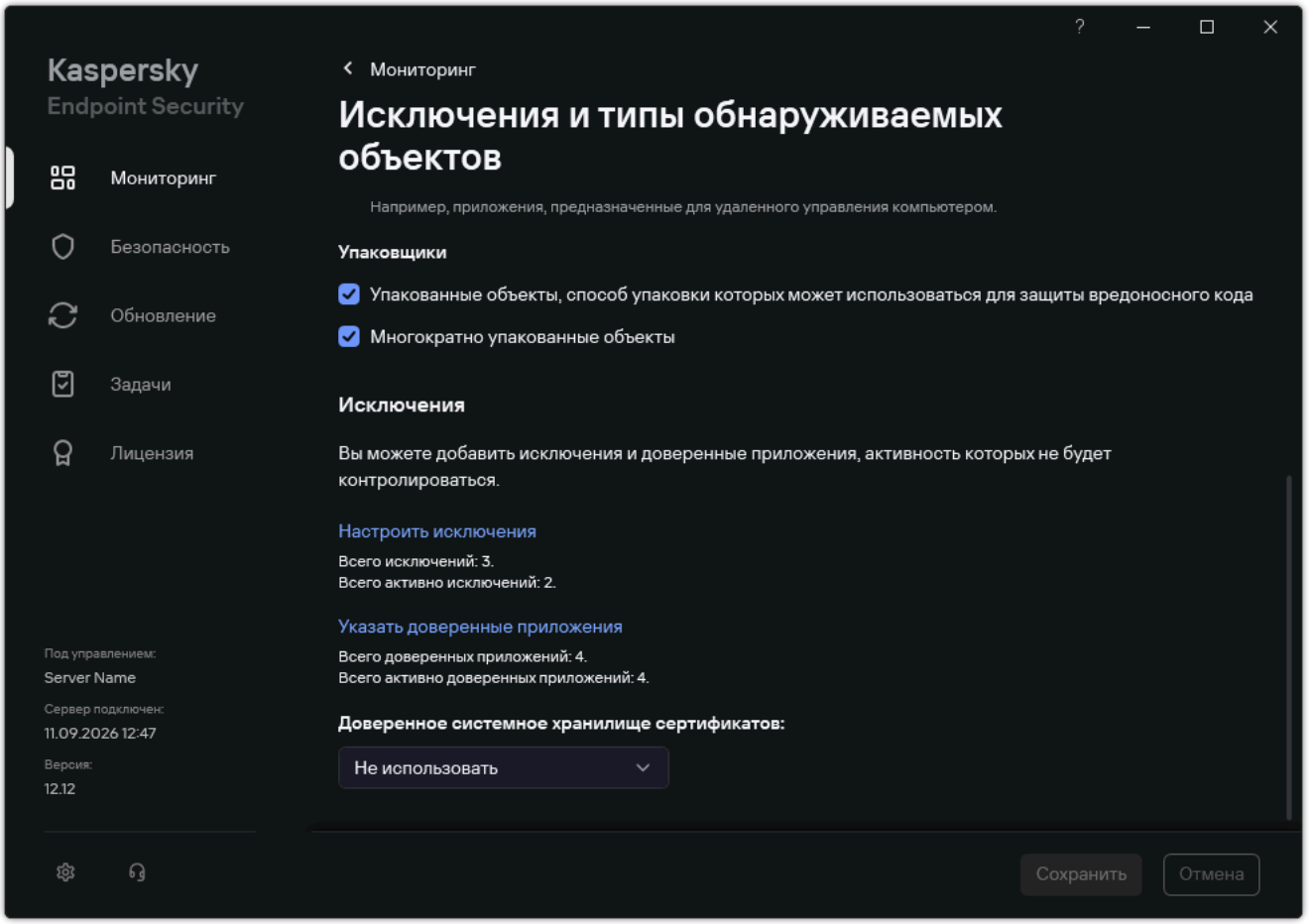
      Если на компьютере уже есть список доверенных приложений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.

9. Сохраните внесенные изменения.

Как экспортировать / импортировать доверенную зону в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.



Параметры исключений

3. Для экспорта списка исключений выполните следующие действия:

   a. В блоке **Исключения** перейдите по ссылке **Настроить исключения**.

   b. Выберите исключения, которые вы хотите экспортировать.

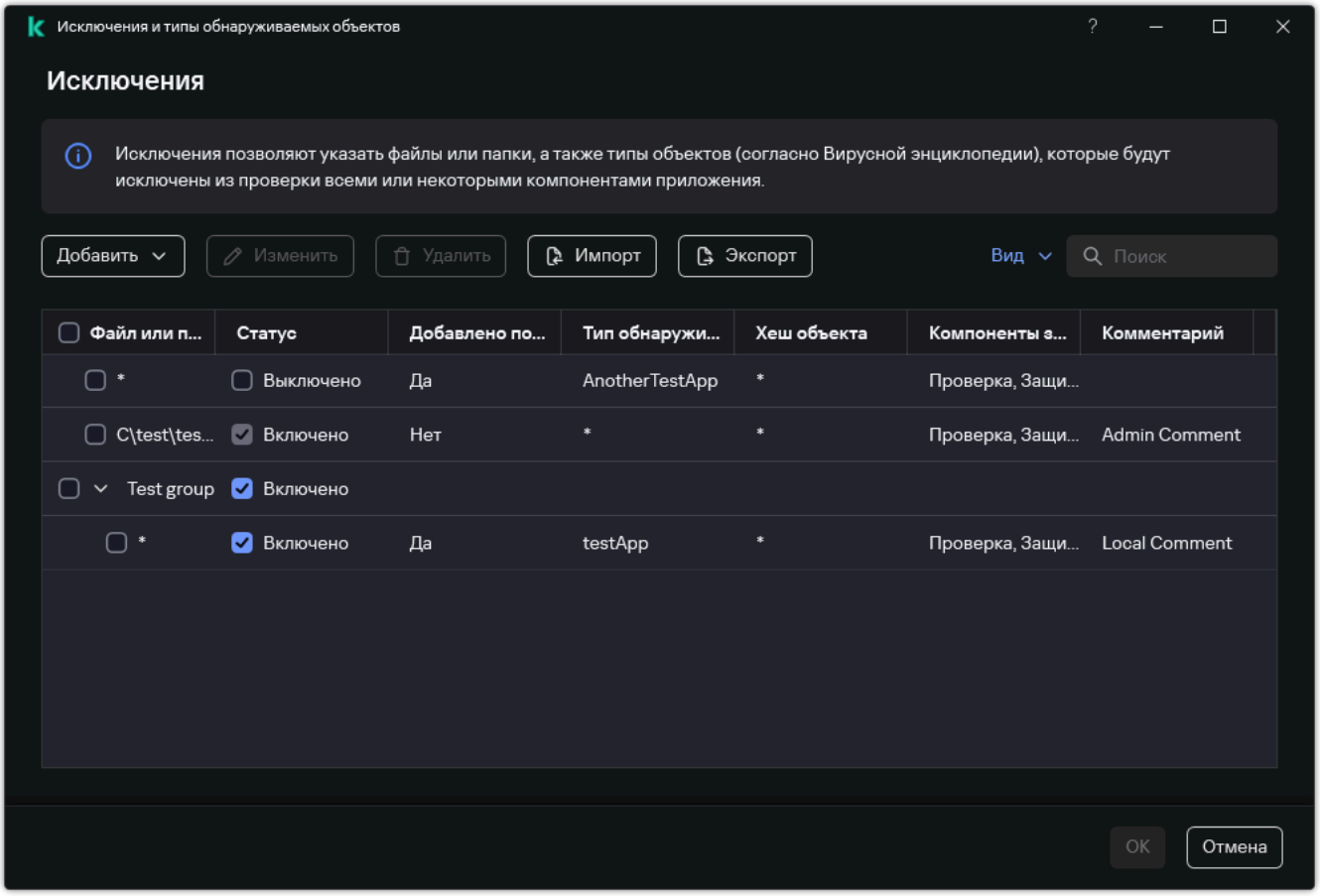
   c. Нажмите на кнопку **Экспорт**.

   d. Подтвердите, что вы хотите экспортировать только выбранные исключения, или экспортируйте весь список.

   e. В открывшемся окне введите имя файла формата CSV, в который вы хотите экспортировать список исключений, а также выберите папку, в которой вы хотите сохранить этот файл.

f. Сохраните файл.

Kaspersky Endpoint Security экспортирует список исключений в CSV-файл.



Список исключений

4. Для экспорта списка доверенных приложений выполните следующие действия:

   a. В блоке **Исключения** перейдите по ссылке **Указать доверенные приложения**.

   b. Выберите доверенные приложения, которые вы хотите экспортировать.

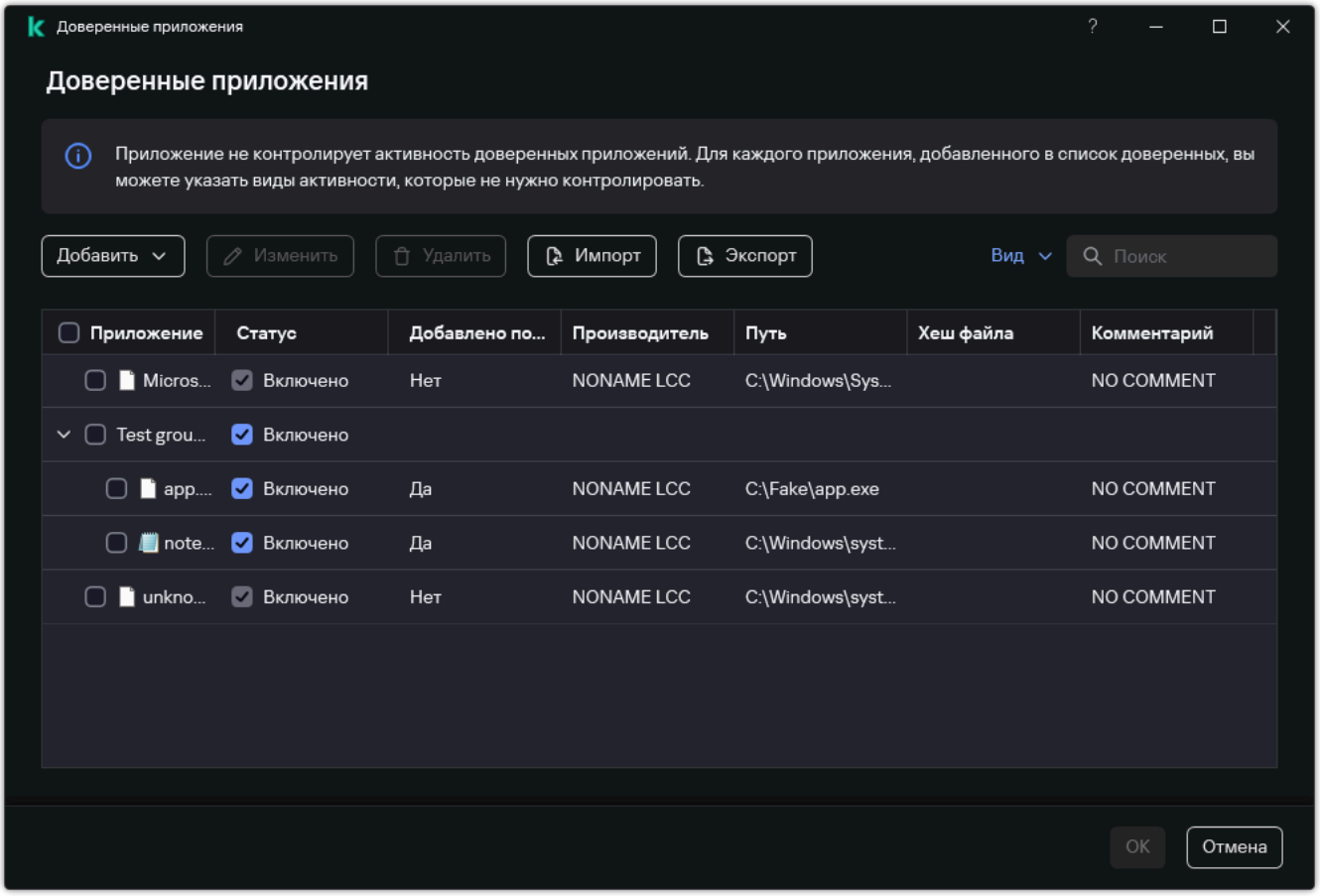
   c. Нажмите на кнопку **Экспорт**.

   d. Подтвердите, что вы хотите экспортировать только выбранные доверенные приложения, или экспортируйте весь список.

   e. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список доверенных приложений, а также выберите папку, в которой вы хотите сохранить этот файл.

f. Сохраните файл.

Kaspersky Endpoint Security экспортирует список доверенных исключений в XML-файл.



Список доверенных приложений

5. Для импорта списка исключений выполните следующие действия:

a. В блоке **Исключения** перейдите по ссылке **Настроить исключения**.

b. Нажмите на кнопку **Импорт**.

c. В открывшемся окне выберите CSV-файл, из которого вы хотите импортировать список исключений.

d. Откройте файл.

Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из CSV-файла.

6. Для импорта списка доверенных приложений выполните следующие действия:

a. В блоке **Исключения** перейдите по ссылке **Указать доверенные приложения**.

b. Нажмите на кнопку **Импорт**.

c. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных приложений.

d. Откройте файл.

Если на компьютере уже есть список доверенных приложений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

7. Сохраните внесенные изменения.

Работа с приложениями, подписанными доверенной цифровой подписью

Использование системного хранилища сертификатов позволяет исключать из антивирусной проверки приложения, подписанные доверенной цифровой подписью. Kaspersky Endpoint Security автоматически помещает такие приложения в группу *Доверенные*.

Как начать использование доверенного системного хранилища сертификата в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Исключения и типы объектов**.
4. В блоке **Доверенное системное хранилище сертификатов** установите флажок **Использовать доверенное системное хранилище сертификатов**.
5. В раскрывающемся списке выберите, какое системное хранилище Kaspersky Endpoint Security должен считать доверенным.
6. Сохраните внесенные изменения.

Как начать использование доверенного системного хранилища сертификата в Web Console и Cloud Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона**.
5. В открывшемся окне перейдите по ссылке **Корневые сертификаты**.
6. В открывшемся окне установите флажок **Использовать доверенное системное хранилище сертификатов**.
7. Выберите, какое системное хранилище Kaspersky Endpoint Security должен считать доверенным.
8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как начать использование доверенного системного хранилища сертификата в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.
3. В раскрывающемся списке **Доверенное системное хранилище сертификатов** выберите, какое системное хранилище Kaspersky Endpoint Security должен считать доверенным.
4. Сохраните внесенные изменения.

Приложение. Предустановленные исключения из проверки и доверенные приложения

Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах. Начиная с версии Kaspersky Endpoint Security для Windows 12.8 добавлена установка приложения в режиме Легкого агента для защиты виртуальных сред. Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в виртуальных средах Citrix и VMware.

Вы можете выбрать предустановленные исключения и доверенные приложения следующими способами:

- Установка приложения.
  - Локальная установка приложения с помощью мастера.
  - Свойства инсталляционного пакета.
- Настройка политики.
  - Мастер создания политики.
  - Свойства политики: исключения из проверки и доверенные приложения.

Microsoft SQL Server

При установке приложения Kaspersky Endpoint Security на SQL-сервер вам нужно сформировать доверенную зону из предустановленных исключений и доверенных приложений для стабильной работы сервера.

Предустановленные исключения из проверки

Путь	Версия SQL
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Microsoft Exchange Server

При установке приложения Kaspersky Endpoint Security на Microsoft Exchange-сервер вам нужно сформировать доверенную зону из предустановленных исключений и доверенных приложений для стабильной работы сервера.

Предустановленные исключения из проверки

Путь	Версия Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019

Путь	Версия Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

Предустановленные доверенные приложения

Путь	Версия Microsoft Exchange
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

Microsoft System Center Configuration Manager

Если в операционной системе защищаемого компьютера установлено решение Microsoft System Center Configuration Manager, вам нужно добавить в список исключений из проверки предустановленное исключение для обеспечения стабильной работы решения.

Предустановленные исключения из проверки

Путь	Версия System Center Configuration Manager
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

При установке приложения Kaspersky Endpoint Security в виртуальную среду Citrix вам нужно сформировать доверенную зону из предустановленных исключений и доверенных приложений для стабильной работы виртуальной среды.

Предустановленные исключения из проверки

Путь
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache

Путь
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

Предустановленные доверенные приложения

Путь	Решение Citrix
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Virtual Apps and Desktops
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Virtual Apps and Desktops
%SystemRoot%\System32\drivers\CVhdFilter.sys	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Virtual Apps and Desktops

Путь	Решение Citrix
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Workspace app
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Provisioning
%SystemRoot%\System32\drivers\bnistack6.sys	Provisioning
%SystemRoot%\System32\drivers\CfsDep2.sys	Provisioning
%SystemRoot%\System32\drivers\cnicteam.sys	Provisioning

Путь	Решение Citrix
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Provisioning
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

При установке приложения Kaspersky Endpoint Security в виртуальную среду VMware вам нужно сформировать доверенную зону из предустановленных доверенных приложений для стабильной работы виртуальной среды.

Предустановленные доверенные приложения

Путь	Решение VMware
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon

Путь	Решение VMware
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

Дедупликация данных в Microsoft Windows Server

Если в операционной системе Microsoft Windows Server с установленным приложением Kaspersky Endpoint Security включена дедупликация данных, вам нужно добавить в список доверенных приложений предустановленное доверенное приложение для оптимизации работы Kaspersky Endpoint Security и снижения нагрузки на центральный процессор.

Предустановленные доверенные приложения

Путь	Версия Microsoft Windows Server
%SystemRoot%\system32\fsdmhost.exe	Все поддерживаемые версии

Работа с резервным хранилищем

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES.14.3\QB`.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security.

> В Kaspersky Endpoint Security отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете попытаться восстановить файл из его резервной копии в папку исходного размещения файла.

Если Kaspersky Endpoint Security работает под управлением Kaspersky Security Center, то резервные копии файлов могут быть передана на Сервер администрирования Kaspersky Security Center. Подробнее о работе с резервными копиями файлов в Kaspersky Security Center можно прочитать в Справочной системе Kaspersky Security Center.

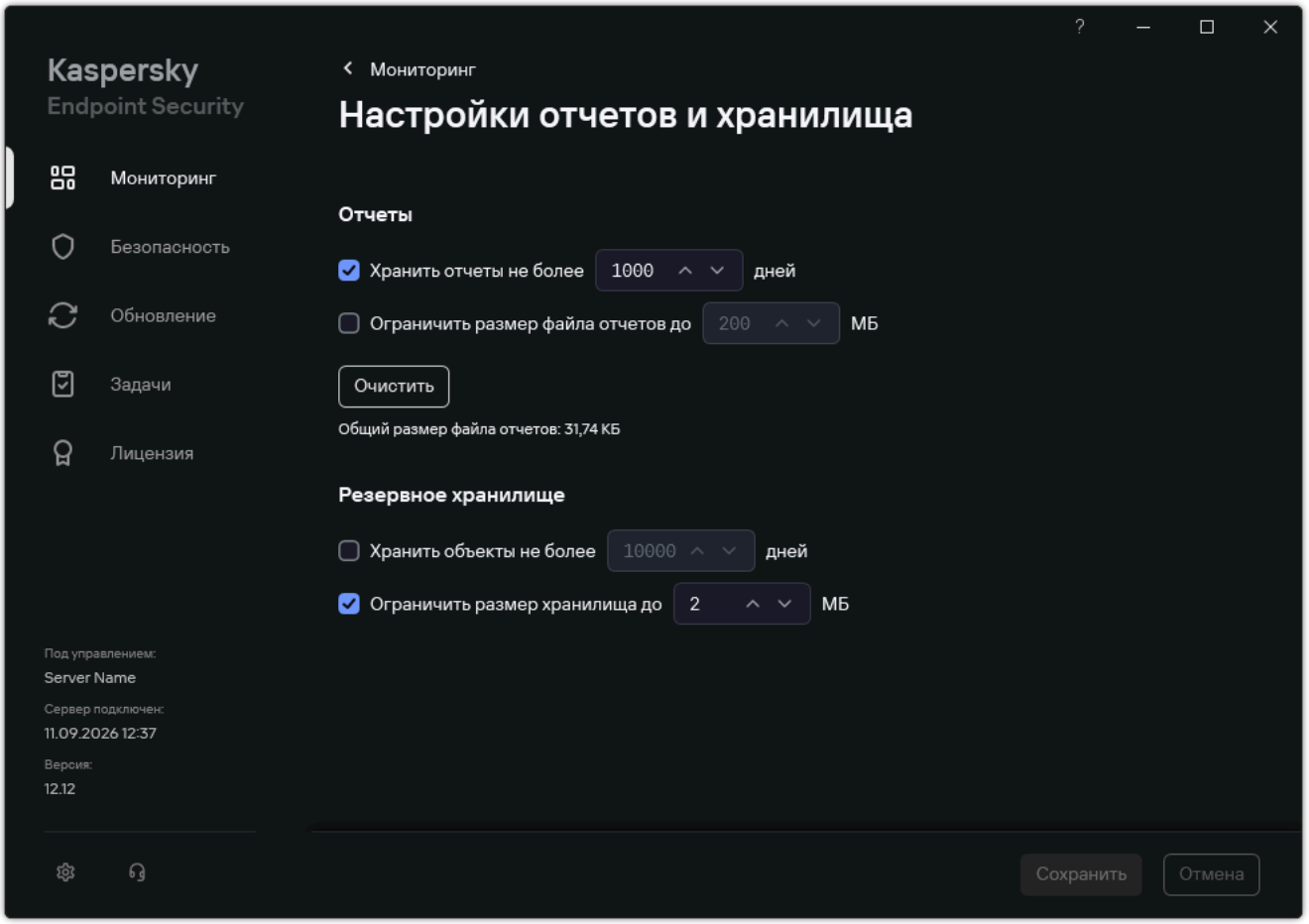
Настройка максимального срока хранения файлов в резервном хранилище

По умолчанию максимальный срок хранения копий файлов в резервном хранилище составляет 30 дней. По истечении максимального срока хранения Kaspersky Endpoint Security удаляет наиболее старые файлы из резервного хранилища.

Чтобы настроить максимальный срок хранения файлов в резервном хранилище, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** нажмите на плитку **Отчеты и хранилище**.



Параметры резервного хранилища

3. В блоке **Резервное хранилище** установите флажок **Хранить объекты не более N дней**, если хотите ограничить срок хранения копий файлов в резервном хранилище. Укажите максимальный срок хранения копий файлов в резервном хранилище.

4. Сохраните внесенные изменения.

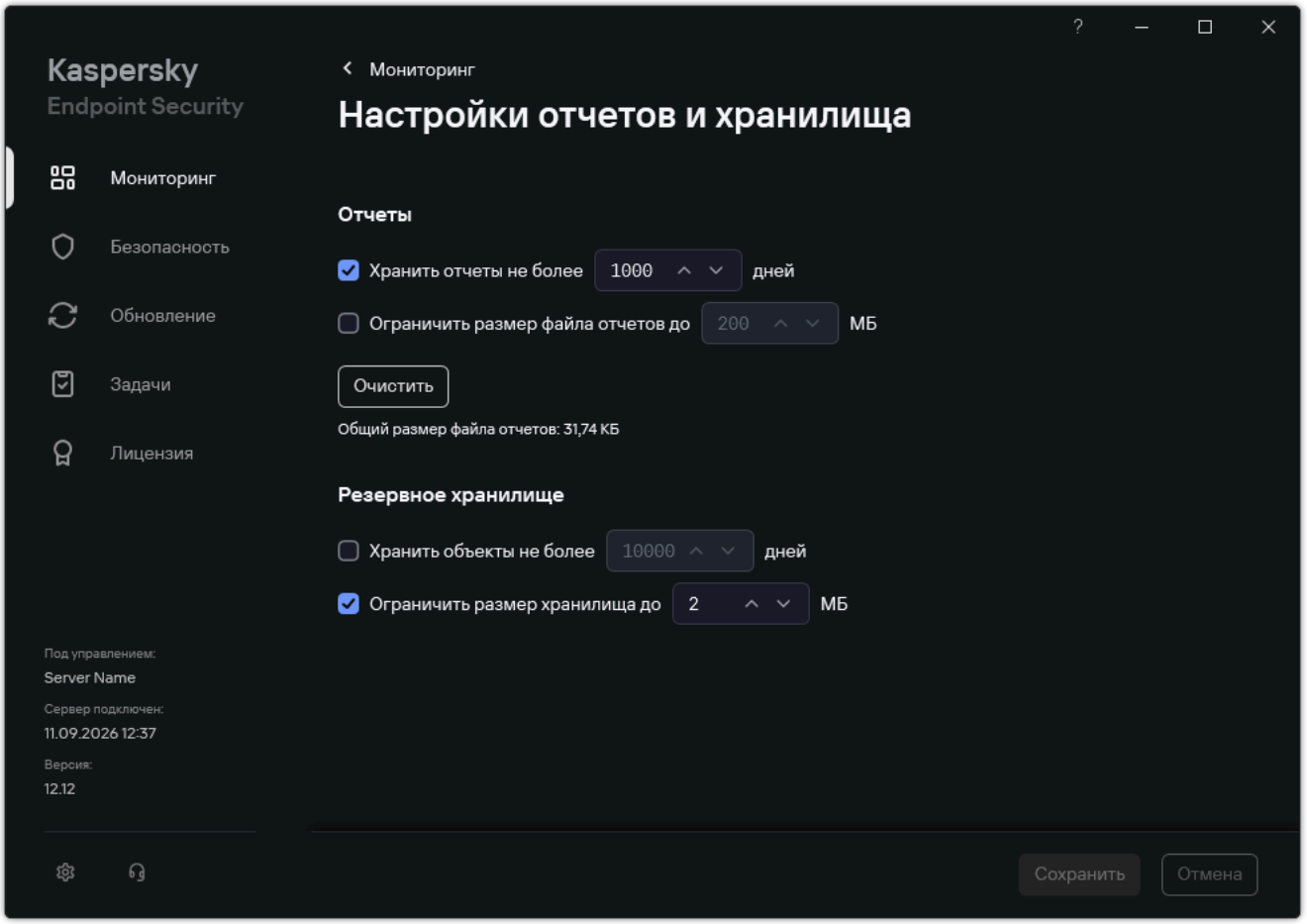
Настройка максимального размера резервного хранилища

Вы можете указать максимальный размер резервного хранилища. По умолчанию размер резервного хранилища не ограничен. После достижения максимального размера Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы из резервного хранилища.

Чтобы настроить максимальный размер резервного хранилища, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** нажмите на плитку **Отчеты и хранилище**.



Параметры резервного хранилища

3. В блоке **Резервное хранилище** установите флажок **Ограничить размер хранилища до N МБ**. Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. По умолчанию максимальный размер составляет 1024 МБ. После достижения максимального размера резервного хранилища приложение Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения.

4. Сохраните внесенные изменения.

Восстановление файлов из резервного хранилища

Если в файле обнаружен вредоносный код, Kaspersky Endpoint Security блокирует файл, присваивает ему статус *Не вылечен*, помещает его копию в резервное хранилище и пытается провести лечение. Если файл удается вылечить, то статус резервной копии файла изменяется на *Вылечен*. Файл становится доступен в папке исходного размещения. Если файл не удается вылечить, то Kaspersky Endpoint Security удаляет его из папки исходного размещения. Вы можете восстановить файл из его резервной копии в папку исходного размещения.

Файлы со статусом *Будет удален при перезагрузке компьютера* восстановить невозможно. Перезагрузите компьютер и статус файла изменится на *Вылечен* или *Удален*. При этом вы можете восстановить файл из его резервной копии в папку исходного размещения.

В случае обнаружения вредоносного кода в файле, который является частью приложения Windows Store, Kaspersky Endpoint Security не помещает копию файла в резервное хранилище, а сразу удаляет его. При этом восстановить целостность приложения Windows Store вы можете средствами операционной системы (подробную информацию о восстановлении приложения Windows Store читайте в Справочной системе к Microsoft Windows).

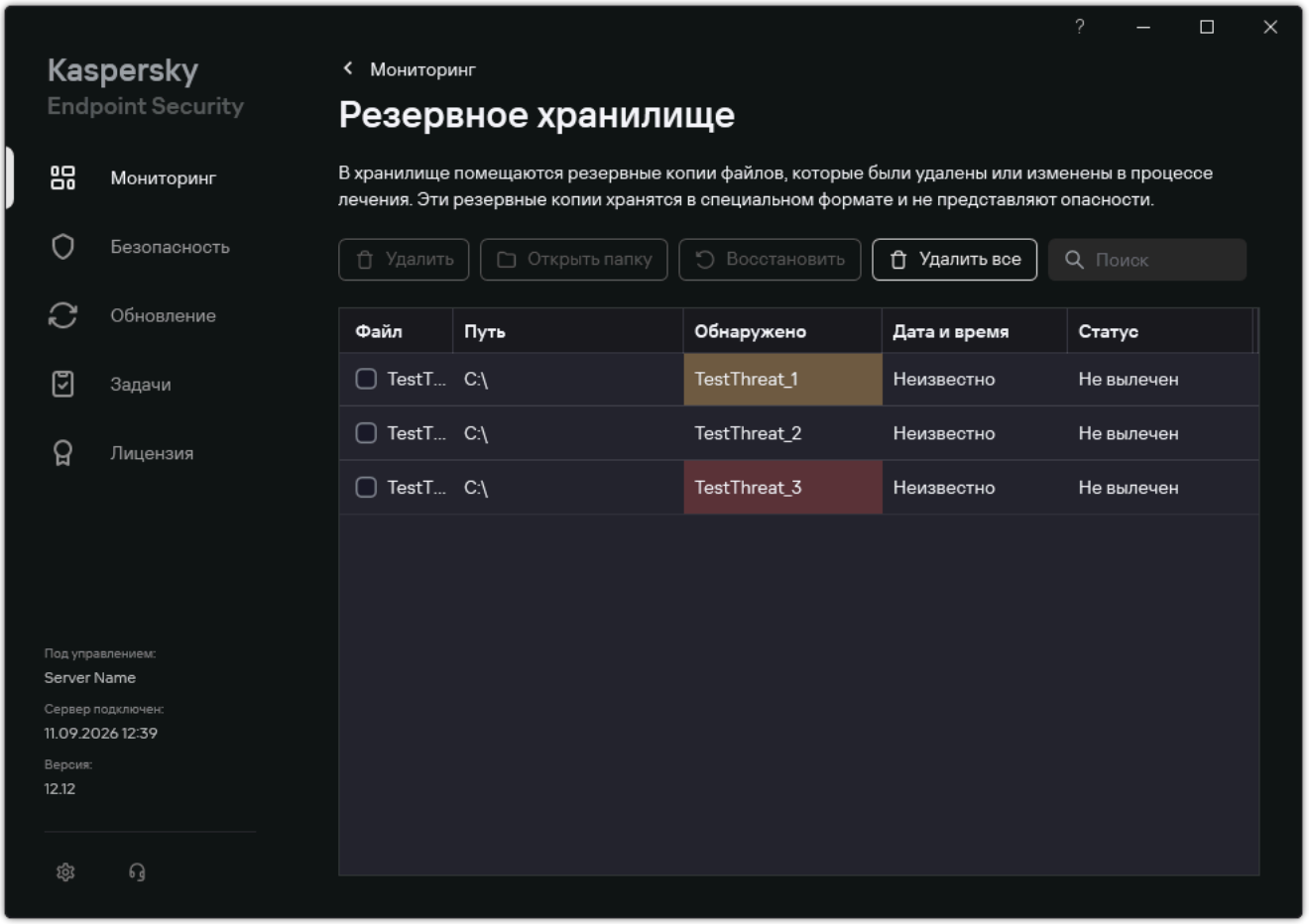
Набор резервных копий файлов представлен в виде таблицы. Для резервной копии файла отображается путь к папке исходного размещения этого файла. Путь к папке исходного размещения файла может содержать персональные данные.

Если в резервное хранилище помещено несколько расположенных в одной и той же папке файлов с одинаковыми именами и различным содержимым, то для восстановления доступен только тот файл, который был помещен в резервное хранилище последним.

Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Резервное хранилище**.
2. В открывшемся списке файлов резервного хранилища выберите файлы, которые вы хотите восстановить, и нажмите на кнопку **Восстановить**.

Kaspersky Endpoint Security восстановит файлы из выбранных резервных копий в папки их исходного размещения.



Резервное хранилище

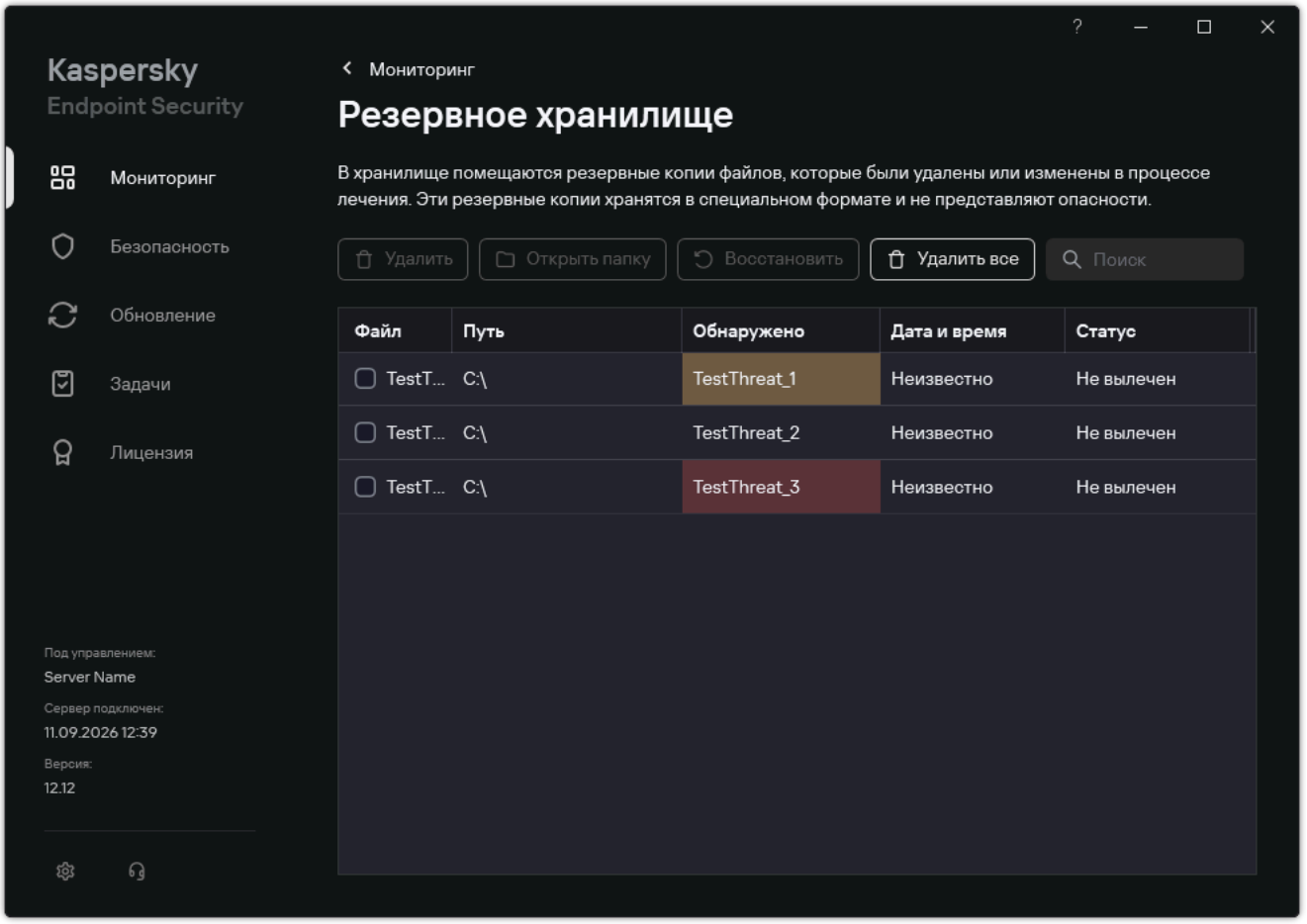
Удаление резервных копий файлов из резервного хранилища

Kaspersky Endpoint Security удаляет резервные копии файлов с любым статусом из резервного хранилища автоматически по истечении времени, заданного в параметрах приложения. Также вы можете самостоятельно удалить любую копию файла из резервного хранилища.

Чтобы удалить резервные копии файлов из резервного хранилища, выполните следующие действия:

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Резервное хранилище**.
2. В открывшемся списке файлов резервного хранилища выберите файлы, которые вы хотите удалить из резервного хранилища, и нажмите на кнопку **Удалить**.

Kaspersky Endpoint Security удалит выбранные резервные копии файлов из резервного хранилища.



Резервное хранилище

Служба уведомлений

В процессе работы Kaspersky Endpoint Security возникают различного рода события. Уведомления об этих событиях могут иметь информационный характер или нести важную информацию. Например, уведомление может информировать об успешно выполненном обновлении баз и модулей программы, а может фиксировать ошибку в работе некоторого компонента, которую вам требуется устранить.

Kaspersky Endpoint Security позволяет вносить информацию о событиях, возникающих в работе программы, в журнал событий Microsoft Windows и / или в журнал Kaspersky Endpoint Security.

Kaspersky Endpoint Security может доставлять уведомления следующими способами:

- с помощью всплывающих уведомлений в области уведомлений панели задач Microsoft Windows;
- по электронной почте.

Вы можете настроить способы доставки уведомлений. Способ доставки уведомлений устанавливается для каждого типа событий.

Работая с таблицей событий для настройки службы уведомлений, вы можете выполнять следующие действия:

- фильтровать события службы уведомлений по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска событий службы уведомлений;
- сортировать события службы уведомлений;
- изменять порядок и набор граф, отображаемых в списке событий службы уведомлений.

Настройка параметров журналов событий

Чтобы настроить параметры журналов событий, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки интерфейса**.
3. В блоке **Уведомления** нажмите на кнопку **Настроить уведомления**.

   В левой части окна представлены компоненты и задачи Kaspersky Endpoint Security. В правой части окна отображается список событий, сформированный для выбранного компонента или выбранной задачи.

   События могут содержать следующие данные пользователя:

   - пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
   - пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
   - имя пользователя Microsoft Windows;
   - адреса веб-страниц, открываемых пользователем.

4. В левой части окна выберите компонент или задачу, для которой вы хотите настроить параметры журналов событий.

5. В графах **Сохранять в локальном отчете** и **Сохранять в журнале событий Windows** установите флажки напротив нужных событий.

   События, напротив которых установлен флажок в графе **Сохранять в локальном отчете**, отображаются в отчетах приложения. События, напротив которых установлен флажок в графе **Сохранять в журнале событий Windows**, отображаются в журналах Windows в канале `Application`.

6. Сохраните внесенные изменения.

Настройка отображения и доставки уведомлений

Чтобы настроить отображение и доставку уведомлений, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки интерфейса**.

3. В блоке **Уведомления** нажмите на кнопку **Настроить уведомления**.

   В левой части окна представлены компоненты и задачи Kaspersky Endpoint Security. В правой части окна отображается список событий, сформированный для выбранного компонента или выбранной задачи.

   События могут содержать следующие данные пользователя:

   - пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
   - пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
   - имя пользователя Microsoft Windows;
   - адреса веб-страниц, открываемых пользователем.

4. В левой части окна выберите компонент или задачу, для которой вы хотите настроить доставку уведомлений.

5. В графе **Уведомлять на экране** установите флажки напротив нужных событий.

   Информация о выбранных событиях отображается на экране в виде всплывающих уведомлений в области уведомлений панели задач Microsoft Windows.

6. В графе **Уведомлять по почте** установите флажки напротив нужных событий.

   Информация о выбранных событиях доставляется по электронной почте, если заданы параметры доставки почтовых уведомлений.

7. Нажмите на кнопку **ОК**.

8. Если вы включили уведомления по почте, настройте параметры доставки электронных сообщений:

   a. Нажмите на кнопку **Настроить почтовые уведомления**.

   b. Установите флажок **Уведомлять о событиях**, чтобы включить доставку информации о событиях в работе Kaspersky Endpoint Security, отмеченных в графе **Уведомлять по почте**.

c. Укажите параметры доставки почтовых уведомлений.

d. Нажмите на кнопку **OK**.

9. Сохраните внесенные изменения.

Настройка отображения предупреждений о состоянии приложения в области уведомлений

Чтобы настроить отображение предупреждений о состоянии приложения в области уведомлений, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки интерфейса**.
3. В блоке **Отображать состояние приложения в области уведомлений** установите флажки напротив тех категорий событий, уведомления о которых вы хотите видеть в области уведомлений Microsoft Windows.
4. Сохраните внесенные изменения.

При возникновении событий, относящихся к выбранным категориям, значок приложения в области уведомлений будет меняться на  или  в зависимости от важности предупреждения.

Обмен сообщениями между пользователем и администратором

Компоненты Контроль приложений, Контроль устройств, Веб-Контроль и Адаптивный контроль аномалий предоставляют пользователям локальной сети организации, на компьютерах которых установлено приложение Kaspersky Endpoint Security, возможность отправлять сообщения администратору.

У пользователя может возникнуть необходимость отправить сообщение администратору локальной сети организации в следующих случаях:

- Контроль устройств заблокировал доступ к устройству.

  Шаблон сообщения с запросом доступа к заблокированному устройству доступен в интерфейсе Kaspersky Endpoint Security в разделе Контроль устройств.

- Контроль приложений запретил запуск приложения.

  Шаблон сообщения с запросом разрешения на запуск заблокированного приложения доступен в интерфейсе Kaspersky Endpoint Security в разделе Контроль приложений.

- Веб-Контроль заблокировал доступ к веб-ресурсу.

  Шаблон сообщения с запросом доступа к заблокированному веб-ресурсу доступен в интерфейсе Kaspersky Endpoint Security в разделе Веб-Контроль.

Способ отправки сообщений, а также выбор используемого шаблона зависит от наличия или отсутствия на компьютере с установленного приложения Kaspersky Endpoint Security действующей политики Kaspersky Security Center и связи с Сервером администрирования Kaspersky Security Center. Возможны следующие сценарии:

- Если на компьютере с установленным приложением Kaspersky Endpoint Security не действует политика Kaspersky Security Center, то сообщение пользователя отправляется администратору локальной сети организации по электронной почте.

  Для заполнения полей сообщения используются значения полей из шаблона, заданного в локальном интерфейсе Kaspersky Endpoint Security.

- Если на компьютере с установленным приложением Kaspersky Endpoint Security действует политика Kaspersky Security Center, то Kaspersky Endpoint Security отправляет стандартное сообщение на Сервер администрирования Kaspersky Security Center.

  В этом случае сообщения пользователей доступны для просмотра в хранилище событий Kaspersky Security Center (см. инструкцию ниже). Для заполнения полей сообщения используются значения полей из шаблона, заданного в политике Kaspersky Security Center.

- Если на компьютере с установленным приложением Kaspersky Endpoint Security действует политика для автономных пользователей Kaspersky Security Center, то способ отправки сообщения зависит от наличия связи с Kaspersky Security Center:

  - Если связь с Kaspersky Security Center установлена, то Kaspersky Endpoint Security отправляет стандартное сообщение на Сервер администрирования Kaspersky Security Center.

  - Если связь с Kaspersky Security Center отсутствует, то сообщение пользователя отправляется администратору локальной сети организации по электронной почте.

  Для заполнения полей сообщения в обоих случаях используются значения полей из шаблона, заданного в политике Kaspersky Security Center.

Чтобы просмотреть сообщение пользователя в хранилище событий Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В узле **Сервер администрирования** дерева Консоли администрирования выберите вкладку **События**.

   В рабочей области Kaspersky Security Center отображаются все события, произошедшие во время работы приложения Kaspersky Endpoint Security, в том числе и сообщения администратору, приходящие от пользователей локальной сети организации.

3. Чтобы настроить фильтр событий, в раскрывающемся списке **Выборки событий** выберите элемент **Запросы пользователей**.

4. Выберите сообщение администратору.

5. Нажмите на кнопку **Открыть окно свойств события** в правой части рабочей области Консоли администрирования.

Работа с отчетами

Информация о работе каждого компонента Kaspersky Endpoint Security, о событиях шифрования данных, о выполнении каждой задачи проверки, задачи обновления и задачи проверки целостности, а также о работе приложения в целом сохраняется в отчетах.

Отчеты хранятся в папке `C:\ProgramData\Kaspersky Lab\KES.14.3\Report`.

Отчеты могут содержать следующие данные пользователя:

- пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
- пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
- имя пользователя Microsoft Windows;
- адреса веб-страниц, открываемых пользователем.

Данные в отчете представлены в виде таблицы. Каждая строка таблицы содержит информацию об отдельном событии, атрибуты события находятся в графах таблицы. Некоторые графы являются составными и содержат вложенные графы с дополнительными атрибутами. Чтобы просмотреть дополнительные атрибуты, нажмите на кнопку ⊞ рядом с названием графы. События, зарегистрированные в работе разных компонентов или при выполнении разных задач, имеют разный набор атрибутов.

Доступны следующие отчеты:

- Отчет **Аудит системы**. Содержит информацию о событиях, возникающих в процессе взаимодействия пользователя с приложением, а также в ходе работы приложения в целом и не относящихся к каким-либо отдельным компонентам или задачам Kaspersky Endpoint Security.
- Отчеты о работе компонентов Kaspersky Endpoint Security.
- Отчеты о выполнении задач Kaspersky Endpoint Security.
- Отчет **Шифрование данных**. Содержит информацию о событиях, возникающих при шифровании и расшифровке данных.

В отчетах применяются следующие уровни важности событий:

ⓘ **Информационные сообщения**. События справочного характера, как правило, не несущие важной информации.

⚠ **Предупреждения**. События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе приложения Kaspersky Endpoint Security.

ⓘ **Критические события**. События критической важности, указывающие на проблемы в работе приложения Kaspersky Endpoint Security или на уязвимости в защите компьютера пользователя.

Для удобства работы с отчетами вы можете изменять представление данных на экране следующими способами:

- фильтровать список событий по различным критериям;
- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке;
- сортировать список событий по каждой графе отчета;
- отображать и скрывать сгруппированные с помощью фильтра события по кнопке ;
- изменять порядок и набор граф, отображаемых в отчете.

При необходимости вы можете сохранить сформированный отчет в текстовый файл. Также вы можете удалять информацию из отчетов по компонентам и задачам Kaspersky Endpoint Security, объединенным в группы.

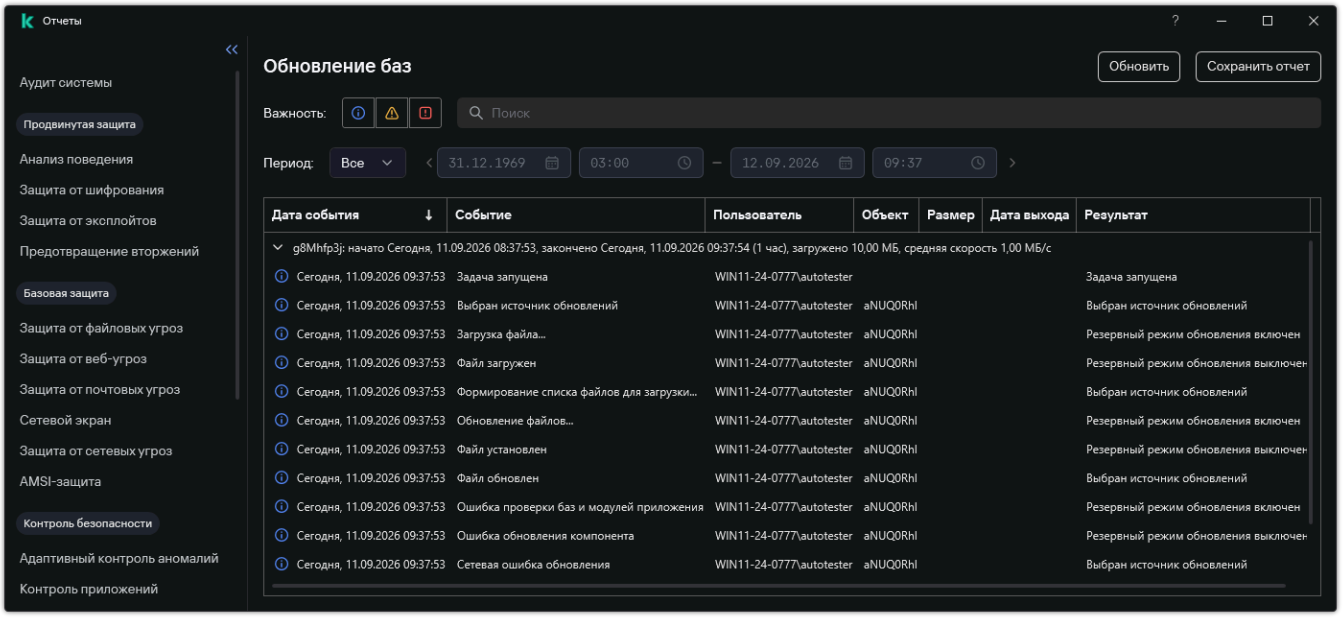
Если Kaspersky Endpoint Security работает под управлением Kaspersky Security Center, то информация о событиях может быть передана на Сервер администрирования Kaspersky Security Center (подробнее см. в справке Kaspersky Security Center).

Просмотр отчетов

Если для пользователя доступен просмотр отчетов, то для этого пользователя доступен просмотр всех событий, отраженных в отчетах.

Чтобы просмотреть отчеты, выполните следующие действия:

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Отчеты**.



Отчеты

2. В списке компонентов и задач выберите компонент или задачу.

   В правой части окна отобразится отчет, содержащий список событий по результатам работы выбранного компонента или выбранной задачи Kaspersky Endpoint Security. Вы можете отсортировать события в отчете по значениям в ячейках одной из граф.

3. Если требуется просмотреть подробную информацию о событии, выберите в отчете нужное событие.

В нижней части окна отобразится блок со сводной информацией о событии.

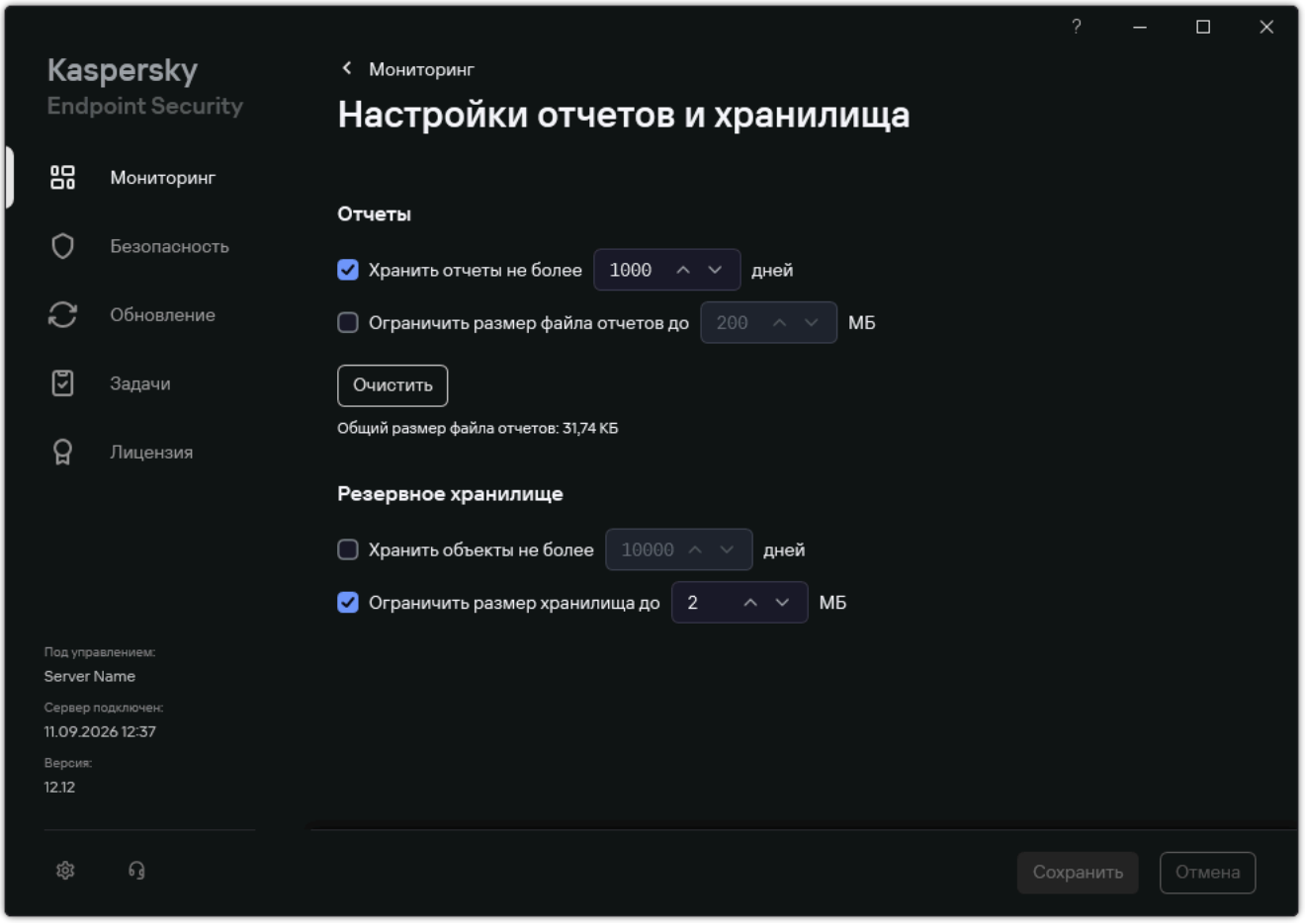
Настройка максимального срока хранения отчетов

По умолчанию максимальный срок хранения отчетов о событиях, фиксируемых Kaspersky Endpoint Security, составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчета.

Чтобы настроить максимальный срок хранения отчетов, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** нажмите на плитку **Отчеты и хранилище**.



Параметры отчетов

3. В блоке **Отчеты** установите флажок **Хранить отчеты не более N дней**, если хотите ограничить срок хранения отчетов. Укажите максимальный срок хранения отчетов.

4. Сохраните внесенные изменения.

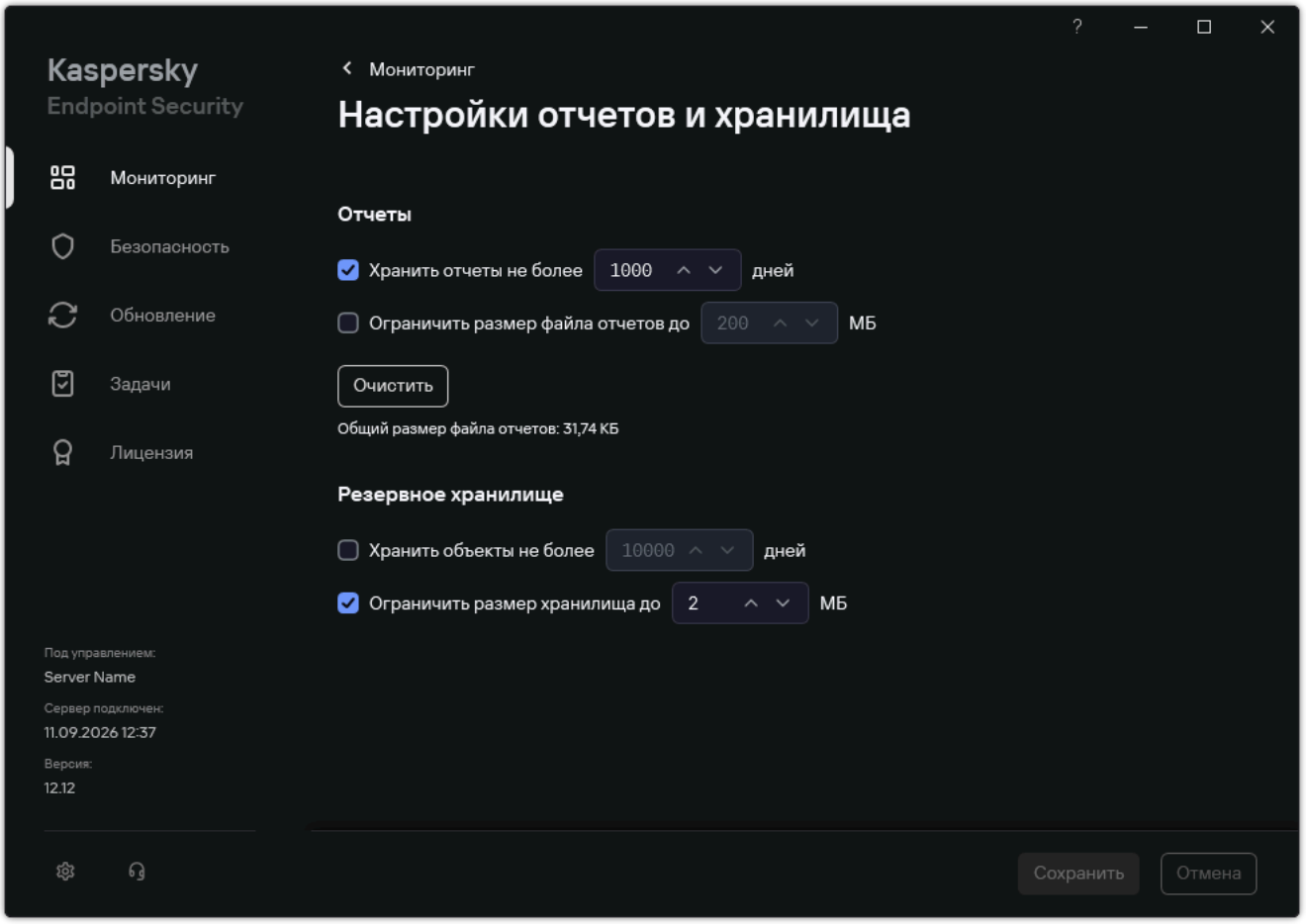
Настройка максимального размера файла отчета

Вы можете указать максимальный размер файла, содержащего отчет. По умолчанию максимальный размер файла отчета составляет 1024 МБ. После достижения максимального размера файла отчета Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчета таким образом, чтобы размер файла отчетов не превышал максимального значения.

Чтобы настроить максимальный размер файла отчета, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** нажмите на плитку **Отчеты и хранилище**.



Параметры отчетов

3. В блоке **Отчеты** установите флажок **Ограничить размер файла отчетов до N МБ**, если хотите ограничить размер файла отчета. Укажите максимальный размер файла отчета.

4. Сохраните внесенные изменения.

Сохранение отчета в файл

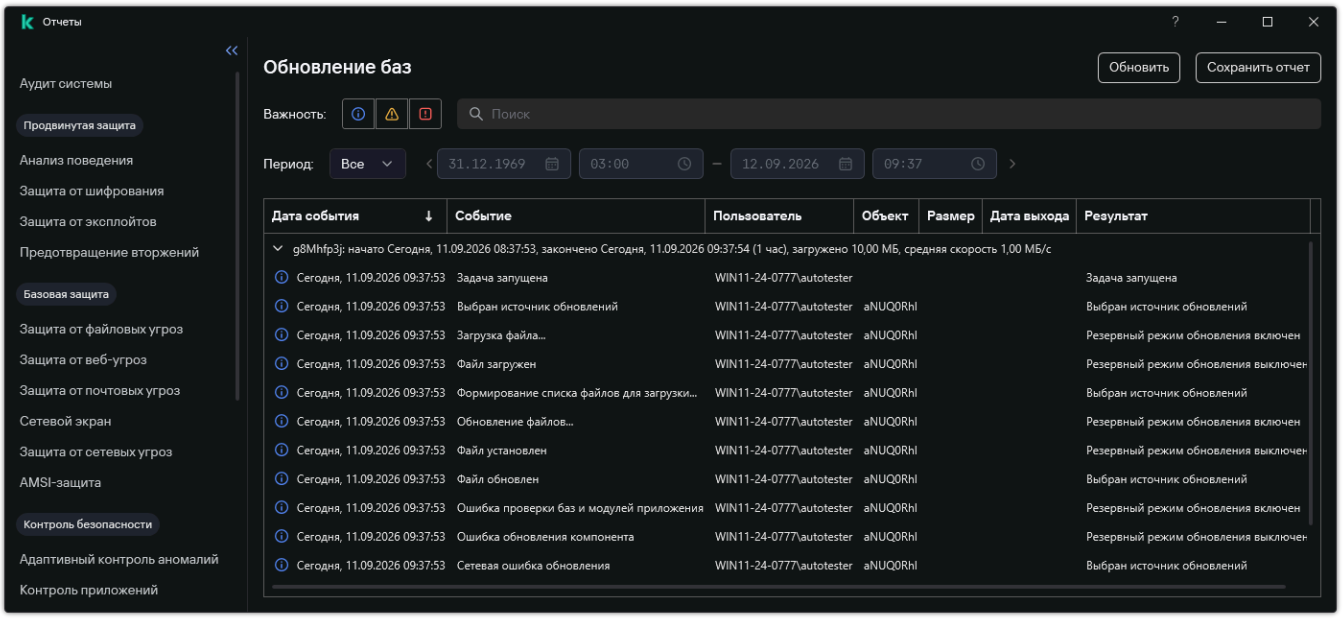
Пользователь сам несет ответственность за обеспечение безопасности информации из сохраненного в файл отчета и, в частности, за контроль и ограничение доступа к этой информации.

Сформированный отчет вы можете сохранить в файл текстового формата TXT или CSV.

Kaspersky Endpoint Security сохраняет событие в отчет в том виде, в каком событие отображается на экране, то есть с тем же составом и с той же последовательностью атрибутов события.

Чтобы сохранить отчет в файл, выполните следующие действия:

1. В главном окне приложения в разделе **Мониторинг** нажмите на плитку **Отчеты**.



Отчеты

2. В открывшемся окне выберите компонент или задачу.

   В правой части окна отобразится отчет, содержащий список событий о работе выбранного компонента или задачи Kaspersky Endpoint Security.

3. Если требуется, измените представление данных в отчете с помощью следующих способов:

   - фильтрация событий;
   - поиск событий;
   - изменение расположения граф;
   - сортировка событий.

4. Нажмите на кнопку **Сохранить отчет**, расположенную в верхней правой части окна.

5. В открывшемся окне укажите папку, в которую вы хотите сохранить файл отчета.

6. Введите название файла отчета.

7. Выберите нужный формат файла отчета: TXT или CSV.

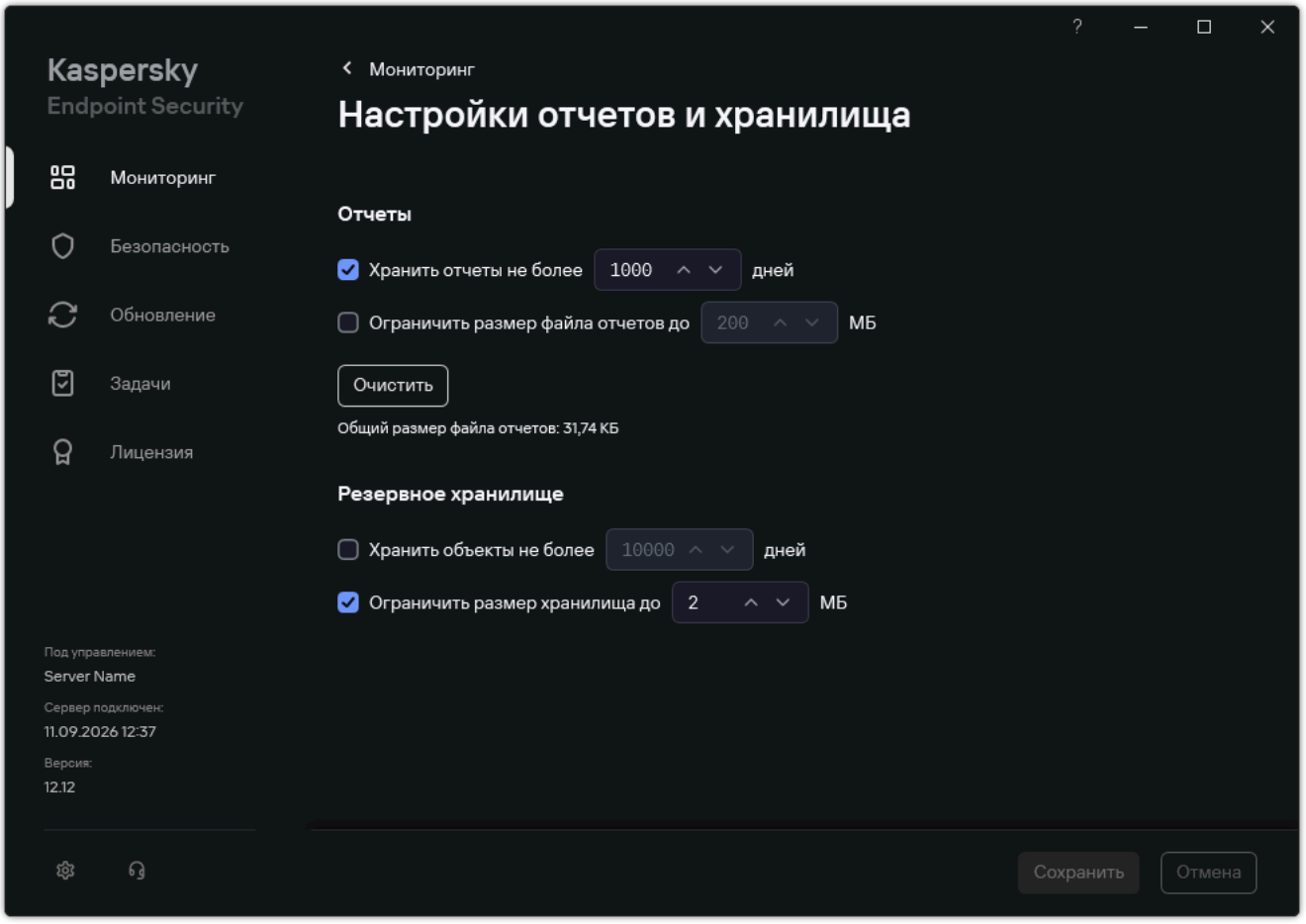
8. Сохраните внесенные изменения.

Удаление информации из отчетов

Чтобы удалить информацию из отчетов, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** нажмите на плитку **Отчеты и хранилище**.



Параметры отчетов

3. В блоке **Отчеты** нажмите на кнопку **Очистить**.

4. Если включена Защита паролем, Kaspersky Endpoint Security может запросить учетные данные пользователя. Приложение запрашивает учетные данные, если у пользователя нет необходимого разрешения.

Kaspersky Endpoint Security удалит все отчеты для всех компонентов и задач приложения.

Самозащита Kaspersky Endpoint Security

Самозащита предотвращает выполнение другими приложениями действий, которые могут нарушить работу Kaspersky Endpoint Security и, например, удалить Kaspersky Endpoint Security с компьютера. Набор доступных технологий самозащиты Kaspersky Endpoint Security зависит от разрядности операционной системы (см. таблицу ниже). Также к средствам самозащиты относятся Защита паролем и Защита подключения к Серверу администрирования.

Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы приложения).

Защита подключения к Серверу администрирования предотвращает несанкционированное переподключение компьютера к недоверенному серверу.

Технологии самозащиты Kaspersky Endpoint Security

Технология	Описание	Компьютер на базе x86	Компьютер на базе x64
Механизм самозащиты	Технология блокирует доступ к следующим компонентам приложения: • файлы в папке установки Kaspersky Endpoint Security и другие файлы приложения; • раздел реестра с ключами приложения; • процессы, которые запускает приложение.	✓	✓
AM-PPL (Antimalware Protected Process Light)	Технология защищает процессы Kaspersky Endpoint Security от вредоносных действий. Подробнее о технологии AM-PPL см. на сайте Microsoft. Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.	✓	✓
Механизм защиты от внешнего управления	Технология блокирует другим приложениям доступ к Kaspersky Endpoint Security (например, приложения TeamViewer или RemotelyAnywhere).	✓	– (кроме Windows 7)

Включение и выключение механизма самозащиты

Kaspersky Endpoint Security предотвращает изменение и удаление файлов приложения на жестком диске, процессов в памяти и записей в системном реестре.

Технология блокирует доступ к следующим компонентам приложения:

- файлы в папке установки Kaspersky Endpoint Security и другие файлы приложения;
- раздел реестра с ключами приложения;
- процессы, которые запускает приложение.

Механизмы самозащиты не распространяются на процессы Kaspersky Endpoint Security, инициированные недоверенными родительскими процессами.

По умолчанию механизм самозащиты Kaspersky Endpoint Security включен.

Как включить или выключить механизм самозащиты в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки → Настройки приложения**.
4. Используйте флажок **Включить самозащиту**, чтобы включить или выключить механизм самозащиты.
5. Сохраните внесенные изменения.

Как включить или выключить механизм самозащиты в Web Console и Cloud Console

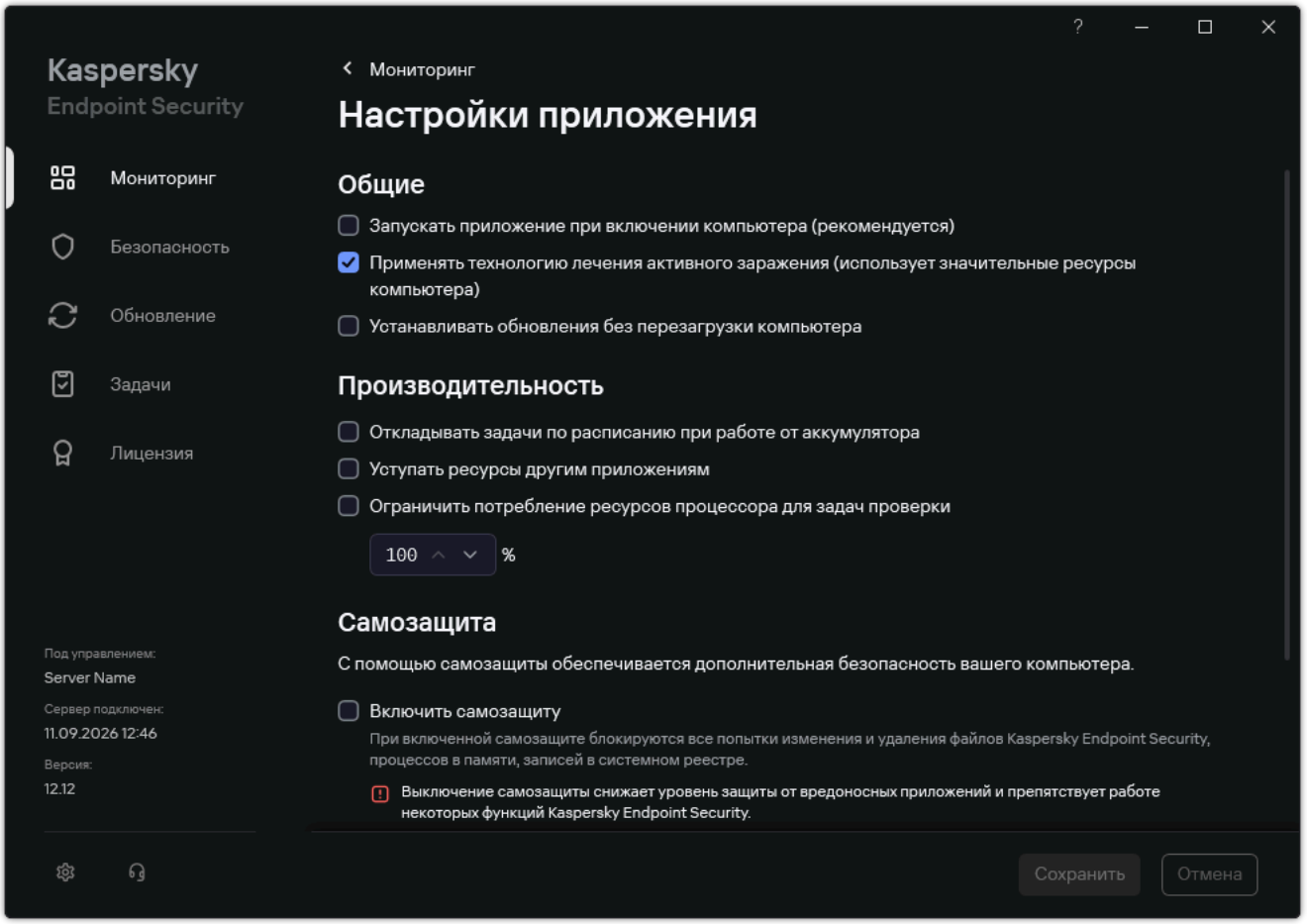
1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки → Самозащита**.
5. Используйте переключатель **Самозащита ВКЛЮЧЕНА**, чтобы включить или выключить механизм самозащиты.
6. Сохраните внесенные изменения.

Как включить или выключить механизм самозащиты в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.



Параметры приложения Kaspersky Endpoint Security для Windows

3. Используйте флажок **Включить самозащиту**, чтобы включить или выключить механизм самозащиты.

4. Сохраните внесенные изменения.

Включение и выключение поддержки AM-PPL

Kaspersky Endpoint Security поддерживает технологию Antimalware Protected Process Light (далее "AM-PPL") от Microsoft. AM-PPL защищает процессы Kaspersky Endpoint Security от вредоносных действий (например, завершение работы приложения). AM-PPL разрешает запуск только доверенных процессов. Процессы Kaspersky Endpoint Security подписаны в соответствии с требованиями безопасности Windows, поэтому являются доверенными. Подробнее о технологии AM-PPL см. на сайте Microsoft. По умолчанию технология AM-PPL включена.

Kaspersky Endpoint Security также имеет встроенные механизмы защиты процессов приложения. Поддержка AM-PPL позволяет делегировать функции защиты процессов операционной системе. Таким образом, вы увеличиваете быстродействие приложения и уменьшаете потребление ресурсов компьютера.

Используйте технологию AM-PPL постоянно. AM-PPL является важным компонентом защиты операционной системы. Выключение поддержки технологии AM-PPL может привести к сбоям в работе некоторых функций Kaspersky Endpoint Security (например, интеграция приложения с Windows Security Center). Разрешается выключать поддержку технологии AM-PPL только в отдельной тестовой среде для диагностики неисправностей в работе приложения.

Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.

Чтобы включить или выключить поддержку технологии AM-PPL, выполните следующие действия:

1. Выключите механизм самозащиты приложения.

   Механизм самозащиты предотвращает изменение и удаление процессов приложения в памяти компьютера, в том числе изменение статуса AM-PPL.

2. Запустите интерпретатор командной строки cmd от имени администратора.

3. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

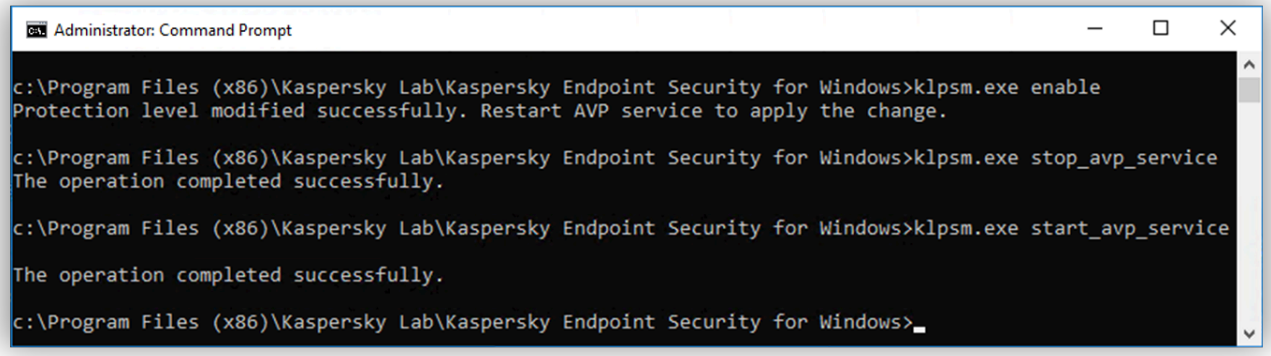
   Вы можете добавить в системную переменную %PATH% путь к исполняемому файлу при установке приложения.

4. В командной строке введите:

   - `klpsm.exe enable` – включение поддержки технологии AM-PPL (см. рис. ниже).
   - `klpsm.exe disable` – выключение поддержки технологии AM-PPL.

5. Перезапустите Kaspersky Endpoint Security.

6. Возобновите работу механизма самозащиты приложения.



Включение поддержки технологии AM-PPL

Защита служб приложения от внешнего управления

Защита служб приложения от внешнего управления блокирует попытки пользователей и других приложений остановить работу служб Kaspersky Endpoint Security. Защита обеспечивает работу следующих служб:

- служба Kaspersky Endpoint Security (AVP.KES.14.3);
- служба Kaspersky Seamless Update Service (AVPSUS.KES.14.3).

Для завершения работы приложения из командной строки необходимо, чтобы защита от внешнего управления службами Kaspersky Endpoint Security была выключена.

Вы можете предоставить возможность внешнего управления службами приложения только на компьютерах без поддержки технологии AM-PPL или с выключенной технологией.

Как включить или выключить защиту служб приложения от внешнего управления в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Настройки приложения**.
4. Используйте флажок **Блокировать внешнее управление службами приложения**, чтобы включить или выключить защиту служб Kaspersky Endpoint Security от внешнего управления.
5. Сохраните внесенные изменения.

Как включить или выключить защиту служб приложения от внешнего управления в Web Console и Cloud Console

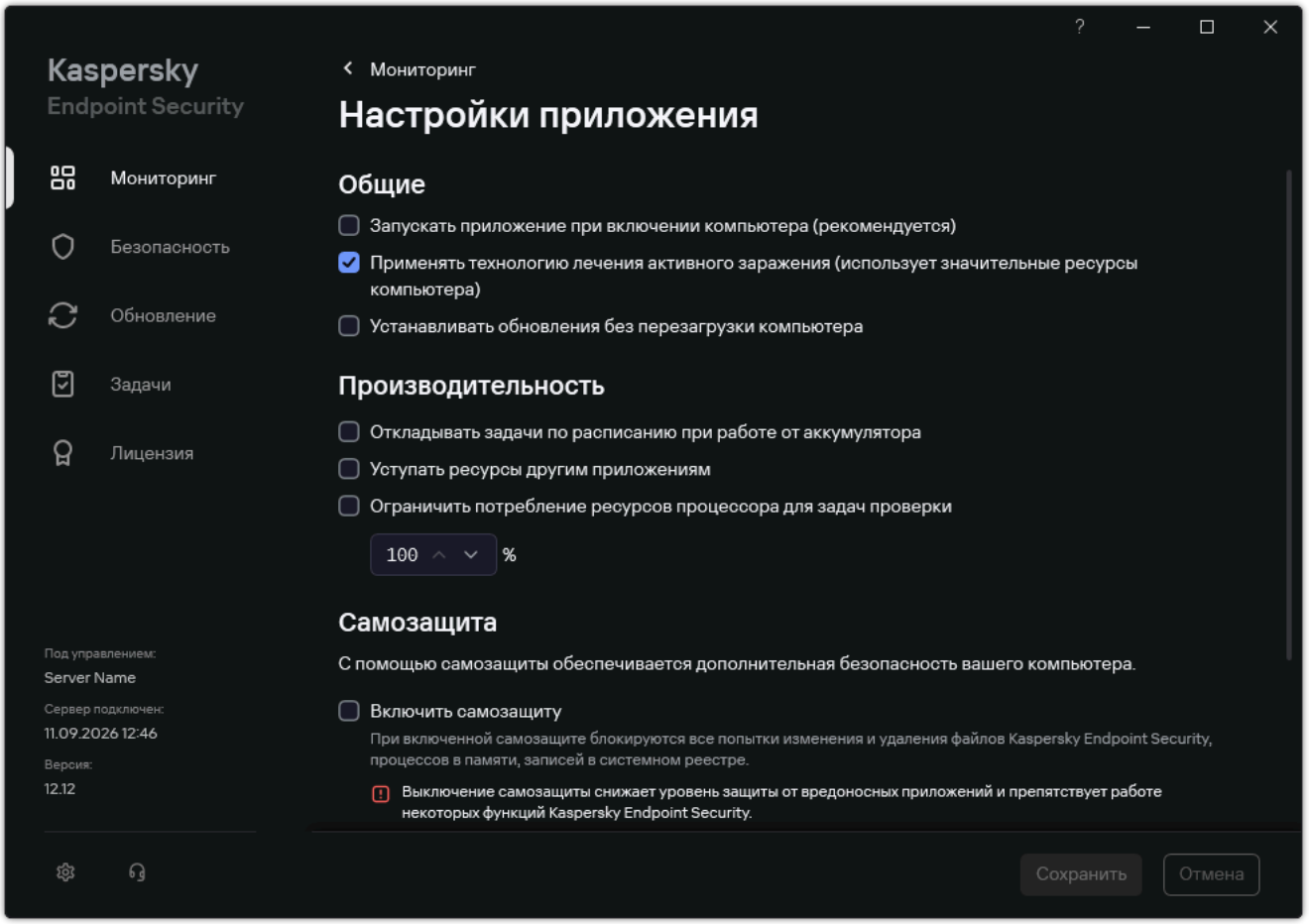
1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Самозащита**.
5. Используйте флажок **Блокировать внешнее управление службами приложения**, чтобы включить или выключить защиту служб Kaspersky Endpoint Security от внешнего управления.
6. Сохраните внесенные изменения.

Как включить или выключить защиту служб приложения от внешнего управления в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.

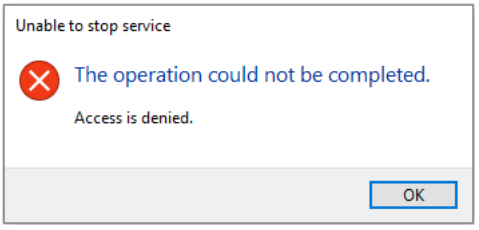


Параметры приложения Kaspersky Endpoint Security для Windows

3. Используйте флажок **Блокировать внешнее управление службами приложения**, чтобы включить или выключить защиту служб Kaspersky Endpoint Security от внешнего управления.

4. Сохраните внесенные изменения.

В результате при попытке пользователя остановить работу служб приложения отображается системное окно с ошибкой. Пользователь может управлять службами приложения только из интерфейса Kaspersky Endpoint Security.



Ошибка доступа к службам приложения

Обеспечение работы приложений удаленного администрирования

Нередко возникают ситуации, когда при использовании механизма защиты от внешнего управления возникает необходимость применить приложения удаленного администрирования.

Чтобы обеспечить работу приложений удаленного администрирования, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Исключения и типы обнаруживаемых объектов**.
3. В блоке **Исключения** перейдите по ссылке **Указать доверенные приложения**.
4. В открывшемся окне нажмите на кнопку **Добавить**.
5. Выберите исполняемый файл приложения удаленного администрирования.

   Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
6. Установите флажок **Разрешить взаимодействие с интерфейсом Kaspersky Endpoint Security для Windows**.
7. Сохраните внесенные изменения.

Защита паролем

Компьютер могут использовать несколько пользователей с разным уровнем компьютерной грамотности. Неограниченный доступ пользователей к Kaspersky Endpoint Security и его параметрам может привести к снижению уровня безопасности компьютера в целом. Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы приложения).

Если пользователь, который запустил сессию Windows, (*сессионный пользователь*) имеет разрешение на выполнение действия, Kaspersky Endpoint Security не запрашивает имя пользователя и пароль или временный пароль. Пользователь получает доступ к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями.

Если у сессионного пользователя отсутствует разрешение на выполнение действия, пользователь может получить доступ к приложению следующими способами:

- Ввод имени пользователя и пароля.

  Этот способ удобен для повседневной работы. Для выполнения действия, защищенного паролем, требуется ввести данные доменной учетной записи пользователя с необходимым разрешением. При этом компьютер должен быть в домене. Если компьютер не в домене, вы можете использовать учетную запись KLAdmin или учетную запись, добавленную вручную.

- Ввод временного пароля.

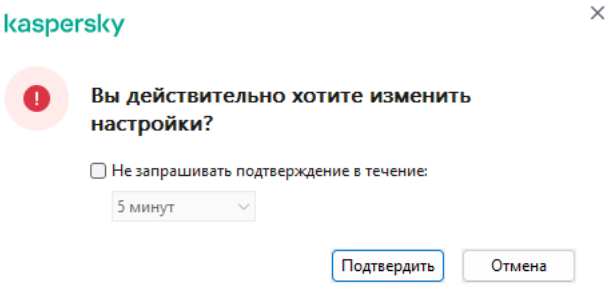
  Этот способ удобен, если пользователь находится вне корпоративной сети и необходимо предоставить ему временное разрешение на выполнение запрещенного действия (например, завершить работу приложения). По истечении срока действия временного пароля или истечении сессии приложение возвращает параметры Kaspersky Endpoint Security в прежнее состояние.

- Токен.

  Этот способ удобен для привилегированных пользователей (специалистов технической поддержки, например). Аутентификация по токену позволяет использовать режим входа в систему по смарт-карте в Active Directory. Это повышает уровень безопасности инфраструктуры организации.

При попытке пользователя выполнить действие, защищенное паролем, Kaspersky Endpoint Security предложит пользователю ввести имя пользователя и пароль, пароль от токена или временный пароль (см. рис. ниже).

В окне ввода пароля язык ввода можно поменять только с помощью одновременного нажатия клавиш **ALT+SHIFT**. При использовании других комбинаций клавиш, даже если они установлены в операционной системе, смена языка ввода не происходит.



Запрос пароля для доступа к Kaspersky Endpoint Security

Имя пользователя и пароль

Для доступа к Kaspersky Endpoint Security необходимо ввести данные учетной записи. Защита паролем поддерживает работу со следующими учетными записями:

- **KLAdmin**. Учетная запись администратора без ограничений доступа к Kaspersky Endpoint Security. Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем. Отменить разрешение для учетной записи KLAdmin невозможно. Kaspersky Endpoint Security требует задать пароль для учетной записи KLAdmin во время включения Защиты паролем.

- **Учетная запись, добавленная вручную**. Учетная запись вне домена Active Directory. Это сервисная учетная запись, которую вы можете использовать вместо KLAdmin, чтобы не делиться паролем от учетной записи администратора. Вы можете задать любые имя пользователя и пароль, а также настроить отдельные разрешения.

- **Группа "Все"**. Стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети. Пользователи из группы "Все" могут получить доступ к приложению в соответствии с предоставленными разрешениями.

- **Отдельные пользователи или группы**. Учетные записи пользователей, для которых вы можете настроить отдельные разрешения. Например, если для группы "Все" выполнение действия запрещено, то вы можете разрешить выполнение действия для отдельного пользователя или группы.

- **Сессионный пользователь**. Учетная запись пользователя, который запустил сессию Windows. Вы можете сменить сессионного пользователя во время ввода пароля (флажок **Запомнить пароль на текущую сессию**). В этом случае Kaspersky Endpoint Security назначает сессионным пользователем, учетные данные которого вы ввели, вместо пользователя, который запустил сессию Windows.

Временный пароль

Временный пароль позволяет предоставить временный доступ к Kaspersky Endpoint Security для отдельного компьютера вне корпоративной сети. Администратор создает временный пароль для отдельного компьютера в Kaspersky Security Center в свойствах компьютера пользователя. Администратор выбирает действия, на которые будет распространяться временный пароль, и срок действия временного пароля.

Токен

Для доступа к Kaspersky Endpoint Security необходимо выбрать нужный сертификат пользователя из списка сертификатов, хранящихся на подключенном токене, и ввести PIN-код. Аутентификация по токену доступна только для пользователей внутри домена Active Directory. Администратор может настроить разрешения для отдельного пользователя или группы. Для работы аутентификации по токену необходимо развернуть доверенную инфраструктуру PKI, а также установить специальное программного обеспечение для работы с токеном.

Включение Защиты паролем

Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы приложения).

Как включить Защиту паролем в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Интерфейс**.
4. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

   Откроется окно с параметрами Защиты паролем.
5. Используйте флажок **Включить защиту паролем**, чтобы включить или выключить компонент.
6. В блоке **Разрешения** выберите учетную запись KLAdmin.

7. В открывшемся окне нажмите на кнопку **Пароль** и задайте пароль для учетной записи KLAdmin.

   Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем.

   > Если вы забыли пароль для учетной записи KLAdmin, вы можете сбросить пароль в свойствах политики.

8. Вернитесь к списку учетных записей.

9. Настройте разрешения для всех пользователей внутри корпоративной сети:

   a. В блоке **Разрешения** выберите группу "Все".

      Группа "Все" – стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети.

   b. В открывшемся окне установите флажки напротив тех действий, которые будут доступны пользователям без ввода пароля.

      Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы приложения** снят, вы можете завершить работу приложения только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением или с помощью временного пароля.

      > Разрешения Защиты паролем имеют ряд особенностей. Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.

10. Сохраните внесенные изменения.

Как включить Защиту паролем в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки** → **Самозащита**.

5. В блоке **Защита паролем** используйте переключатель **Защита паролем ВКЛЮЧЕНА**, чтобы включить или выключить компонент.

6. Задайте пароль для учетной записи KLAdmin и подтвердите его.

   Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем.

   > Если вы забыли пароль для учетной записи KLAdmin, вы можете сбросить пароль в свойствах политики.

7. Вернитесь к списку учетных записей.

8. Настройте разрешения для всех пользователей внутри корпоративной сети:

   a. В таблице учетных записей выберите группу "Все".

      Группа "Все" – стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети.

   b. В открывшемся окне установите флажки напротив тех действий, которые будут доступны пользователям без ввода пароля.

      Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы приложения** снят, вы можете завершить работу приложения только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением или с помощью временного пароля.

      Разрешения Защиты паролем имеют ряд особенностей. Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.

9. Сохраните внесенные изменения.

Как включить Защиту паролем в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки интерфейса**.

3. Используйте переключатель **Защита паролем**, чтобы включить или выключить компонент.

4. Задайте пароль для учетной записи KLAdmin и подтвердите его.

   Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем.

   Если компьютер работает под управлением политики, администратор может сбросить пароль для учетной записи KLAdmin в свойствах политики. Если компьютер не подключен к Kaspersky Security Center, и вы забыли пароль для учетной записи KLAdmin, восстановить пароль невозможно.

5. Настройте разрешения для всех пользователей внутри корпоративной сети:

   a. В таблице учетных записей откройте список разрешений для группы "Все" по кнопке **Изменить**.

      Группа "Все" – стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети.

   b. Установите флажки напротив тех действий, которые будут доступны пользователям без ввода пароля.

      Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы приложения** снят, вы можете завершить работу приложения только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением или с помощью временного пароля.

      Разрешения Защиты паролем имеют ряд особенностей. Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.

6. Сохраните внесенные изменения.

После включения Защиты паролем приложение ограничит доступ пользователей к Kaspersky Endpoint Security в соответствии с разрешениями для группы "Все". Вы можете выполнить запрещенные для группы "Все" действия только с помощью учетной записи KLAdmin, отдельной учетной записи с нужными разрешениями или с помощью временного пароля.

Вы можете выключить Защиту паролем только с помощью учетной записи KLAdmin. Выключить защиту паролем с помощью другой учетной записи или с помощью временного пароля невозможно.

Во время проверки пароля вы можете установить флажок **Запомнить пароль на текущую сессию**. В этом случае Kaspersky Endpoint Security не будет требовать ввода пароля при попытке пользователя выполнить другое разрешенное действие, защищенное паролем, в течение сессии.

Предоставление разрешений для отдельных пользователей или групп

Защита паролем позволяет предоставить доступ к Kaspersky Endpoint Security для отдельных учетных записей Active Directory, а также учетных записей, добавленных вручную.

Учетные записи Active Directory

Вы можете предоставить доступ к Kaspersky Endpoint Security для отдельных пользователей или групп внутри домена Active Directory. Например, если группе "Все" запрещено завершать работу приложения, вы можете предоставить отдельному пользователю разрешение **Завершение работы приложения**. В результате вы можете завершить работу приложения только с помощью учетной записи этого пользователя или учетной записи KLAdmin.

Вы можете использовать данные учетной записи для доступа к приложению, только если компьютер в домене. Если компьютер не в домене, вы можете использовать учетную запись KLAdmin или временный пароль.

Учетные записи, добавленные вручную

Вы можете создать учетную запись, которой нет в Active Directory, и назначить этой учетной записи отдельные разрешения. То есть вы можете создать *сервисную учетную запись* и использовать эту учетную запись вместо KLAdmin. Таким образом, вам не нужно делиться паролем от KLAdmin с другими пользователями или создавать новые учетные записи Active Directory. Вы можете задать любые имя пользователя и пароль. Например, вы можете предоставить пользователю сервисной учетной записи разрешение **Просмотр отчетов**. В результате, если для группы "Все" просмотр отчетов запрещен, вы можете открыть отчеты приложения с помощью сервисной учетной записи или учетной записи KLAdmin.

Предоставление разрешений для отдельных пользователей или групп

Как предоставить разрешение для отдельных пользователей или групп в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Интерфейс**.
4. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

   Откроется окно с параметрами Защиты паролем.
5. В таблице учетных записей нажмите на кнопку **Добавить**.
6. Выберите тип учетной записи, которую вы хотите добавить:

   - **Выбрать пользователя / группу из Active Directory** – учетные записи Active Directory.

     Для выбора учетной записи нажмите на кнопку **Выбрать**. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.

   - **Добавить пользователя / группу вручную** – сервисная учетная запись, заданная вручную.

     Для добавления сервисной учетной записи введите имя пользователя и пароль (например, SecureAdmin).

     Вы можете сбросить пароль сервисной учетной записи в свойствах политики. Действия по сбросу пароля сервисной учетной записи не отличаются от действий по сбросу пароля KLAdmin. Если изменение параметров Защиты паролем разрешено ("замок" открыт) или политика на компьютере отсутствует, вы можете сбросить пароль сервисной учетной записи в интерфейсе приложения. Для этого нужно подтвердить изменение данных сервисной учетной записи с помощью пароля KLAdmin.
7. В списке **Разрешения** установите флажки напротив тех действий, которые будут доступны добавленному пользователю или группе без ввода пароля.

   Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы приложения** снят, вы можете завершить работу приложения только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением или с помощью временного пароля.

   Разрешения Защиты паролем имеют ряд особенностей. Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.
8. Сохраните внесенные изменения.

Как предоставить разрешение для отдельных пользователей или групп в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Самозащита**.
5. В блоке **Защита паролем** перейдите по ссылке **Пользовательские разрешения**.

   Откроется форма предоставления разрешений Защиты паролем.
6. Нажмите на кнопку **Добавить**.
7. Выберите тип учетной записи, которую вы хотите добавить:

   - **Выбрать из Active Directory** – учетные записи Active Directory.

     Для выбора учетной записи нажмите на кнопку **Изменить**. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.
   - **Добавить вручную** – сервисная учетная запись, заданная вручную.

     Для добавления сервисной учетной записи введите имя пользователя и пароль (например, SecureAdmin).

     > Вы можете сбросить пароль сервисной учетной записи в свойствах политики. Действия по сбросу пароля сервисной учетной записи не отличаются от действий по сбросу пароля KLAdmin. Если изменение параметров Защиты паролем разрешено ("замок" открыт) или политика на компьютере отсутствует, вы можете сбросить пароль сервисной учетной записи в интерфейсе приложения. Для этого нужно подтвердить изменение данных сервисной учетной записи с помощью пароля KLAdmin.
8. В списке **Разрешения** установите флажки напротив тех действий, которые будут доступны добавленному пользователю или группе без ввода пароля.

   Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы приложения** снят, вы можете завершить работу приложения только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением или с помощью временного пароля.

   > Разрешения Защиты паролем имеют ряд особенностей. Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.
9. Нажмите на кнопку **Добавить**.
10. Сохраните внесенные изменения.

Как предоставить разрешение для отдельных пользователей или групп в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки интерфейса**.

3. В таблице учетных записей нажмите на кнопку **Добавить**.

4. Выберите тип учетной записи, которую вы хотите добавить:

   - **Выбрать пользователя / группу из Active Directory** – учетные записи Active Directory.

     Для выбора учетной записи нажмите на кнопку **Выбрать пользователя или группу**. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.

   - **Добавить пользователя вручную** – сервисная учетная запись, заданная вручную.

     Для добавления сервисной учетной записи введите имя пользователя и пароль (например, SecureAdmin).

     Вы можете сбросить пароль сервисной учетной записи в свойствах политики. Действия по сбросу пароля сервисной учетной записи не отличаются от действий по сбросу пароля KLAdmin. Если изменение параметров Защиты паролем разрешено ("замок" открыт) или политика на компьютере отсутствует, вы можете сбросить пароль сервисной учетной записи в интерфейсе приложения. Для этого нужно подтвердить изменение данных сервисной учетной записи с помощью пароля KLAdmin.

5. В списке **Разрешения** установите флажки напротив тех действий, которые будут доступны добавленному пользователю или группе без ввода пароля.

   Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы приложения** снят, вы можете завершить работу приложения только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением или с помощью временного пароля.

   Разрешения Защиты паролем имеют ряд особенностей. Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.

6. Сохраните внесенные изменения.

В результате, если для группы "Все" доступ к приложению ограничен, пользователи получат доступ к Kaspersky Endpoint Security в соответствии с разрешениями для этих пользователей.

Использование временного пароля для предоставления разрешений

Временный пароль позволяет предоставить временный доступ к Kaspersky Endpoint Security для отдельного компьютера вне корпоративной сети. Это нужно, чтобы разрешить выполнение запрещенного действия без передачи пользователю учетных данных KLAdmin. Для использования временного пароля компьютер должен быть добавлен в Kaspersky Security Center.

Как предоставить пользователю разрешение на выполнение запрещенного действия с помощью временного пароля через Консоль администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите вкладку **Устройства**.

4. Откройте свойства компьютера двойным щелчком мыши.

5. В окне свойств компьютера выберите раздел **Приложения**.

6. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows (14.3)** и откройте свойства приложения двойным щелчком мыши.

7. В окне параметров приложения выберите раздел **Общие настройки → Интерфейс**.

8. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

9. В открывшемся окне в блоке **Временный пароль** нажмите на кнопку **Список временных паролей**.

   Откроется окно Мониторинга временных паролей.

10. Нажмите на кнопку **Добавить**.

11. В поле **Дата истечения** установите срок действия временного пароля.

12. В таблице **Область действия временного пароля** установите флажки напротив тех действий, которые будут доступны пользователю после ввода временного пароля.

13. Нажмите на кнопку **Создать**.

    Откроется окно с временным паролем (см. рис. ниже).

14. Скопируйте и передайте пользователю пароль.

Как предоставить пользователю разрешение на выполнение запрещенного действия с помощью временного пароля через Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.

2. Нажмите на имя компьютера, на котором вы хотите предоставить пользователю разрешение на выполнение запрещенного действия.

3. Выберите вкладку **Приложения**.

4. Нажмите на **Kaspersky Endpoint Security для Windows**.

   Откроются локальные параметры приложения.

5. Выберите вкладку **Параметры приложения**.

6. В окне параметров приложения выберите раздел **Общие настройки → Интерфейс**.

7. В блоке **Временные пароли** нажмите на кнопку **Добавить**.

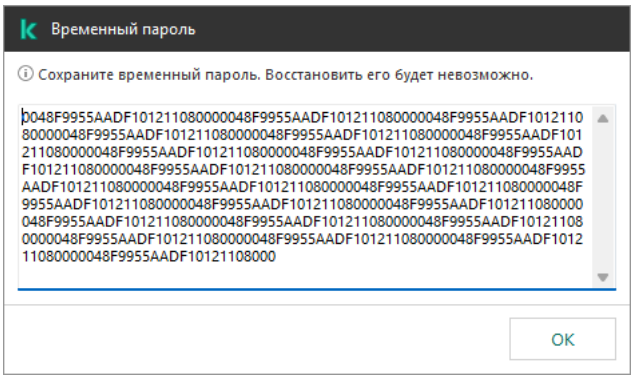
8. В поле **Дата истечения** установите срок действия временного пароля.

9. В таблице **Область действия временного пароля** установите флажки напротив тех действий, которые будут доступны пользователю после ввода временного пароля.

10. Нажмите на кнопку **Создать**.

    Откроется окно с временным паролем.

11. Скопируйте и передайте пользователю пароль.

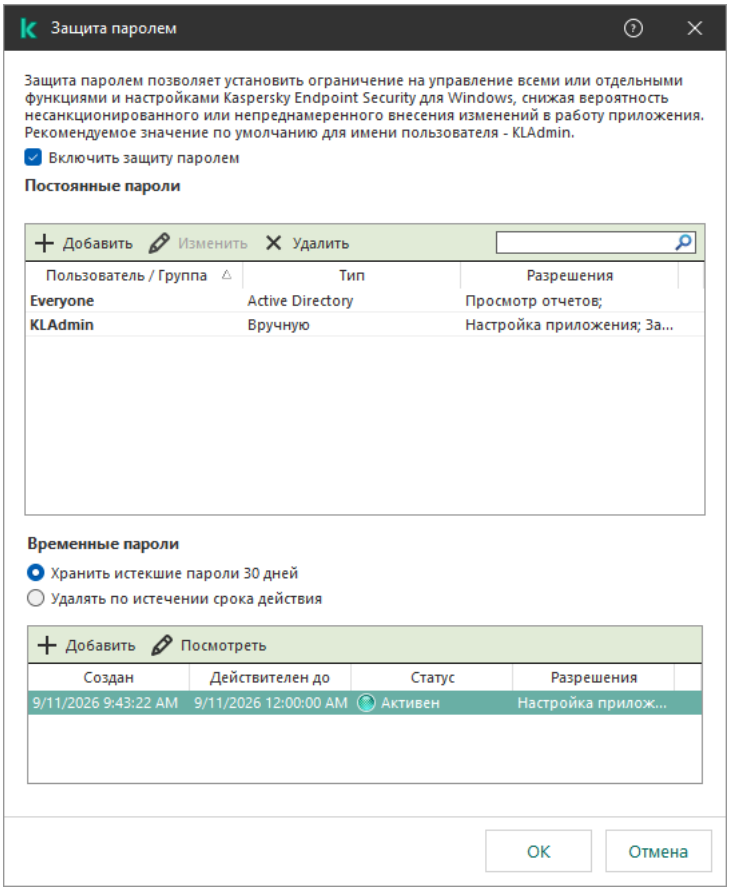


Временный пароль

Отзыв временного пароля

Начиная с версии Kaspersky Endpoint Security для Windows 12.9 добавлен инструмент *Мониторинг временных паролей*. Мониторинг временных паролей позволяет выполнять следующие действия:

- сохранять историю паролей (до 30 дней);
- контролировать статус временного пароля: *Активен*, *Истек*, *Отозван*,
- отзывать временные пароли.



Мониторинг временных паролей

Мониторинг временных паролей обновляет статус пароля и отзывает пароль только после синхронизации компьютера с Kaspersky Security Center.

Как отозвать временный пароль через Консоль администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите вкладку **Устройства**.
4. Откройте свойства компьютера двойным щелчком мыши.
5. В окне свойств компьютера выберите раздел **Приложения**.
6. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows (14.3)** и откройте свойства приложения двойным щелчком мыши.
7. В окне параметров приложения выберите раздел **Общие настройки → Интерфейс**.
8. В блоке **Защита паролем** нажмите на кнопку **Настройка**.
9. В открывшемся окне в блоке **Временный пароль** настройте параметры хранения истекших паролей.
10. Нажмите на кнопку **Список временных паролей**.

    Откроется окно Мониторинга временных паролей. Мониторинг временных паролей отображает срок действия пароля, статус пароля и список разрешений.
11. Выберите активный временный пароль, который вы хотите отозвать, и откройте свойства пароля двойным щелчком мыши.
12. В открывшемся окне нажмите на кнопку **Отозвать**.
13. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как отозвать временный пароль через Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите предоставить пользователю разрешение на выполнение запрещенного действия.
3. Выберите вкладку **Приложения**.
4. Нажмите на **Kaspersky Endpoint Security для Windows**.

    Откроются локальные параметры приложения.
5. Выберите вкладку **Параметры приложения**.
6. В окне параметров приложения выберите раздел **Общие настройки → Интерфейс**.
7. В блоке **Временные пароли** настройте параметры хранения истекших паролей.

8. Перейдите по ссылке **Временный пароль**.

   Откроется окно Мониторинга временных паролей. Мониторинг временных паролей отображает срок действия пароля, статус пароля и список разрешений.

9. Выберите активный временный пароль, который вы хотите отозвать.

10. В открывшемся окне нажмите на кнопку **Отозвать пароль**.

11. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

В результате Мониторинг временных паролей установит статус пароля *Отзывается (синхронизация с хостом)*. После синхронизации компьютера с Kaspersky Security Center приложение отзывает временный пароль и блокирует предоставленные разрешения немедленно.

Особенности разрешений Защиты паролем

Разрешения Защиты паролем имеют ряд особенностей и ограничений.

Настройка приложения

Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты открыты).

Завершение работы приложения

Особенностей и ограничений нет.

Выключение компонентов защиты

- Предоставить разрешение на выключение компонентов защиты для группы "Все" невозможно. Чтобы разрешить выключение компонентов защиты не только пользователю KL Admin, но и другим пользователям, добавьте пользователя или группу с разрешением **Выключение компонентов защиты** в параметрах Защиты паролем.

- Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты открыты).

- Для выключения компонентов защиты в параметрах приложения пользователь должен иметь разрешение **Настройка приложения**.

- Для выключения компонентов защиты из контекстного меню (пункт **Приостановить защиту**) пользователь, кроме разрешения **Выключение компонентов защиты**, должен иметь разрешение **Выключение компонентов контроля**.

Выключение компонентов контроля

- Предоставить разрешение на выключение компонентов контроля для группы "Все" невозможно. Чтобы разрешить выключение компонентов защиты не только пользователю KL Admin, но и другим пользователям, добавьте пользователя или группу с разрешением **Выключение компонентов контроля** в параметрах Защиты паролем.
- Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты открыты).
- Для выключения компонентов контроля в параметрах приложения пользователь должен иметь разрешение **Настройка приложения**.
- Для выключения компонентов контроля из контекстного меню (пункт **Приостановить защиту**) пользователь, кроме разрешения **Выключение компонентов контроля**, должен обладать разрешением **Выключение компонентов защиты**.

Выключение политики Kaspersky Security Center

Предоставить разрешение на выключение политики Kaspersky Security Center для группы "Все" невозможно. Чтобы разрешить выключение политики не только пользователю KL Admin, но и другим пользователям, добавьте пользователя или группу с разрешением **Выключение политики Kaspersky Security Center** в параметрах Защиты паролем.

Удаление ключа

Особенностей и ограничений нет.

Удаление / изменение / восстановление приложения

Если вы предоставили разрешение на удаление, изменение и восстановление приложения для группы "Все", Kaspersky Endpoint Security не будет требовать ввода пароля при попытке пользователя выполнить эти операции. Таким образом, любой пользователь, включая пользователей вне домена, может установить, изменить или восстановить приложение.

Восстановление доступа к данным на зашифрованном устройстве

Вы можете восстановить доступ к данным на зашифрованных устройствах только с помощью учетной записи KL Admin. Разрешить это действие другому пользователю невозможно.

Просмотр отчетов

Особенностей и ограничений нет.

Восстановление из резервного хранилища

Особенностей и ограничений нет.

Экспорт настроек

По умолчанию экспорт настроек приложения запрещен для группы "Все". Вы можете экспортировать настройки приложения с помощью учетной записи KLAdmin. Экспорт настроек приложения включает в себя только создание конфигурационного файла с параметрами Kaspersky Endpoint Security в интерфейсе приложения. Разрешение не ограничивает экспорт списков исключений из проверки, доверенных веб-адресов, доверенных устройств или других списков компонентов приложения.

Сброс пароля KLAdmin

Если вы забыли пароль для учетной записи KLAdmin, вы можете сбросить пароль в свойствах политики. Сбросить пароль в интерфейсе приложения невозможно.

Вы можете выполнять действия, защищенные паролем, с помощью временного пароля. В этом случае вводить данные учетной записи KLAdmin не нужно.

Если компьютер не подключен к Kaspersky Security Center и вы забыли пароль для учетной записи KLAdmin, восстановить пароль невозможно.

Как сбросить пароль для учетной записи KLAdmin в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Интерфейс**.
4. В блоке **Защита паролем** нажмите на кнопку **Настройка**.
5. В открывшемся окне снимите флажок **Включить защиту паролем**.
6. Сохраните внесенные изменения.
7. Повторно установите флажок **Включить защиту паролем**.

8. Нажмите на кнопку **OK**.

   Откроется окно для ввода пароля администратора.

9. Задайте новый пароль для учетной записи KLAdmin и подтвердите его.

10. Сохраните внесенные изменения.

Как сбросить пароль для учетной записи KLAdmin в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.

2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.

3. Выберите вкладку **Приложения**.

4. Нажмите на **Kaspersky Endpoint Security для Windows 14.2**.

   Откроются локальные параметры приложения.

5. Выберите вкладку **Параметры приложения**.

6. Перейдите в раздел **Общие настройки → Самозащита**.

7. В блоке **Защита паролем** выключите переключатель **Защита паролем**.

8. Сохраните внесенные изменения.

9. Повторно включите переключатель **Защита паролем**.

10. Задайте новый пароль для учетной записи KLAdmin и подтвердите его.

11. Сохраните внесенные изменения.

В результате пароль для учетной записи KLAdmin будет обновлен после применения политики.

Защита подключения к Серверу администрирования

Для подключения компьютера к Серверу администрирования предназначен компонент Kaspersky Security Center – *Агент администрирования*. Если злоумышленник обладает достаточными правами для изменения параметров подключения к серверу, есть риск переподключения компьютера к недоверенному серверу. Таким образом, злоумышленник может применить собственные групповые политики и, например, выключить самозащиту приложения. Kaspersky Endpoint Security позволяет предотвратить несанкционированное переподключение компьютера к другому серверу. Для защиты подключения к серверу приложение предлагает задать пароль и использовать стандарт формирования ключа на основе пароля (англ. Password-Based key Derivation Function, PBKDF2). В результате получить доступ к приложению без пароля невозможно.

Для комплексной защиты Kaspersky Endpoint Security и Агента администрирования от несанкционированного доступа рекомендуется включить дополнительную защиту. Для Kaspersky Endpoint Security рекомендуется включить Защиту паролем. Для защиты Агента администрирования рекомендуется установить пароль деинсталляции. Подробнее о защите Агента администрирования от удаления см. в справке Kaspersky Security Center.

Для управления подключением компьютера к Серверу администрирования предназначена задача *Защита подключения к Серверу администрирования*. Задача позволяет выполнять следующие действия:

- Задать пароль для защиты подключения к серверу.
- Сменить пароль.
- Переподключить компьютер к другому серверу.
- Выключить защиту подключения к серверу.

Аутентификация компьютера при подключении к Серверу администрирования

После установки пароля приложение создает массив данных с помощью PBKDF2-преобразования пароля. Далее приложение зашифровывает этот массив данных с помощью ключа Агента администрирования. На основании зашифрованного массива данных приложение осуществляет проверку прав и полномочий Сервера администрирования при следующих соединениях.

В дальнейшем при попытке переподключить компьютер к Серверу администрирования приложение расшифровывает массив данных с помощью ключа Агента администрирования и сравнивает его с локальной копией. Если они не совпадают, доступ к приложению ограничен.

Защита подключения к Серверу администрирования

Как установить пароль для защиты подключения компьютера к серверу в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Защита подключения к Серверу администрирования**.

Шаг 2. Защита подключения к Серверу администрирования

Установите пароль для защиты подключения к Серверу администрирования:

1. В блоке **Защита подключения к Серверу администрирования** выберите **Защищать паролем**.
2. В раскрывающемся списке **Сервер администрирования** выберите **Новый сервер**.
3. В поле **Пароль для подключения к Серверу администрирования** задайте пароль для подключения к Серверу администрирования и подтвердите его.

   Если вы забудете пароль, вы сможете сменить его с помощью задачи.
4. Если у вас развернуто приложение Kaspersky Endpoint Security версии 12.7 или более ранние версии приложения, установите флажок **Включить совместимость шифрования пароля для более ранних версий приложения (12.7 и ниже)**.

   Начиная с версии Kaspersky Endpoint Security для Windows 12.8 в приложении используется более сильное шифрование пароля. Если в вашей организации развернуто приложение Kaspersky Endpoint Security 12.8 и выше, рекомендуется снять флажок и использовать более сильное шифрование пароля. Более ранние версии приложения не поддерживает сильное шифрование пароля. Для выполнения задачи необходимо установить флажок.

Шаг 3. Выбор учетной записи для запуска задачи

Выберите **Учетная запись по умолчанию**. По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

Шаг 4. Настройка расписания запуска задачи

В блоке **Запуск по расписанию** выберите **Вручную**.

Шаг 5. Определение названия задачи

Введите название задачи, например, *Пароль для подключения к главному серверу*.

Шаг 6. Завершение создания задачи

Завершите работу мастера. Установите флажок **Запустить задачу после завершения работы мастера** или запустите задачу вручную. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как установить пароль для защиты подключения компьютера к серверу в Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Защита подключения к Серверу администрирования**.

   c. В поле **Название задачи** введите короткое описание, например, *Пароль для подключение к главному серверу*.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

5. Выберите учетную запись по умолчанию. По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера.

   В списке задач отобразится новая задача.

7. Нажмите на задачу Kaspersky Endpoint Security **Защита подключения к Серверу администрирования**.

   Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. В блоке **Защита подключения к Серверу администрирования** выберите **Защищать паролем**.

10. В раскрывающемся списке **Подключение к Серверу администрирования** выберите **Новый пароль**.

11. В поле **Пароль для подключения к Серверу администрирования** задайте пароль для подключения к Серверу администрирования и подтвердите его.

    Если вы забудете пароль, вы сможете сменить его с помощью задачи.

12. Если у вас развернуто приложение Kaspersky Endpoint Security версии 12.7 или более ранние версии приложения, установите флажок **Включить совместимость шифрования пароля для более ранних версий приложения (12.7 и ниже)**.

    Начиная с версии Kaspersky Endpoint Security для Windows 12.8 в приложении используется более сильное шифрование пароля. Если в вашей организации развернуто приложение Kaspersky Endpoint Security 12.8 и выше, рекомендуется снять флажок и использовать более сильное шифрование пароля. Более ранние версии приложения не поддерживает сильное шифрование пароля. Для выполнения задачи необходимо установить флажок.

13. Сохраните внесенные изменения.

14. Установите флажок напротив задачи.

15. Нажмите на кнопку **Запустить**.

Вы можете отслеживать статус задачи, количество устройств, на которых задача выполнена успешно или завершилась с ошибкой.

Переподключение компьютера к другому Серверу администрирования

Переподключение компьютера к другому Серверу администрирования состоит из следующих этапов:

1. В консоли текущего сервера `[KSC1]` нужно запустить задачу *Смена Сервера администрирования* для Агента администрирования.

   После выполнения задачи компьютер будет переподключен к новому серверу `[KSC2]`.

   Компьютер будет отображаться в консоли сервера `[KSC1]` со статусом *Критический*. Настроить параметры приложения с помощью политик или дистанционно запустить задачи на компьютере будет невозможно.

2. В консоли нового сервера `[KSC2]` нужно создать новую задачу *Защита подключения к Серверу администрирования* для Kaspersky Endpoint Security. В свойствах задачи вам нужно ввести пароль от прежнего сервера и задать пароль для нового сервера.

   Как установить новый пароль для переподключения к новому серверу в Консоли администрирования (MMC)

   1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

      Откроется список задач.

   2. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Защита подключения к Серверу администрирования**.

Шаг 2. Защита подключения к Серверу администрирования

Установите пароль для защиты подключения к новому Серверу администрирования:

1. В блоке **Защита подключения к Серверу администрирования** выберите **Защищать паролем**.

2. В раскрывающемся списке **Сервер администрирования** выберите **Переподключиться от другого сервера**.

3. В поле **Текущий пароль** введите пароль, установленный для подключения к прежнему доверенному серверу.

4. В поле **Новый пароль** задайте пароль для подключения к новому Серверу администрирования и подтвердите его.

   Если вы забудете пароль, вы сможете сменить его с помощью задачи.

5. Если у вас развернуто приложение Kaspersky Endpoint Security версии 12.7 или более ранние версии приложения, установите флажок **Включить совместимость шифрования пароля для более ранних версий приложения (12.7 и ниже)**.

   Начиная с версии Kaspersky Endpoint Security для Windows 12.8 в приложении используется более сильное шифрование пароля. Если в вашей организации развернуто приложение Kaspersky Endpoint Security 12.8 и выше, рекомендуется снять флажок и использовать более сильное шифрование пароля. Более ранние версии приложения не поддерживает сильное шифрование пароля. Для выполнения задачи необходимо установить флажок.

Шаг 3. Выбор учетной записи для запуска задачи

Выберите **Учетная запись по умолчанию**. По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

Шаг 4. Настройка расписания запуска задачи

В блоке **Запуск по расписанию** выберите **Вручную**.

Шаг 5. Определение названия задачи

Введите название задачи, например, *Пароль для подключения к главному серверу*.

Шаг 6. Завершение создания задачи

Завершите работу мастера. Установите флажок **Запустить задачу после завершения работы мастера** или запустите задачу вручную. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как установить новый пароль для переподключения к новому серверу в Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Защита подключения к Серверу администрирования**.

   c. В поле **Название задачи** введите короткое описание, например, *Пароль для подключение к главному серверу*.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

5. Выберите учетную запись по умолчанию. По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера.

   В списке задач отобразится новая задача.

7. Нажмите на задачу Kaspersky Endpoint Security **Защита подключения к Серверу администрирования**.

   Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. В блоке **Защита подключения к Серверу администрирования** выберите **Защищать паролем**.

10. В раскрывающемся списке **Подключение к Серверу администрирования** выберите **Переподключиться от другого сервера**.

11. В поле **Текущий пароль** введите пароль, установленный для подключения к прежнему доверенному серверу.

12. В поле **Новый пароль** задайте пароль для подключения к новому Серверу администрирования и подтвердите его.

    Если вы забудете пароль, вы сможете сменить его с помощью задачи.

13. Если у вас развернуто приложение Kaspersky Endpoint Security версии 12.7 или более ранние версии приложения, установите флажок **Включить совместимость шифрования пароля для более ранних версий приложения (12.7 и ниже)**.

    Начиная с версии Kaspersky Endpoint Security для Windows 12.8 в приложении используется более сильное шифрование пароля. Если в вашей организации развернуто приложение Kaspersky Endpoint Security 12.8 и выше, рекомендуется снять флажок и использовать более сильное шифрование пароля. Более ранние версии приложения не поддерживает сильное шифрование пароля. Для выполнения задачи необходимо установить флажок.

14. Сохраните внесенные изменения.

15. Установите флажок напротив задачи.

16. Нажмите на кнопку **Запустить**.

    Вы можете отслеживать статус задачи, количество устройств, на которых задача выполнена успешно или завершилась с ошибкой.

После выполнения задачи убедитесь, что компьютер в консоли нового сервера [KSC2] имеет статус *OK* . Проверьте дистанционный запуск задач и настройку параметров приложения с помощью политик.

Сброс пароля для подключения к Серверу администрирования

Если вы забыли пароль для подключения к Серверу администрирования или пароль раскрыт, вы можете сбросить пароль в свойствах задачи. Также вы можете сбросить пароль и задать новый пароль для группы компьютеров с разным статусом защиты подключения к Серверу администрирования. То есть, если для некоторых компьютеров защита включена, а для некоторых нет, после выполнения задачи пароль будет установлен для всех компьютеров.

Вы можете сбросить пароль для подключения к Серверу администрирования только в консоли доверенного сервера, к которому подключен компьютер.

Как сбросить пароль для подключения к Серверу администрирования в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Задачи**.
3. Выберите задачу **Защита подключения к Серверу администрирования** и откройте свойства задачи двойным щелчком мыши.
4. В окне свойств задачи выберите раздел **Настройки**.
5. В блоке **Защита подключения к Серверу администрирования** выберите **Защищать и сменить пароль**.
6. В поле **Пароль для подключения к Серверу администрирования** задайте новый пароль для подключения к текущему доверенному серверу и подтвердите его.
7. Сохраните внесенные изменения.
8. Запустите задачу.

Как сбросить пароль для подключения к Серверу администрирования в Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.
2. Нажмите на задачу Kaspersky Endpoint Security **Защита подключения к Серверу администрирования**.

   Откроется окно свойств задачи.
3. Выберите вкладку **Параметры приложения**.
4. В блоке **Защита подключения к Серверу администрирования** выберите **Защищать и сменить пароль**.
5. В поле **Пароль для подключения к Серверу администрирования** задайте новый пароль для подключения к текущему доверенному серверу и подтвердите его.
6. Сохраните внесенные изменения.

7. Установите флажок напротив задачи.

8. Нажмите на кнопку **Запустить**.

В результате пароль для подключения к Серверу администрирования будет обновлен после выполнения задачи.

Выключение защиты подключения к Серверу администрирования

Вы можете дистанционно выключить защиту подключения к Серверу администрирования только в консоли доверенного сервера, к которому подключен компьютер. Также вы можете выключить защиту локально через командную строку.

Как выключить защиту подключения компьютера к серверу в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите папку **Задачи**.

3. Выберите задачу **Защита подключения к Серверу администрирования** и откройте свойства задачи двойным щелчком мыши.

4. В окне свойств задачи выберите раздел **Настройки**.

5. В блоке **Защита подключения к Серверу администрирования** выберите **Не защищать**.

6. Сохраните внесенные изменения.

7. Запустите задачу.

   Вы можете отслеживать статус задачи, количество устройств, на которых задача выполнена успешно или завершилась с ошибкой.

Как выключить защиту подключения компьютера к серверу в Web Console и Cloud Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Защита подключения к Серверу администрирования**.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. В блоке **Защита подключения к Серверу администрирования** выберите **Не защищать паролем**.

5. Сохраните внесенные изменения.

6. Установите флажок напротив задачи.

7. Нажмите на кнопку **Запустить**.

   Вы можете отслеживать статус задачи, количество устройств, на которых задача выполнена успешно или завершилась с ошибкой.

Как выключить защиту подключения компьютера к серверу через командную строку

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Выполните команду:

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   где `<password>` – пароль учетной записи KLAdmin или пароль из задачи *Защита подключения к Серверу администрирования*. Если параметр не задан, Kaspersky Endpoint Security предложит ввести пароль в следующей строке.

   > Для выполнения команды должна быть включена Защита паролем.

Пример

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

Шифрование данных

Kaspersky Endpoint Security позволяет шифровать файлы и папки, хранящиеся на локальных дисках компьютера и съемных дисках, съемные и жесткие диски целиком. Шифрование данных снижает риски утечки информации в случае кражи / утери портативного компьютера, съемного диска или жесткого диска, а также при доступе посторонних пользователей и приложений к данным. Kaspersky Endpoint Security использует алгоритм шифрования Advanced Encryption Standard (AES).

Если срок действия лицензии истек, то приложение не шифрует новые данные, а старые зашифрованные данные остаются зашифрованными и доступными для работы. В этом случае для шифрования новых данных требуется активировать приложение по новой лицензии, которая допускает использование шифрования.

Если приложение Kaspersky Endpoint Security установлено на компьютере с Arm-архитектурой, то доступно только шифрование диска BitLocker. Приложение не поддерживает остальные компоненты шифрования данных.

В случае истечения срока действия лицензии, нарушения Лицензионного соглашения, удаления лицензионного ключа, удаления приложения Kaspersky Endpoint Security или компонентов шифрования с компьютера пользователя не гарантируется, что файлы, зашифрованные ранее, останутся зашифрованными. Это связано с тем, что некоторые приложения, например Microsoft Office Word, при редактировании файлов создают их временную копию, которой подменяют исходный файл при его сохранении. В результате при отсутствии или недоступности на компьютере функциональности шифрования файл остается незашифрованным.

Kaspersky Endpoint Security обеспечивает следующие направления защиты данных:

- **Шифрование файлов на локальных дисках компьютера**. Вы можете сформировать списки из файлов по расширению или группам расширений и из папок, расположенных на локальных дисках компьютера, а также создать правила шифрования файлов, создаваемых отдельными приложениями. После применения политики приложение Kaspersky Endpoint Security шифрует и расшифровывает следующие файлы:
  - файлы, отдельно добавленные в списки для шифрования и расшифровки;
  - файлы, хранящиеся в папках, добавленных в списки для шифрования и расшифровки;
  - файлы, создаваемые отдельными приложениями.
- **Шифрование съемных дисков**. Вы можете указать правило шифрования по умолчанию, в соответствии с которым приложение выполняет одинаковое действие по отношению ко всем съемным дискам, и указать правила шифрования отдельных съемных дисков.

  Правило шифрования по умолчанию имеет меньший приоритет, чем правила шифрования, созданные для отдельных съемных дисков. Правила шифрования, созданные для съемных дисков с указанной моделью устройства, имеют меньший приоритет, чем правила шифрования, созданные для съемных дисков с указанным идентификатором устройства.

Чтобы выбрать правило шифрования файлов на съемном диске, Kaspersky Endpoint Security проверяет, известны ли модель устройства и его идентификатор. Далее приложение выполняет одно из следующих действий:

- Если известна только модель устройства, приложение применяет правило шифрования, созданное для съемных дисков с данной моделью устройства, если такое правило есть.
- Если известен только идентификатор устройства, приложение применяет правило шифрования, созданное для съемных дисков с данным идентификатором устройства, если такое правило есть.
- Если известны и модель устройства, и идентификатор устройства, приложение применяет правило шифрования, созданное для съемных дисков с данным идентификатором устройства, если такое правило есть. Если такого правила нет, но есть правило шифрования, созданное для съемных дисков с данной моделью устройства, приложение применяет его. Если не заданы правила шифрования ни для данного идентификатора устройства, ни для данной модели устройства, приложение применяет правило шифрования по умолчанию.
- Если неизвестны ни модель устройства, ни идентификатор устройства, приложение применяет правило шифрования по умолчанию.

Приложение позволяет подготовить съемный диск для работы с зашифрованными на нем файлами в портативном режиме. После включения портативного режима становится доступной работа с зашифрованными файлами на съемных дисках, подключенных к компьютеру с недоступной функциональностью шифрования.

- **Управление правами доступа программ к зашифрованным файлам**. Для любого приложения вы можете создать правило доступа к зашифрованным файлам, запрещающее доступ к зашифрованным файлам или разрешающее доступ к зашифрованным файлам только в виде шифротекста – последовательности символов, полученной в результате применения шифрования.
- **Создание зашифрованных архивов**. Вы можете создавать зашифрованные архивы и защищать доступ к этим архивам паролем. Доступ к содержимому зашифрованных архивов можно получить только после ввода паролей, которыми вы защитили доступ к этим архивам. Такие архивы можно безопасно передавать по сети или на съемных дисках.
- **Полнодисковое шифрование**. Вы можете выбрать технологию шифрования: Шифрование диска Kaspersky или Шифрование диска BitLocker (далее также "BitLocker").

  BitLocker – технология, являющаяся частью операционной системы Windows. Если компьютер оснащен доверенным платформенным модулем (англ. Trusted Platform Module, TPM), BitLocker использует его для хранения ключей восстановления, позволяющих получить доступ к зашифрованному жесткому диску. При загрузке компьютера BitLocker запрашивает у доверенного платформенного модуля ключи восстановления жесткого диска и разблокирует его. Вы можете настроить использование пароля и / или PIN-кода для доступа к ключам восстановления.

  Вы можете указать правило полнодискового шифрования по умолчанию и сформировать список жестких дисков для исключения из шифрования. Kaspersky Endpoint Security выполняет полнодисковое шифрование по секторам после применения политики Kaspersky Security Center. Приложение шифрует сразу все логические разделы жестких дисков.

После шифрования системных жестких дисков при последующем включении компьютера доступ к ним, а также загрузка операционной системы возможны только после прохождения процедуры аутентификации с помощью Агента аутентификации. Для этого требуется ввести пароль токена или смарт-карты, подключенных к компьютеру, или имя и пароль учетной записи Агента аутентификации, созданной системным администратором локальной сети организации с помощью задачи *Управление учетными записями Агента аутентификации*. Эти учетные записи основаны на учетных записях пользователей Microsoft Windows, под которыми пользователи выполняют вход в операционную систему. Также вы можете использовать технологию единого входа (англ. Single Sign-On, SSO), позволяющую осуществлять автоматический вход в операционную систему с помощью имени и пароля учетной записи Агента аутентификации.

Если для компьютера была создана резервная копия, затем данные компьютера были зашифрованы, после чего была восстановлена резервная копия компьютера и данные компьютера снова были зашифрованы, Kaspersky Endpoint Security формирует дубликаты учетных записей Агента аутентификации. Для удаления дубликатов требуется использовать утилиту klmover с ключом `dupfix`. Утилита klmover поставляется со сборкой Kaspersky Security Center. Подробнее о ее работе вы можете прочитать в справке для Kaspersky Security Center.

Доступ к зашифрованным жестким дискам возможен только с компьютеров, на которых установлено приложение Kaspersky Endpoint Security с доступной функциональностью полнодискового шифрования. Это условие сводит к минимуму вероятность утечки информации, хранящейся на зашифрованном жестком диске, при использовании зашифрованного жесткого диска вне локальной сети организации.

Для шифрования жестких и съемных дисков вы можете использовать функцию шифрования только занятого пространства. Рекомендуется применять эту функцию только для новых, ранее не использовавшихся устройств. Если вы применяете шифрование на уже используемом устройстве, рекомендуется зашифровать все устройство. Это гарантирует защиту всех данных – даже удаленных, но еще содержащих извлекаемые сведения.

Перед началом шифрования Kaspersky Endpoint Security получает карту секторов файловой системы. В первом потоке шифруются секторы, занятые файлами на момент запуска шифрования. Во втором потоке шифруются секторы, в которые выполнялась запись после начала шифрования. После завершения шифрования все секторы, содержащие данные, оказываются зашифрованными.

Если после завершения шифрования пользователь удаляет файл, то секторы, в которых хранился этот файл, становятся свободными для дальнейшей записи информации на уровне файловой системы, но остаются зашифрованными. Таким образом, по мере записи файлов на новом устройстве при регулярном запуске шифрования с включенной функцией **Шифровать только занятое пространство** на компьютере через некоторое время будут зашифрованы все секторы.

Данные, необходимые для расшифровки объектов, предоставляет Сервер администрирования Kaspersky Security Center, под управлением которого находился компьютер в момент шифрования. Если по каким-либо причинам компьютер с зашифрованными объектами попал под управление другого Сервера администрирования, то получить доступ к зашифрованным данным возможно одним из следующих способов:

- Серверы администрирования в одной иерархии:
  - Вам не нужно предпринимать никаких дополнительных действий. У пользователя останется доступ к зашифрованным объектам. Ключи шифрования распространяются на все Серверы администрирования.

- Серверы администрирования разрознены:
  - Запросить доступ к зашифрованным объектам у администратора локальной сети организации.
  - Восстановить данные на зашифрованных устройствах с помощью утилиты восстановления.
  - Восстановить конфигурацию Сервера администрирования Kaspersky Security Center, под управлением которого находился компьютер в момент шифрования, из резервной копии и использовать эту конфигурацию на Сервере администрирования, под управлением которого оказался компьютер с зашифрованными объектами.

При отсутствии доступа к зашифрованным данным следуйте специальным инструкциям по работе с зашифрованными данными (Восстановление доступа к зашифрованным файлам, Работа с зашифрованными устройствами при отсутствии доступа к ним).

Ограничения функциональности шифрования

Шифрование данных имеет следующие ограничения:

- В процессе шифрования приложение создает служебные файлы. Для их хранения требуется около 0,5% нефрагментированного свободного пространства на жестком диске компьютера. Если нефрагментированного свободного пространства на жестком диске недостаточно, то шифрование не запускается до тех пор, пока не обеспечено это условие.
- Управление всеми компонентами шифрования данных доступно в Консоли администрирования Kaspersky Security Center и Kaspersky Security Center Web Console. В Kaspersky Security Center Cloud Console доступно только управление BitLocker.
- Шифрование данных доступно только при использовании Kaspersky Endpoint Security с системой администрирования Kaspersky Security Center или Kaspersky Security Center Cloud Console (только BitLocker). Шифрование данных при использовании Kaspersky Endpoint Security в автономном режиме невозможно, так как Kaspersky Endpoint Security хранит в Kaspersky Security Center ключи шифрования.
- Если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Microsoft Windows для серверов, то доступно только полнодисковое шифрование с помощью технологии Шифрование диска BitLocker. Если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций, то функциональность шифрования данных доступна в полном объеме.
- Если приложение Kaspersky Endpoint Security установлено на компьютере с Arm-архитектурой, то доступно только полнодисковое шифрование с помощью технологии Шифрование диска BitLocker, остальные компоненты шифрования данных не поддерживаются.

Функциональность полнодискового шифрования с помощью технологии Шифрование диска Kaspersky недоступна для жестких дисков, которые не отвечают аппаратным и программным требованиям.

Не поддерживается совместимость между функциональностью полнодискового шифрования Kaspersky Endpoint Security и Антивирусом Касперского для UEFI. Антивирус Касперского для UEFI запускается до загрузки операционной системы. При полнодисковом шифровании приложение обнаружит отсутствие установленной операционной системы на компьютере. В результате работа Антивируса Касперского для UEFI завершится с ошибкой. Шифрование файлов (FLE) не влияет на работу Антивируса Касперского для UEFI.

Kaspersky Endpoint Security поддерживает следующие конфигурации:

- HDD, SSD, USB-диски.

  Технология Шифрование диска Kaspersky (FDE) поддерживает работу с SSD-дисками с сохранением производительности и срока службы SSD-дисков.

- Диски, подключенные по шине: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.
- Несъемные диски, подключенные по шинам SD или MMC.
- Диски с размером сектора 512 байт.
- Диски с размером сектора 4096 байт, которые эмулируют 512 байт.
- Диски с типом партиций: GPT, MBR, VBR (съемные диски).
- Встроенное программное обеспечение стандарта UEFI 64 и Legacy BIOS.
- Встроенное программное обеспечение стандарта UEFI с поддержкой Secure Boot.

  Secure Boot – технология проверки цифровых подписей для UEFI приложений-загрузчиков и драйверов. Secure Boot запрещает запуск неподписанных или подписанных неизвестными издателями UEFI приложений и драйверов. Шифрование диска Kaspersky (FDE) полностью поддерживает Secure Boot. Агент аутентификации подписан сертификатом Microsoft Windows UEFI Driver Publisher.

  На некоторых устройствах (например, Microsoft Surface Pro и Microsoft Surface Pro 2) по умолчанию может быть установлен устаревший список сертификатов для проверки цифровых подписей. Перед шифрованием диска вам нужно обновить список сертификатов.

- Встроенное программное обеспечение стандарта UEFI с поддержкой Fast Boot.

  Fast Boot – технология, позволяющая ускорить загрузку компьютера. При включенной технологии Fast Boot обычно загружается только минимальный набор UEFI-драйверов, необходимый для запуска операционной системы. При включенной технологии Fast Boot при работе с Агентом аутентификации могут не работать USB-клавиатуры, мыши, USB-токены, тачпады или тачскрины.

  Для использования технологии Шифрование диска Kaspersky (FDE) рекомендуется выключить технологию Fast Boot. Вы можете проверить работу технологии Шифрование диска Kaspersky (FDE) с помощью FDE Test Utility.

Kaspersky Endpoint Security не поддерживает следующие конфигурации:

- Схема, при которой загрузчик расположен на одном диске, а операционная система – на другом.
- Встроенное программное обеспечение стандарта UEFI 32.
- Система с технологией Intel® Rapid Start Technology и диски с разделом гибернации (hibernation partition), даже при отключенном использовании Intel® Rapid Start Technology.
- Диски в формате MBR, имеющие более 10 расширенных разделов (extended partitions).
- Система, в которой есть файл подкачки, расположенный не на системном диске.
- Мультизагрузочная система с несколькими одновременно установленными операционными системами.

- Динамические разделы (поддерживаются только разделы основного типа).
- Диски, на которых менее 0,5% свободного нефрагментированного пространства.
- Диски с размером сектора, отличным от 512 байт или 4096 байт, которые эмулируют 512 байт.
- Гибридные диски.
- Система со сторонними загрузчиками.
- Диски со сжатыми NTFS-директориями.
- Технология Шифрование диска Kaspersky (FDE) несовместима с другими технологиями полнодискового шифрования (например, BitLocker, McAfee Drive Encryption, WinMagic SecureDoc).
- Технология Шифрование диска Kaspersky (FDE) несовместима с технологией ExpressCache.
- Создание, удаление и изменение разделов на зашифрованном диске не поддерживается. Вы можете потерять данные.
- Не поддерживается форматирование файловых систем. Вы можете потерять данные.

  Если необходимо отформатировать диск, зашифрованный технологией Шифрование диска Kaspersky (FDE), выполняйте форматирование диска на компьютере без Kaspersky Endpoint Security для Windows и используйте только полное форматирование.

  Зашифрованный диск, отформатированный с помощью быстрого форматирования, при следующем подключении к компьютеру с Kaspersky Endpoint Security для Windows может быть ошибочно распознан как зашифрованный. Пользовательские данные будут недоступны.
- Агент аутентификации поддерживает не более 100 учетных записей.
- Технология единого входа (Single Sign-On) несовместима с другими технологиями сторонних производителей.
- Технология Шифрование диска Kaspersky (FDE) не поддерживается на следующих моделях устройств:
  - Dell Latitude E6410 (UEFI mode);
  - HP Compaq nc8430 (Legacy BIOS mode);
  - Lenovo ThinkCentre 8811 (Legacy BIOS mode).
- Агент аутентификации не поддерживает работу с USB-токенами при включенной функции Legacy USB Support. На компьютере будет возможна аутентификация только по паролю.
- При шифровании диска в режиме Legacy BIOS рекомендуется включить функцию Legacy USB Support на следующих моделях устройств:
  - Acer Aspire 5560G;
  - Acer Aspire 6930;
  - Acer TravelMate 8572T;
  - Dell Inspiron 1420;

- Dell Inspiron 1545;
- Dell Inspiron 1750;
- Dell Inspiron N4110;
- Dell Latitude E4300;
- Dell Studio 1537;
- Dell Studio 1569;
- Dell Vostro 1310;
- Dell Vostro 1320;
- Dell Vostro 1510;
- Dell Vostro 1720;
- Dell Vostro V13;
- Dell XPS L502x;
- Fujitsu Celsius W370;
- Fujitsu LifeBook A555;
- HP Compaq dx2450 Microtower PC;
- Lenovo G550;
- Lenovo ThinkPad L530;
- Lenovo ThinkPad T510;
- Lenovo ThinkPad W540;
- Lenovo ThinkPad X121e;
- Lenovo ThinkPad X200s (74665YG);
- Samsung R530;
- Toshiba Satellite A350;
- Toshiba Satellite U400 10O;
- MSI 760GM-E51 (материнская плата).

Смена длины ключа шифрования (AES56 / AES256)

Kaspersky Endpoint Security использует алгоритм шифрования AES (Advanced Encryption Standard). Kaspersky Endpoint Security поддерживает алгоритм шифрования AES с эффективной длиной ключа 256 и 56 бит. Алгоритм шифрования данных зависит от библиотеки шифрования AES, входящей в состав дистрибутива: *Strong encryption (AES256)* или *Lite encryption (AES56)*. Библиотека шифрования AES устанавливается вместе с приложением.

Смена длины ключа шифрования доступна только для Kaspersky Endpoint Security 11.2.0 и выше.

Смена длины ключа шифрования состоит из следующих этапов:

1. Расшифруйте объекты, которые приложение Kaspersky Endpoint Security зашифровало до начала смены длины ключа шифрования:

   a. Расшифруйте жесткие диски.

   b. Расшифруйте файлы на локальных дисках.

   c. Расшифруйте съемные диски.

   После смены длины ключа шифрования объекты, зашифрованные ранее, становятся недоступны.

2. Удалите Kaspersky Endpoint Security.

3. Установите Kaspersky Endpoint Security из дистрибутива Kaspersky Endpoint Security с другой библиотекой шифрования.

Вы также можете сменить длину ключа шифрования через обновление приложения. Смена длины ключа через обновление приложения доступна при выполнении следующих условий:

- На компьютере установлено приложение Kaspersky Endpoint Security версии 10 Service Pack 2 и выше.
- На компьютере не установлены компоненты шифрования данных: Шифрование файлов, Полнодисковое шифрование.

  По умолчанию компоненты шифрования данных не включены в состав Kaspersky Endpoint Security. Компонент Управление BitLocker не влияет на смену длины ключа шифрования.

Для смены длины ключа шифрования запустите файл kes_win.msi или setup_kes.exe из дистрибутива с нужной библиотекой шифрования. Также вы можете обновить приложение дистанционно с помощью инсталляционного пакета.

Невозможно сменить длину ключа шифрования с помощью дистрибутива той же версии приложения, которое установлено на вашем компьютере, без предварительного удаления приложения.

Шифрование диска Kaspersky

Шифрование диска Kaspersky не поддерживается на компьютерах с Arm-архитектурой.

Технология Шифрование диска Kaspersky доступна только для компьютеров под управлением операционной системы Windows для рабочих станций. Для компьютеров под управлением операционной системы Windows для серверов используйте технологию Шифрование диска BitLocker.

Kaspersky Endpoint Security поддерживает полнодисковое шифрование в файловых системах FAT32, NTFS и exFat.

Перед запуском полнодискового шифрования приложение выполняет ряд проверок на возможность шифрования устройства, в том числе и проверку совместимости системного жесткого диска с Агентом аутентификации или с компонентами шифрования BitLocker. Для проверки совместимости требуется выполнить перезагрузку компьютера. После перезагрузки компьютера приложение в автоматическом режиме выполняет все необходимые проверки. Если проверка на совместимость проходит успешно, то после загрузки операционной системы и запуска приложения запускается полнодисковое шифрование. Если в процессе проверки обнаруживается несовместимость системного жесткого диска с Агентом аутентификации или с компонентами шифрования BitLocker, требуется перезагрузить компьютер с помощью аппаратной кнопки (Reset). Kaspersky Endpoint Security фиксирует информацию о несовместимости, на основе которой не запускает полнодисковое шифрование после старта операционной системы. В отчетах Kaspersky Security Center выводится информация об этом событии.

Если аппаратная конфигурация компьютера изменилась, то для проверки системного жесткого диска на совместимость с Агентом аутентификации и компонентами шифрования BitLocker требуется удалить информацию о несовместимости, полученную приложением при предыдущей проверке. Для этого перед полнодисковым шифрованием в командной строке требуется ввести команду `avp pbatestreset`. Если после проверки системного жесткого диска на совместимость с Агентом аутентификации операционная система не может запуститься, требуется удалить объекты и данные, оставшиеся после тестовой работы Агента аутентификации, с помощью утилиты восстановления, далее запустить Kaspersky Endpoint Security и выполнить команду `avp pbatestreset` повторно.

После запуска полнодисковое шифрование Kaspersky Endpoint Security шифрует все, что записывается на жесткие диски.

Если во время полнодискового шифрования пользователь выключает или перезагружает компьютер, то перед последующей загрузкой операционной системы загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет полнодисковое шифрование.

Если во время полнодискового шифрования операционная система переходит в режим гибернации (hibernation mode), то при выводе операционной системы из режима гибернации загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет полнодисковое шифрование.

Если во время полнодискового шифрования операционная система переходит в спящий режим (sleep mode), то при выводе операционной системы из спящего режима Kaspersky Endpoint Security возобновляет полнодисковое шифрование без загрузки Агента аутентификации.

Аутентификация пользователя в Агенте аутентификации может выполняться двумя способами:

- путем ввода имени и пароля учетной записи Агента аутентификации, созданной администратором локальной сети организации средствами Kaspersky Security Center;
- путем ввода пароля подключенного к компьютеру токена или смарт-карты.

  Использование токена или смарт-карты доступно, только если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES256. Если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES56, то в добавлении файла электронного сертификата в команду будет отказано.

Агент аутентификации поддерживает раскладки клавиатуры для следующих языков:

- Английский (Великобритания);
- Английский (США);
- Арабский (Алжир, Марокко, Тунис, раскладка AZERTY);
- Испанский (Латинская Америка);
- Итальянский;
- Немецкий (Германия и Австрия);
- Немецкий (Швейцария);
- Португальский (Бразилия, раскладка ABNT2);
- Русский (для 105-клавишных клавиатур IBM / Windows с раскладкой ЙЦУКЕН);
- Турецкий (раскладка QWERTY);
- Французский (Франция);
- Французский (Швейцария);
- Французский (Бельгия, раскладка AZERTY);
- Японский (для 106-клавишных клавиатур с раскладкой QWERTY).

Раскладка клавиатуры становится доступной в Агенте аутентификации, если она добавлена в настройках языка и региональных стандартов операционной системы и доступна на экране приветствия Microsoft Windows.

Если имя учетной записи Агента аутентификации содержит символы, которые невозможно ввести с помощью доступных в Агенте аутентификации раскладок клавиатуры, то доступ к зашифрованным жестким дискам возможен только после их восстановления с помощью утилиты восстановления или после восстановления имени и пароля учетной записи Агента аутентификации.

Особенности шифрования SSD-дисков

Приложение поддерживает шифрование SSD-дисков, гибридных SSHD-дисков и дисков с функцией Intel Smart Response. Приложение не поддерживает шифрование дисков с функцией Intel Rapid Start. Перед шифрованием диска выключите функцию Intel Rapid Start.

Шифрование SSD-дисков имеет следующие особенности:

- Если SSD-диск новый и на нем нет конфиденциальных данных, включите функцию шифрования только занятого пространства. Это позволит перезаписать необходимые секторы диска.
- Если SSD-диск используется и на нем хранятся конфиденциальные данные, выберите один из вариантов:
  - Выполните полную очистку SSD-диска (Secure Erase), установите операционную систему и запустите шифрование SSD-диска с включенной функцией шифрования только занятого пространства.
  - Запустите шифрование SSD-диска с выключенной функцией шифрования только занятого пространства.

Для запуска шифрования SSD-диска требуется 5-10 ГБ свободного пространства. Требования к свободному пространству для хранения служебных данных шифрования представлены в таблице ниже.

Требования к свободному пространству для хранения служебных данных шифрования

Объем SSD-диска (ГБ)	Объем свободного пространства на первичном разделе SSD-диска (МБ)	Объем свободного пространства на вторичном разделе SSD-диска (МБ)
128	250	64
256	250	640
512	300	128

Запуск шифрования диска Kaspersky

Перед запуском полнодискового шифрования рекомендуется убедиться в том, что компьютер не заражен. Для этого запустите полную проверку или проверку важных областей компьютера. Выполнение полнодискового шифрования на компьютере, зараженном руткитом, может привести к неработоспособности компьютера.

Перед запуском шифрования диска вам нужно проверить параметры учетных записей Агента аутентификации. Агент аутентификации нужен для работы с дисками, которые защищены с помощью технологии Шифрование диска Kaspersky (FDE). Перед загрузкой операционной системы пользователю нужно пройти аутентификацию с помощью агента. Kaspersky Endpoint Security позволяет автоматически создавать учетные записи Агента аутентификации перед шифрованием диска. Вы можете включить автоматическое создание учетных записей Агента аутентификации в параметрах политики полнодискового шифрования (см. инструкцию ниже). Также вы можете использовать технологию единого входа (SSO).

Kaspersky Endpoint Security позволяет автоматически создавать учетные записи Агента аутентификации для следующих групп пользователей:

- **Все учетные записи компьютера**. Все учетные записи компьютера, которые когда-либо были активными.
- **Все доменные учетные записи компьютера**. Все учетные записи компьютера, которые принадлежат какому-либо домену и которые когда-либо были активными.
- **Все локальные учетные записи компьютера**. Все локальные учетные записи компьютера, которые когда-либо были активными.
- **Служебная учетная запись с одноразовым паролем**. Служебная учетная запись нужна для доступа к компьютеру в случаях, когда пользователь, например, забыл пароль. Также вы можете использовать служебную учетную запись в качестве резервной учетной записи. Вам нужно указать имя учетной записи (по умолчанию `ServiceAccount`). Kaspersky Endpoint Security создаст пароль автоматически. Пароль вы можете посмотреть в консоли Kaspersky Security Center.
- **Локальный администратор**. Kaspersky Endpoint Security создает учетную запись Агента аутентификации для локального администратора компьютера.
- **Менеджер компьютера**. Kaspersky Endpoint Security создает учетную запись Агента аутентификации для учетной записи менеджера компьютера. Вы можете посмотреть какая учетная запись имеет роль менеджера компьютера в свойствах компьютера в Active Directory. По умолчанию роль менеджера компьютера не определена, то есть не соответствует ни одной учетной записи.
- **Активная учетная запись**. Kaspersky Endpoint Security автоматически создает учетную запись Агента аутентификации для учетной записи активной в момент выполнения шифрования диска.

Для настройки параметров аутентификации пользователей предназначена задача *Управление учетными записями Агента аутентификации*. С помощью задачи вы можете добавлять новые учетные записи, изменять параметры текущих учетных записей или удалять учетные записи, если требуется. Вы можете использовать как локальные задачи для отдельных компьютеров, так и групповые задачи для компьютеров из отдельных групп администрирования или выборки компьютеров.

Как запустить шифрование диска Kaspersky через Консоль администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных → Полнодисковое шифрование**.
4. В раскрывающемся списке **Технология шифрования** выберите элемент **Шифрование диска Kaspersky**.

   Применение технологии шифрования Шифрование диска Kaspersky невозможно, если на компьютере есть жесткие диски, зашифрованные с помощью BitLocker.

5. В раскрывающемся списке **Режим шифрования** выберите элемент **Шифровать все жесткие диски**.

   Если на компьютере установлено несколько операционных систем, то после шифрования всех жестких дисков вы сможете выполнить загрузку только той операционной системы, в которой установлено приложение.

Если некоторые жесткие диски нужно исключить из шифрования, сформируйте их список.

6. Настройте дополнительные параметры шифрования диска Kaspersky (см. таблицу ниже).
7. Сохраните внесенные изменения.

Как запустить шифрование диска Kaspersky через Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

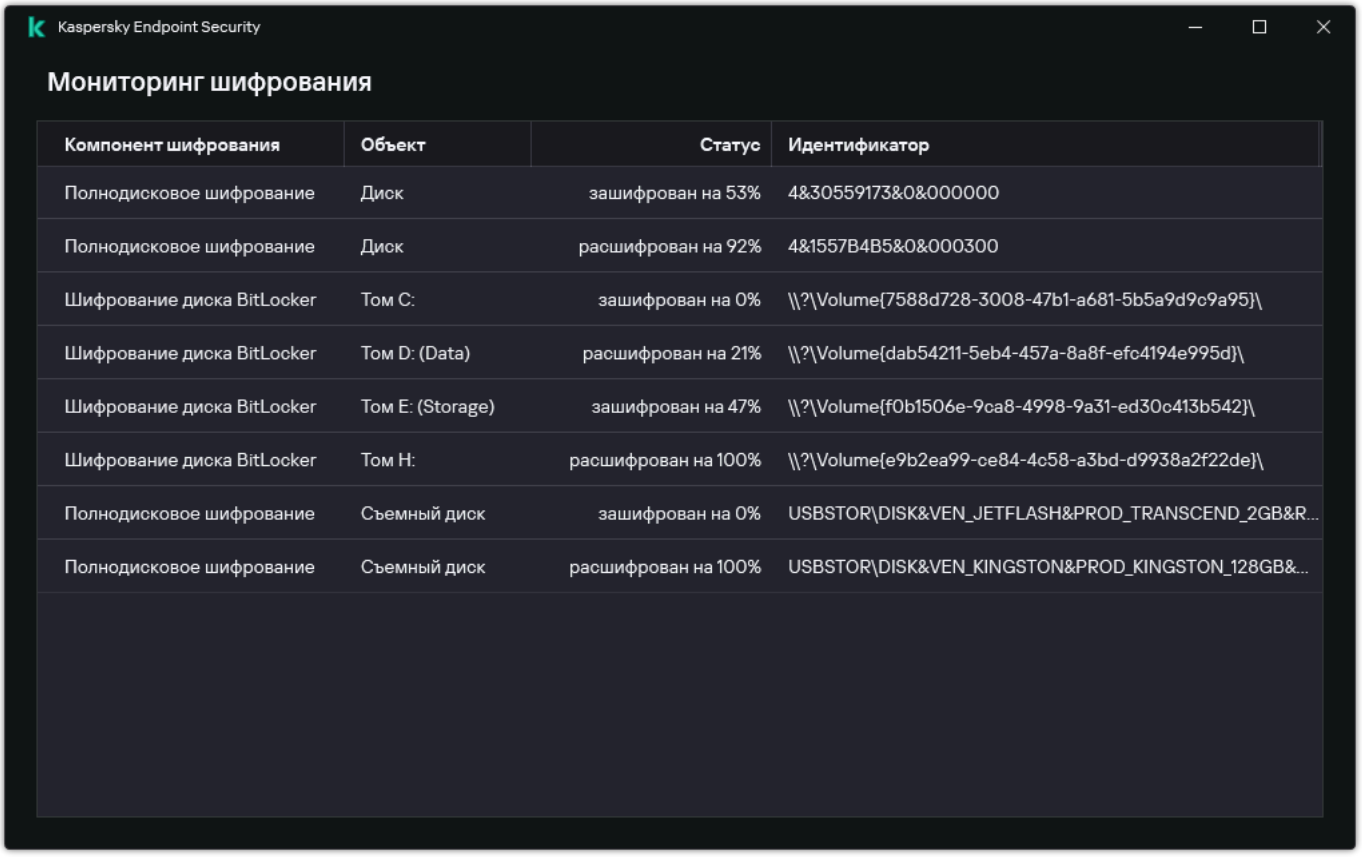
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Шифрование данных** → **Полнодисковое шифрование**.
5. Выберите технологию **Шифрование диска Kaspersky**.

   Применение технологии шифрования Шифрование диска Kaspersky невозможно, если на компьютере есть жесткие диски, зашифрованные с помощью BitLocker.
6. В блоке **Действие с устройствами** выберите элемент **Шифровать все жесткие диски**.

   Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой выполнялось шифрование.

   Если некоторые жесткие диски нужно исключить из шифрования, сформируйте их список.
7. Настройте дополнительные параметры шифрования диска Kaspersky (см. таблицу ниже).
8. Сохраните внесенные изменения.

Вы можете контролировать процесс шифрования или расшифровки диска на компьютере пользователя с помощью инструмента Мониторинг шифрования. Вы можете запустить инструмент Мониторинг шифрования из главного окна приложения.



Мониторинг шифрования

Если системные жесткие диски зашифрованы, перед загрузкой операционной системы загружается Агент аутентификации. С помощью Агента аутентификации требуется пройти процедуру аутентификации для получения доступа к зашифрованным системным жестким дискам и загрузки операционной системы. После успешного прохождения процедуры аутентификации загружается операционная система. При последующих перезагрузках операционной системы требуется повторно проходить процедуру аутентификации.

Параметры компонента Шифрование диска Kaspersky

Параметр	Описание
Автоматически создавать учетные записи Агента аутентификации для пользователей при применении шифрования на компьютере	Если флажок установлен, приложение создает учетные записи Агента аутентификации на основе списков учетных записей Windows на компьютере. По умолчанию Kaspersky Endpoint Security использует все локальные и доменные учетные записи, с помощью которых пользователь выполнял вход в операционную систему за последние 30 дней.
Автоматически создавать учетные записи Агента аутентификации для всех пользователей на компьютере при входе	Если флажок установлен, приложение проверяет информацию об учетных записях Windows на компьютере перед запуском Агента аутентификации. Если Kaspersky Endpoint Security обнаружит учетную запись Windows, для которой нет учетной записи Агента аутентификации, приложение создаст новую учетную запись для доступа к зашифрованным дискам. Новая учетная запись Агента аутентификации будет иметь параметры по умолчанию: вход только по паролю, смена пароля при первой аутентификации. Таким образом, вам не нужно вручную добавлять учетные записи Агента аутентификации с помощью задачи *Управление учетными записями Агента аутентификации* для компьютеров с уже зашифрованными дисками.
Сохранять введенное в Агенте аутентификации имя пользователя	Если флажок установлен, то приложение сохраняет имя учетной записи Агента аутентификации. При последующей аутентификации в Агенте аутентификации под той же учетной записью имя учетной записи вводить не требуется.

Параметр	Описание
Шифровать только занятое пространство (сокращает время шифрования)	Флажок включает / выключает функцию, ограничивающую область шифрования только занятыми секторами жесткого диска. Это ограничение позволяет сократить время шифрования. Включение / выключение функции **Шифровать только занятое пространство (сокращает время шифрования)** после запуска шифрования не изменяет этого параметра до тех пор, пока жесткие диски не будут расшифрованы. Требуется установить или снять флажок до начала шифрования. Если флажок установлен, то шифруется только та часть жесткого диска, которая занята файлами. Kaspersky Endpoint Security зашифровывает новые данные автоматически по мере их добавления. Если флажок снят, то шифруется весь жесткий диск, в том числе остатки удаленных и отредактированных ранее файлов. Данную функцию рекомендуется применять для новых жестких дисков, данные которых не редактировались и не удалялись. Если вы применяете шифрование на уже используемом жестком диске, рекомендуется зашифровать весь жесткий диск. Это гарантирует защиту всех данных – даже удаленных, но потенциально восстанавливаемых. По умолчанию флажок снят.
Использовать Legacy USB Support (не рекомендуется)	Флажок включает / выключает функцию Legacy USB Support. *Legacy USB Support* – функция BIOS / UEFI, которая позволяет использовать USB-устройства (например, токен) на этапе загрузки компьютера до запуска операционной системы (BIOS-режим). Функция Legacy USB Support не влияет на поддержку USB-устройств после запуска операционной системы. Если флажок установлен, то будет включена поддержка USB-устройств на этапе начальной загрузки компьютера. При включенной функции Legacy USB Support Агент аутентификации в BIOS-режиме не поддерживает работу с токенами по USB. Функцию рекомендуется использовать только при возникновении проблемы несовместимости с аппаратным обеспечением и только для тех компьютеров, на которых возникла проблема.

Формирование списка жестких дисков для исключения из шифрования

Вы можете сформировать список исключений из шифрования только для технологии Шифрование диска Kaspersky.

Чтобы сформировать список жестких дисков для исключения из шифрования, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных → Полнодисковое шифрование**.
4. В раскрывающемся списке **Технология шифрования** выберите вариант **Шифрование диска Kaspersky**.

   В таблице **Не шифровать следующие жесткие диски** отобразятся записи о жестких дисках, которые приложение не будет шифровать. Если вы ранее не сформировали список жестких дисков для исключения из шифрования, эта таблица пуста.

5. Если вы хотите добавить жесткие диски в список жестких дисков, которые приложение не будет шифровать, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне укажите значения параметров **Название**, **Компьютер**, **Тип диска**, **Шифрование диска Kaspersky**.

   c. Нажмите на кнопку **Обновить**.

   d. В графе **Название** установите флажки в строках таблицы, соответствующих тем жестким дискам, которые вы хотите добавить в список жестких дисков для исключения из шифрования.

   e. Нажмите на кнопку **OK**.

   Выбранные жесткие диски отобразятся в таблице **Не шифровать следующие жесткие диски**.

6. Сохраните внесенные изменения.

Экспорт и импорт списка жестких дисков для исключения из шифрования

Вы можете экспортировать список исключений жестких дисков из шифрования в файл в формате XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных исключений. Также вы можете использовать функцию экспорта / импорта для резервного копирования списка исключений или для миграции исключений на другой сервер.

Как экспортировать / импортировать список исключений жестких дисков из шифрования в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Шифрование данных** → **Полнодисковое шифрование**.

4. В раскрывающемся списке **Технология шифрования** выберите вариант **Шифрование диска Kaspersky**.

   В таблице **Не шифровать следующие жесткие диски** отобразятся записи о жестких дисках, которые приложение не будет шифровать.

5. Для экспорта списка исключений, выполните следующие действия:

   a. Выберите исключения, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

      Если вы не выбрали ни одного исключения, Kaspersky Endpoint Security экспортирует все исключения.

   b. Нажмите на кнопку → **Экспортировать**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список исключений, а также выберите папку, в которой вы хотите сохранить этот файл.

d. Сохраните файл.

Kaspersky Endpoint Security экспортирует список исключений в XML-файл.

6. Для импорта списка исключений, выполните следующие действия:

a. Нажмите на кнопку → **Импортировать**.

b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

c. Откройте файл.

Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

7. Сохраните внесенные изменения.

Как экспортировать / импортировать список исключений жестких дисков из шифрования в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Шифрование данных** → **Полнодисковое шифрование**.

Выберите технологию **Шифрование диска Kaspersky**.

5. Перейдите по ссылке **Исключения**.

Откроется список исключений.

6. Для экспорта списка исключений выполните следующие действия:

a. Выберите исключения, которые вы хотите экспортировать.

b. Нажмите на кнопку → **Экспортировать**.

Kaspersky Endpoint Security экспортирует список исключений в JSON-файл в папку для загрузки по умолчанию.

7. Для импорта списка исключений выполните следующие действия:

a. Нажмите на кнопку → **Импортировать**.

В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать список исключений.

b. Откройте файл.

Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из JSON-файла.

8. Сохраните внесенные изменения.

Включение использования технологии единого входа (SSO)

Технология единого входа (англ. Single Sign-On, SSO) позволяет выполнить автоматический вход в операционную систему с помощью учетных данных Агента аутентификации. Таким образом, при входе в Windows пользователю нужно ввести пароль только один раз (пароль учетной записи Агента аутентификации). Также технология единого входа позволяет автоматически обновлять пароль учетной записи Агента аутентификации при смене пароля учетной записи Windows.

При использовании технологии единого входа Агент аутентификации игнорирует требования к надежности пароля, заданные в Kaspersky Security Center. Вы можете задать требования к надежности пароля в параметрах операционной системы.

Включение использования технологии единого входа

Как включить использование технологии единого входа в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных → Общие настройки шифрования**.
4. В блоке **Настройки паролей** нажмите на кнопку **Настройка**.
5. В открывшемся окне на вкладке **Агент аутентификации** установите флажок **Использовать технологию единого входа (SSO)**.
6. Если вы используете стороннего поставщика учетных данных, установите флажок **Включить поддержку сторонних поставщиков учетных данных**.
7. Сохраните внесенные изменения.

В результате пользователю нужно пройти процедуру аутентификации только один раз с помощью агента. Проходить процедуру аутентификации для загрузки операционной системы не требуется. Операционная система загружается автоматически.

Как включить использование технологии единого входа в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Шифрование данных → Полнодисковое шифрование**.
5. Выберите технологию **Шифрование диска Kaspersky**.
6. В блоке **Настройки паролей** установите флажок **Использовать технологию единого входа (SSO)**.

7. Если вы используете стороннего поставщика учетных данных, установите флажок **Включить поддержку сторонних поставщиков учетных данных**.

8. Сохраните внесенные изменения.

В результате пользователю нужно пройти процедуру аутентификации только один раз с помощью агента. Проходить процедуру аутентификации для загрузки операционной системы не требуется. Операционная система загружается автоматически.

Для работы технологии единого входа пароль учетной записи Windows и пароль учетной записи Агента аутентификации должны совпадать. Если пароли не совпадают, то пользователю нужно выполнить процедуру аутентификации дважды: в интерфейсе Агента аутентификации и перед загрузкой операционной системы. Эти действия нужно выполнить только один раз, чтобы синхронизировать пароли. После этого Kaspersky Endpoint Security заменит пароль учетной записи Агента аутентификации на пароль учетной записи Windows. При смене пароля учетной записи Windows приложение будет автоматически обновлять пароль для учетной записи Агента аутентификации.

Сторонние поставщики учетных данных

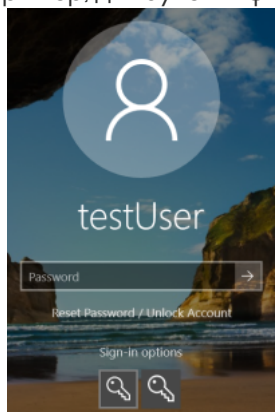
Kaspersky Endpoint Security поддерживает стороннего поставщика учетных данных ADSelfService Plus.

При работе со сторонними поставщиками учетных данных Агент аутентификации перехватывает пароль перед загрузкой операционной системы. Таким образом, при входе в Windows пользователю нужно ввести пароль только один раз. После входа в Windows пользователь может использовать возможности стороннего поставщика учетных данных, например, для аутентификации в сервисах организации. Также сторонние поставщики учетных данных позволяют пользователям самостоятельно сбрасывать пароль. В этом случае Kaspersky Endpoint Security обновит пароль для Агента аутентификации автоматически.

Если вы используете стороннего поставщика учетных данных, который не поддерживается приложением, вы можете столкнуться с ограничениями в работе технологии единого входа. При входе в Windows пользователю будут доступны два профиля: системный поставщик учетных данных и сторонний поставщик учетных данных. При этом иконки профилей будут одинаковые (см. рис. ниже). В результате возможны следующие варианты продолжения работы:

- Если пользователь выбирает *стороннего поставщика учетных данных*, Агент аутентификации не может синхронизировать пароль с учетной записью Windows. Таким образом, если пользователь сменил пароль учетной записи Windows, Kaspersky Endpoint Security не может обновить пароль для учетной записи Агента аутентификации. В результате пользователю нужно выполнять процедуру аутентификации дважды: в интерфейсе Агента аутентификации и перед загрузкой операционной системы. При этом пользователь может использовать возможности стороннего поставщика учетных данных, например, для аутентификации в сервисах организации.

- Если пользователь выбирает *системного поставщика учетных данных*, Агент аутентификации синхронизирует пароли с учетной записью Windows. При этом пользователь не может использовать возможности стороннего поставщика, например, для аутентификации в сервисах организации.



Системный и сторонний профили аутентификации при входе в Windows

Управление учетными записями Агента аутентификации

Агент аутентификации нужен для работы с дисками, которые защищены с помощью технологии Шифрование диска Kaspersky (FDE). Перед загрузкой операционной системы пользователю нужно пройти аутентификацию с помощью агента. Для настройки параметров аутентификации пользователей предназначена задача *Управление учетными записями Агента аутентификации*. Вы можете использовать как локальные задачи для отдельных компьютеров, так и групповые задачи для компьютеров из отдельных групп администрирования или выборки компьютеров.

Настроить расписание запуска задачи *Управление учетными записями Агента аутентификации* невозможно. Также невозможно принудительно остановить выполнение задачи.

Как создать задачу Управление учетными записями Агента аутентификации в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Управление учетными записями Агента аутентификации**.

Шаг 2. Выбор команды управления учетными записями Агента аутентификации

Сформируйте список команд управления учетными записями Агента аутентификации. Команды управления позволяют добавлять, изменять и удалять учетные записи Агента аутентификации (см. инструкции ниже). Только пользователи, которые имеют учетную запись Агента аутентификации, могут пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Определение названия задачи

Введите название задачи, например, *Учетные записи администраторов*.

Шаг 5. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

В результате после выполнения задачи при следующей загрузке компьютера новый пользователь может пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Как создать задачу Управление учетными записями Агента аутентификации в Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.
2. В раскрывающемся списке **Тип задачи** выберите **Управление учетными записями Агента аутентификации**.
3. В поле **Название задачи** введите короткое описание, например, *Учетные записи администраторов*.
4. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Управление учетными записями Агента аутентификации

Сформируйте список команд управления учетными записями Агента аутентификации. Команды управления позволяют добавлять, изменять и удалять учетные записи Агента аутентификации (см. инструкции ниже). Только пользователи, которые имеют учетную запись Агента аутентификации, могут пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Шаг 3. Завершение создание задачи

Завершите работу мастера. В списке задач отобразится новая задача.

Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку **Запустить**.

В результате после выполнения задачи при следующей загрузке компьютера новый пользователь может пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Для добавления учетной записи Агента аутентификации нужно добавить специальную команду в задачу *Управление учетными записями Агента аутентификации*. Групповую задачу удобно использовать, например, для добавления учетной записи администратора на все компьютеры.

Kaspersky Endpoint Security позволяет автоматически создавать учетные записи Агента аутентификации перед шифрованием диска. Вы можете включить автоматическое создание учетных записей Агента аутентификации в параметрах политики полнодискового шифрования. Также вы можете использовать технологию единого входа (SSO).

Как добавить учетную запись Агента аутентификации через Консоль администрирования (MMC)

1. Откройте свойства задачи *Управление учетными записями Агента аутентификации*.
2. В свойствах задачи выберите раздел **Настройки**.
3. Нажмите на кнопку **Добавить** → **Команду для добавления учетной записи**.
4. В открывшемся окне в поле **Учетная запись Windows** укажите имя учетной записи Microsoft Windows, на основе которой будет создана учетная запись Агента аутентификации.
5. Если вы ввели имя учетной записи Windows вручную, нажмите на кнопку **Разрешить**, чтобы определить идентификатор безопасности учетной записи (англ. Security Identifier, SID).

   Если вы не определяете идентификатор безопасности по кнопке **Разрешить**, то он будет определен в момент выполнения задачи на компьютере.

   > Определение идентификатора безопасности учетной записи Windows нужно для проверки корректности ввода имени учетной записи Windows. Если учетная запись Windows не существует на компьютере или в доверенном домене, задача *Управление учетными записями Агента аутентификации* будет завершена с ошибкой.

6. Установите флажок **Заменить существующую учетную запись**, если вы хотите, чтобы уже заведенная для Агента аутентификации учетная запись с таким же именем была заменена на добавляемую.

   > Этот шаг доступен, если вы добавляете команду для создания учетной записи Агента аутентификации в свойствах групповой задачи управления учетными записями Агента аутентификации. Этот шаг недоступен, если вы добавляете команду для создания учетной записи Агента аутентификации в свойствах локальной задачи *Управление учетными записями Агента аутентификации*.

7. В поле **Имя пользователя** введите имя учетной записи Агента аутентификации, которое требуется вводить при аутентификации для доступа к зашифрованным жестким дискам.
8. Установите флажок **Разрешать вход по паролю**, если вы хотите, чтобы при аутентификации для получения доступа к зашифрованным жестким дискам приложение требовало пароль учетной записи Агента аутентификации. Задайте пароль учетной записи Агента аутентификации. Если нужно, вы можете запросить у пользователя новый пароль после первой аутентификации.
9. Установите флажок **Разрешать вход по сертификату**, если вы хотите, чтобы при аутентификации для доступа к зашифрованным жестким дискам приложение требовало подключения токена или смарт-карты к компьютеру. Выберите файл сертификата для аутентификации с помощью смарт-карты или токена.
10. Если требуется, в поле **Описание команды** введите информацию об учетной записи Агента аутентификации, необходимую вам для работы с командой.
11. В блоке **Доступ к аутентификации в Агенте аутентификации** настройте доступ к аутентификации в Агенте аутентификации пользователю, работающему под учетной записью, указанной в команде.
12. Сохраните внесенные изменения.

Как добавить учетную запись Агента аутентификации через Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Управление учетными записями Агента аутентификации**.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. В списке учетных записей Агента аутентификации нажмите на кнопку **Добавить** и выберите тип команды **Добавление учетной записи**.

5. Выберите учетную запись пользователя. Вы можете выбрать учетную запись из списка доменных учетных записей или ввести имя учетной записи вручную. Перейдите к следующему шагу.

   Kaspersky Endpoint Security определяет идентификатор безопасности учетной записи (англ. Security Identifier, SID). Это нужно для проверки учетной записи. Если вы ввели имя пользователя неверно, Kaspersky Endpoint Security завершит выполнение задачи с ошибкой.

6. Настройте параметры учетной записи Агента аутентификации:

   - **Создать новую учетную запись Агента аутентификации взамен существующей**. Kaspersky Endpoint Security проверяет существующие учетные записи на компьютере. Если идентификатор безопасности пользователя на компьютере и в задаче совпадают, то Kaspersky Endpoint Security изменит параметры учетной записи в соответствии с задачей.

   - **Имя пользователя**. По умолчанию имя пользователя учетной записи Агента аутентификации соответствует доменному имени пользователя.

   - **Разрешать вход по паролю**. Задайте пароль учетной записи Агента аутентификации. Если нужно, вы можете запросить у пользователя новый пароль после первой аутентификации. Таким образом, у каждого пользователя будет свой уникальный пароль. Также вы можете задать требования к надежности пароля для учетной записи Агента аутентификации в политике.

   - **Разрешать вход по сертификату**. Выберите файл сертификата для аутентификации с помощью смарт-карты или токена. Таким образом, пользователю нужно будет ввести пароль от смарт-карты или токена.

   - **Доступ учетной записи к зашифрованным данным**. Настройте доступ пользователя к зашифрованному диску. Вы можете, например, временно запретить аутентификацию пользователя и не удалять учетную запись Агента аутентификации.

   - **Комментарий**. Введите описание учетной записи, если требуется.

7. Сохраните внесенные изменения.

8. Установите флажок напротив задачи и нажмите на кнопку **Запустить**.

   В результате после выполнения задачи при следующей загрузке компьютера новый пользователь может пройти процедуру аутентификации, загрузить операционную систему и получить доступ к зашифрованному диску.

Для изменения пароля и других параметров учетной записи Агента аутентификации нужно добавить специальную команду в задачу *Управление учетными записями Агента аутентификации*. Групповую задачу удобно использовать, например, для замены сертификата токена администратора на всех компьютерах.

Как изменить учетную запись Агента аутентификации через Консоль администрирования (MMC)

1. Откройте свойства задачи *Управление учетными записями Агента аутентификации*.
2. В свойствах задачи выберите раздел **Настройки**.
3. Нажмите на кнопку **Добавить** → **Команду для изменения учетной записи**.
4. В открывшемся окне в поле **Учетная запись Windows** укажите имя учетной записи пользователя Microsoft Windows, которую вы хотите изменить.
5. Если вы ввели имя учетной записи Windows вручную, нажмите на кнопку **Разрешить**, чтобы определить идентификатор безопасности учетной записи (англ. Security Identifier, SID).

   Если вы не определяете идентификатор безопасности по кнопке **Разрешить**, то он будет определен в момент выполнения задачи на компьютере.

   > Определение идентификатора безопасности учетной записи Windows нужно для проверки корректности ввода имени учетной записи Windows. Если учетная запись Windows не существует на компьютере или в доверенном домене, задача *Управление учетными записями Агента аутентификации* будет завершена с ошибкой.

6. Установите флажок **Изменить имя пользователя** и введите новое имя учетной записи Агента аутентификации, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, приложение Kaspersky Endpoint Security изменило имя пользователя на указанное в поле ниже.
7. Установите флажок **Изменить настройки входа по паролю**, если вы хотите сделать доступными для изменения параметры входа по паролю.
8. Установите флажок **Разрешать вход по паролю**, если вы хотите, чтобы при аутентификации для получения доступа к зашифрованным жестким дискам приложение требовало пароль учетной записи Агента аутентификации. Задайте пароль учетной записи Агента аутентификации.
9. Установите флажок **Изменить правило смены пароля при аутентификации в Агенте аутентификации**, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, приложение Kaspersky Endpoint Security изменило значение параметра смены пароля на установленное ниже.
10. Установите значение параметра смены пароля при аутентификации в Агенте аутентификации.
11. Установите флажок **Изменить настройки входа по сертификату**, если вы хотите сделать доступными для изменения параметры входа по электронному сертификату токена или смарт-карте.
12. Установите флажок **Разрешать вход по сертификату**, если вы хотите, чтобы при аутентификации для доступа к зашифрованным жестким дискам приложение требовало ввод пароля к подключенному к компьютеру токену или смарт-карте. Выберите файл сертификата для аутентификации с помощью смарт-карты или токена.
13. Установите флажок **Изменить описание команды** и измените описание команды, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, приложение Kaspersky Endpoint Security изменило описание команды.

14. Установите флажок **Изменить правило доступа к аутентификации в Агенте аутентификации**, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, программа Kaspersky Endpoint Security изменила правило доступа пользователя к аутентификации в Агенте аутентификации на установленное ниже.

15. Установите правило доступа к аутентификации в Агенте аутентификации.

16. Сохраните внесенные изменения.

Как изменить учетную запись Агента аутентификации через Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Управление учетными записями Агента аутентификации**.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. В списке учетных записей Агента аутентификации нажмите на кнопку **Добавить** и выберите тип команды **Изменение учетной записи**.

5. Выберите учетную запись пользователя. Вы можете выбрать учетную запись из списка доменных учетных записей или ввести имя учетной записи вручную. Перейдите к следующему шагу.

   Kaspersky Endpoint Security определяет идентификатор безопасности учетной записи (англ. Security Identifier, SID). Это нужно для проверки учетной записи. Если вы ввели имя пользователя неверно, Kaspersky Endpoint Security завершит выполнение задачи с ошибкой.

6. Установите флажки напротив тех параметров, которые вы хотите изменить.

7. Настройте параметры учетной записи Агента аутентификации:

   - **Создать новую учетную запись Агента аутентификации взамен существующей**. Kaspersky Endpoint Security проверяет существующие учетные записи на компьютере. Если идентификатор безопасности пользователя на компьютере и в задаче совпадают, то Kaspersky Endpoint Security изменит параметры учетной записи в соответствии с задачей.

   - **Имя пользователя**. По умолчанию имя пользователя учетной записи Агента аутентификации соответствует доменному имени пользователя.

   - **Разрешать вход по паролю**. Задайте пароль учетной записи Агента аутентификации. Если нужно, вы можете запросить у пользователя новый пароль после первой аутентификации. Таким образом, у каждого пользователя будет свой уникальный пароль. Также вы можете задать требования к надежности пароля для учетной записи Агента аутентификации в политике.

   - **Разрешать вход по сертификату**. Выберите файл сертификата для аутентификации с помощью смарт-карты или токена. Таким образом, пользователю нужно будет ввести пароль от смарт-карты или токена.

   - **Доступ учетной записи к зашифрованным данным**. Настройте доступ пользователя к зашифрованному диску. Вы можете, например, временно запретить аутентификацию пользователя и не удалять учетную запись Агента аутентификации.

   - **Комментарий**. Введите описание учетной записи, если требуется.

8. Сохраните внесенные изменения.

9. Установите флажок напротив задачи и нажмите на кнопку **Запустить**.

Для удаления учетной записи Агента аутентификации нужно добавить специальную команду в задачу *Управление учетными записями Агента аутентификации*. Групповую задачу удобно использовать, например, для удаления учетной записи уволенного сотрудника.

Как удалить учетную запись Агента аутентификации через Консоль администрирования (MMC)

1. Откройте свойства задачи *Управление учетными записями Агента аутентификации*.

2. В свойствах задачи выберите раздел **Настройки**.

3. Нажмите на кнопку **Добавить** → **Команду для удаления учетной записи**.

4. В открывшемся окне в поле **Учетная запись Windows** укажите имя учетной записи пользователя Windows, на основе которой создана учетная запись для Агента аутентификации, которую вы хотите удалить.

5. Если вы ввели имя учетной записи Windows вручную, нажмите на кнопку **Разрешить**, чтобы определить идентификатор безопасности учетной записи (англ. Security Identifier, SID).

   Если вы не определяете идентификатор безопасности по кнопке **Разрешить**, то он будет определен в момент выполнения задачи на компьютере.

   > Определение идентификатора безопасности учетной записи Windows нужно для проверки корректности ввода имени учетной записи Windows. Если учетная запись Windows не существует на компьютере или в доверенном домене, задача *Управление учетными записями Агента аутентификации* будет завершена с ошибкой.

6. Сохраните внесенные изменения.

Как удалить учетную запись Агента аутентификации через Web Console

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Управление учетными записями Агента аутентификации**.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. В списке учетных записей Агента аутентификации нажмите на кнопку **Добавить** и выберите тип команды **Удаление учетной записи**.

5. Выберите учетную запись пользователя. Вы можете выбрать учетную запись из списка доменных учетных записей или ввести имя учетной записи вручную.

6. Сохраните внесенные изменения.

7. Установите флажок напротив задачи и нажмите на кнопку **Запустить**.

В результате после выполнения задачи при следующей загрузке компьютера пользователь не сможет пройти процедуру аутентификацию и загрузить операционную систему. Kaspersky Endpoint Security запретит доступ к зашифрованным данным.

Для просмотра списка пользователей, которые могут пройти аутентификацию с помощью агента и загрузить операционную систему, нужно перейти в свойства управляемого компьютера.

Как просмотреть список учетных записей Агента аутентификации через Консоль администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Устройства**.
3. Откройте свойства компьютера двойным щелчком мыши.
4. В окне свойств компьютера выберите раздел **Задачи**.
5. В списке задач выберите **Управление учетными записями Агента аутентификации** и откройте свойства задачи двойным щелчком мыши.
6. В свойствах задачи выберите раздел **Настройки**.

В результате вам будет доступен список учетных записей Агента аутентификации на этом компьютере. Только пользователи из списка могут пройти аутентификацию с помощью агента и загрузить операционную систему.

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите просмотреть список учетных записей Агента аутентификации.
3. В свойствах компьютера выберите вкладку **Задачи**.
4. В списке задач выберите **Управление учетными записями Агента аутентификации**.
5. В свойствах задачи выберите вкладку **Параметры приложения**.

В результате вам будет доступен список учетных записей Агента аутентификации на этом компьютере. Только пользователи из списка могут пройти аутентификацию с помощью агента и загрузить операционную систему.

Использование токена и смарт-карты при работе с Агентом аутентификации

При аутентификации для доступа к зашифрованным жестким дискам можно использовать токен или смарт-карту. Для этого необходимо добавить файл электронного сертификата токена или смарт-карты в задачу *Управление учетными записями Агента аутентификации*.

Использование токена или смарт-карты доступно, только если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES256. Если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES56, то в добавлении файла электронного сертификата в команду будет отказано.

Kaspersky Endpoint Security работает со следующими токенами, считывателями смарт-карт и смарт-картами:

- SafeNet eToken PRO 64K (4.2b);
- SafeNet eToken PRO 72K Java;
- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- ruToken Рутокен ЭЦП;
- ruToken Рутокен ЭЦП Flash;
- Athena IDProtect Laser;
- SafeNet eToken PRO 72K Java;
- Aladdin-RD JaCarta PKI.

Чтобы добавить файл электронного сертификата токена или смарт-карты в команду для создания учетной записи Агента аутентификации, его требуется предварительно сохранить с помощью стороннего программного обеспечения, предназначенного для управления сертификатами.

Сертификат токена или смарт-карты должен обладать следующими свойствами:

- Сертификат удовлетворяет стандарту X.509, а файл сертификата имеет кодировку DER.
- Сертификат содержит RSA-ключ длиной не менее 1024 бит.

Если электронный сертификат токена или смарт-карты не удовлетворяет этим требованиям, загрузить файл сертификата в команду для создания учетной записи Агента аутентификации невозможно.

Также параметр `KeyUsage` сертификата должен иметь значение `keyEncipherment` или `dataEncipherment`. Параметр `KeyUsage` определяет назначение сертификата. Если параметр имеет другое значение, Kaspersky Security Center загрузит файл сертификата, но покажет предупреждение.

Если пользователь потерял токен или смарт-карту, администратору требуется добавить файл электронного сертификата нового токена или новой смарт-карты в команду для создания учетной записи Агента аутентификации. После этого пользователю требуется пройти процедуру получения доступа к зашифрованным устройствам или восстановления данных на зашифрованных устройствах.

Расшифровка жестких дисков

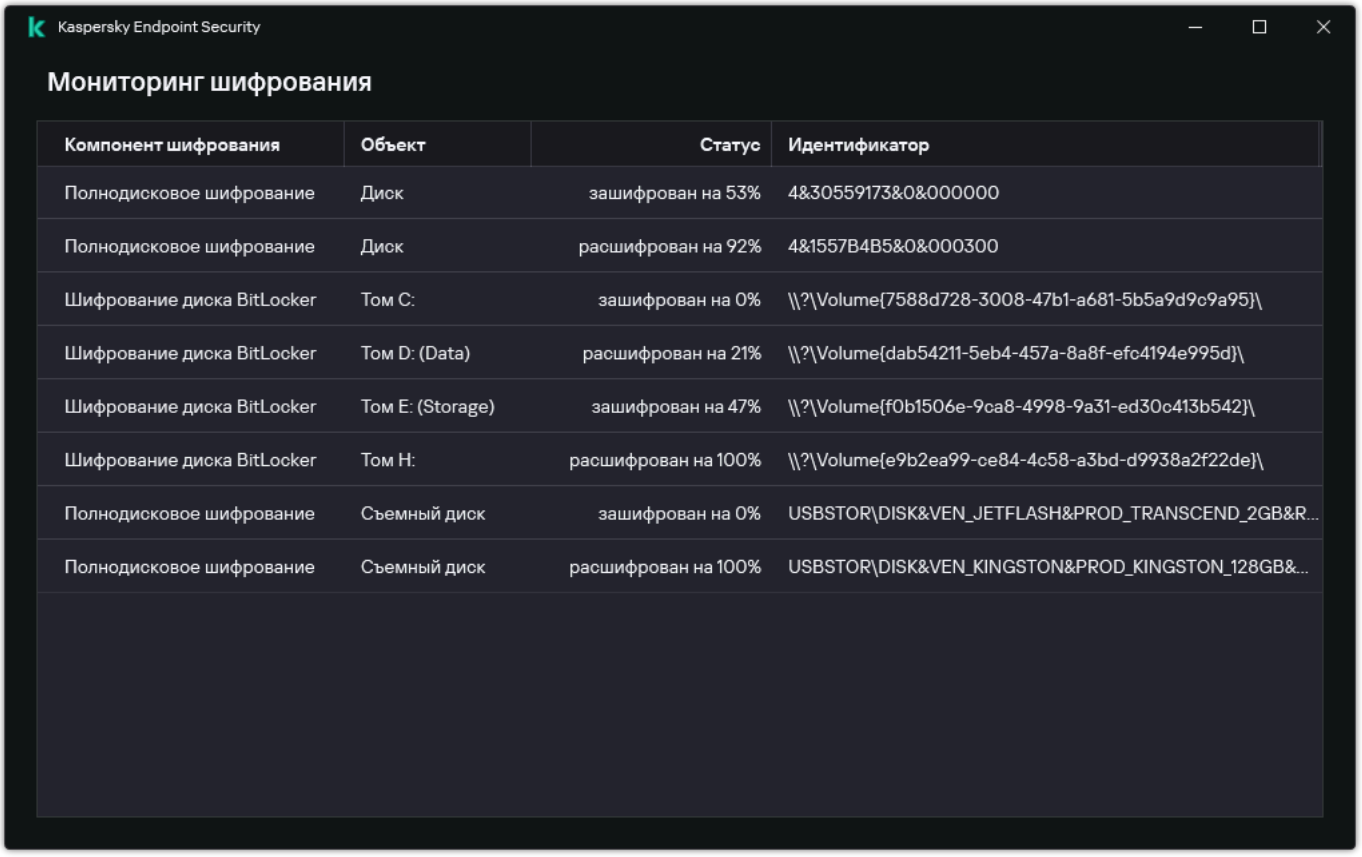
Вы можете расшифровать жесткие диски даже при отсутствии действующей лицензии, допускающей шифрование данных.

Чтобы расшифровать жесткие диски, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных** → **Полнодисковое шифрование**.
4. В раскрывающемся списке **Технология шифрования** выберите ту технологию, с помощью которой были зашифрованы жесткие диски.
5. Выполните одно из следующих действий:
   - В раскрывающемся списке **Режим шифрования** выберите элемент **Расшифровывать все жесткие диски**, если вы хотите расшифровать все зашифрованные жесткие диски.
   - В таблицу **Не шифровать следующие жесткие диски** добавьте те зашифрованные жесткие диски, которые вы хотите расшифровать.

     Этот вариант доступен только для технологии шифрования Шифрование диска Kaspersky.
6. Сохраните внесенные изменения.

Вы можете контролировать процесс шифрования или расшифровки диска на компьютере пользователя с помощью инструмента Мониторинг шифрования. Вы можете запустить инструмент Мониторинг шифрования из главного окна приложения.



Мониторинг шифрования

Если во время расшифровки жестких дисков, зашифрованных с помощью технологии Шифрование диска Kaspersky, пользователь выключает или перезагружает компьютер, то перед последующей загрузкой операционной системы загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет расшифровку жестких дисков.

Если во время расшифровки жестких дисков, зашифрованных с помощью технологии Шифрование диска Kaspersky, операционная система переходит в режим гибернации (hibernation mode), то при выводе операционной системы из режима гибернации загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет расшифровку жестких дисков. После расшифровки жестких дисков режим гибернации недоступен до первой перезагрузки операционной системы.

Если во время расшифровки жестких дисков операционная система переходит в спящий режим (sleep mode), то при выводе операционной системы из спящего режима Kaspersky Endpoint Security возобновляет расшифровку жестких дисков без загрузки Агента аутентификации.

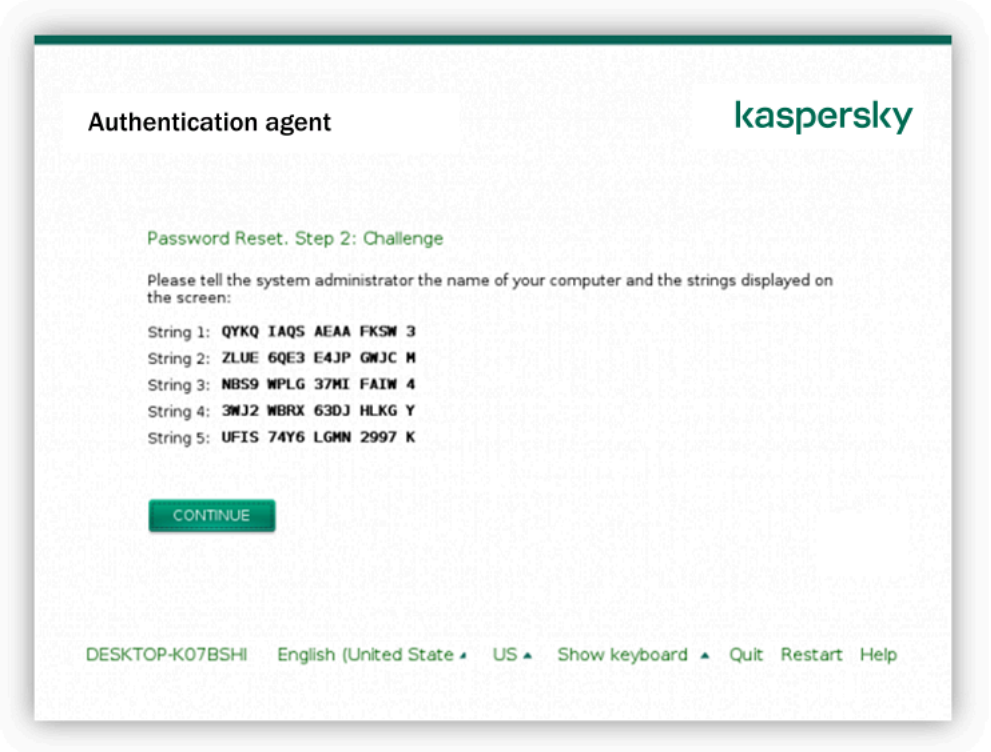
Восстановление доступа к диску, защищенному технологией Шифрование диска Kaspersky

Если пользователь забыл пароль доступа к жесткому диску, защищенному технологией Шифрование диска Kaspersky, нужно запустить процедуру восстановления ("Запрос - Ответ"). Также вы можете воспользоваться служебной учетной записью для доступа к жесткому диску, если вы включили эту функцию в параметрах шифрования диска.

Восстановление доступа к системному жесткому диску

Восстановление доступа к системному жесткому диску, защищенному технологией Шифрование диска Kaspersky, состоит из следующих этапов:

1. Пользователь сообщает администратору блоки запроса (см. рис. ниже).
2. Администратор вводит блоки запроса в Kaspersky Security Center, получает блоки ответа и сообщает блоки ответа пользователю.
3. Пользователь вводит блоки ответа в интерфейсе Агента аутентификации и получает доступ к жесткому диску.



Восстановление доступа к системному жесткому диску, защищенного технологией Шифрование диска Kaspersky

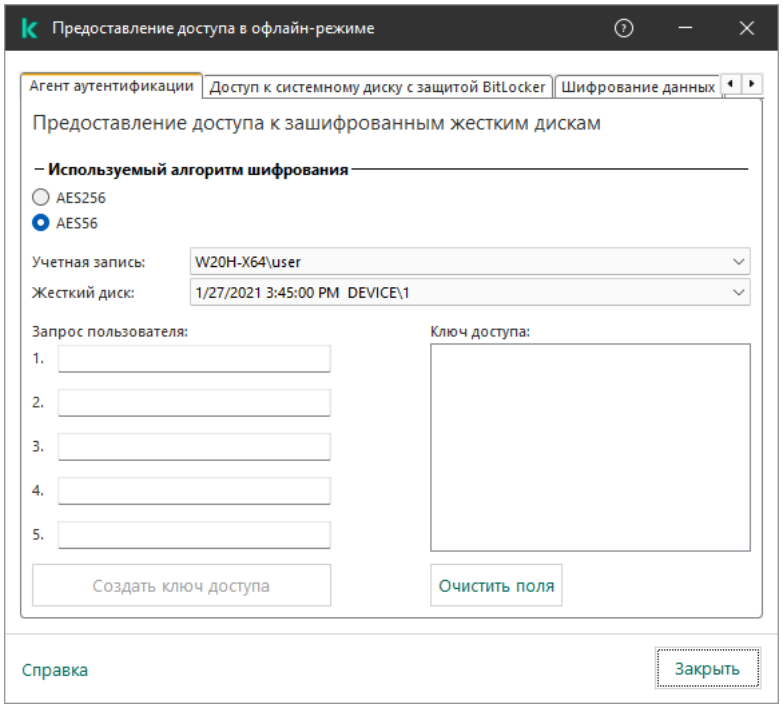
Для запуска процедуры восстановления пользователю нужно в интерфейсе Агента аутентификации нажать на кнопку **Forgot your password**.

Как получить блоки ответа для системного жесткого диска, защищенного технологией Шифрование диска Kaspersky, в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Устройства**.
3. На вкладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
4. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
5. В открывшемся окне выберите вкладку **Агент аутентификации**.
6. В блоке **Используемый алгоритм шифрования** выберите алгоритм шифрования: **AES56** или **AES256**.

   Алгоритм шифрования данных зависит от библиотеки шифрования AES, входящей в состав дистрибутива: *Strong encryption (AES256)* или *Lite encryption (AES56)*. Библиотека шифрования AES устанавливается вместе с приложением.
7. В раскрывающемся списке **Учетная запись** выберите имя учетной записи Агента аутентификации пользователя, запросившего восстановление доступа к диску.
8. В раскрывающемся списке **Жесткий диск** выберите зашифрованный жесткий диск, доступ к которому необходимо восстановить.
9. В блоке **Запрос пользователя** введите блоки запроса, продиктованные пользователем.

В результате содержимое блоков ответа на запрос пользователя о восстановлении имени и пароля учетной записи Агента аутентификации отобразится в поле **Ключ доступа**. Передайте содержимое блоков ответа пользователю.



Предоставление доступа в офлайн-режиме

Как получить блоки ответа для системного жесткого диска, защищенного технологией Шифрование диска Kaspersky, в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Установите флажок рядом с именем компьютера, доступ к диску которого вы хотите восстановить.
3. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.
4. В открывшемся окне выберите раздел **Агент аутентификации**.
5. В раскрывающемся списке **Учетная запись** выберите имя учетной записи Агента аутентификации, созданной для пользователя, запросившего восстановление имени и пароля учетной записи Агента аутентификации.
6. Введите блоки запроса, продиктованные пользователем.

   Содержимое блоков ответа на запрос пользователя о восстановлении имени и пароля учетной записи Агента аутентификации отобразится внизу окна. Передайте содержимое блоков ответа пользователю.

После прохождения процедуры восстановления Агент аутентификации предложит пользователю сменить пароль.

Восстановление доступа к несистемному жесткому диску

Восстановление доступа к несистемному жесткому диску, защищенному технологией Шифрование диска Kaspersky, состоит из следующих этапов:

1. Пользователь отправляет администратору файл запроса.
2. Администратор добавляет файл запроса в Kaspersky Security Center, создает файл ключа доступа и отправляет файл пользователю.
3. Пользователь добавляет файл ключа доступа в Kaspersky Endpoint Security и получает доступ к жесткому диску.

Для запуска процедуры восстановления пользователю нужно обратиться к жесткому диску. В результате Kaspersky Endpoint Security создаст файл запроса (файл с расширением kesdc), который пользователю нужно передать администратору, например, по электронной почте.

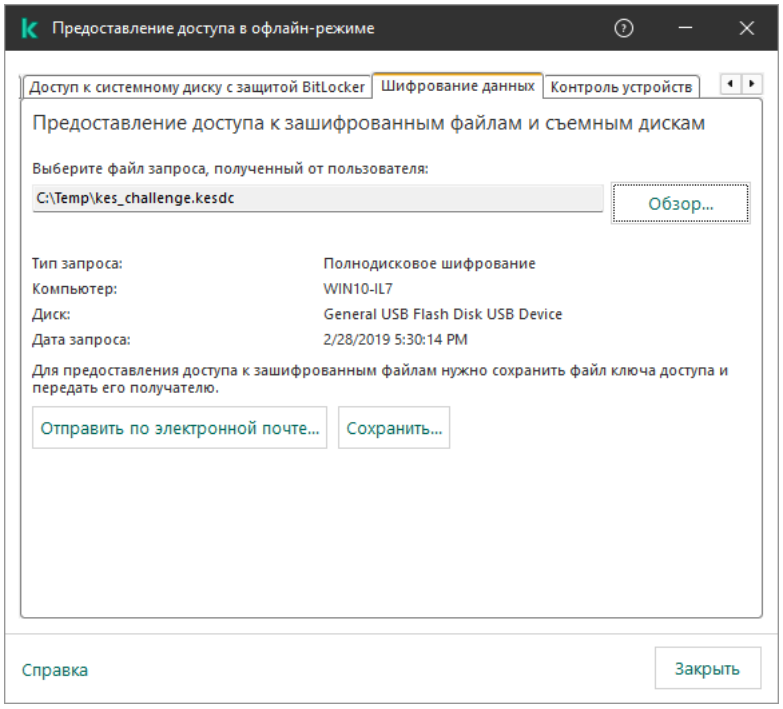
Как получить файл ключа доступа к зашифрованному несистемному жесткому диску в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Устройства**.
3. На вкладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
4. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
5. В открывшемся окне выберите вкладку **Шифрование данных**.

6. На вкладке **Шифрование данных** нажмите на кнопку **Обзор**.

7. В окне выбора файла запроса укажите путь к файлу, полученного от пользователя.

Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.



Предоставление доступа в офлайн-режиме

Как получить файл ключа доступа к зашифрованному несистемному жесткому диску в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.

2. Установите флажок рядом с именем компьютера, доступ к данным которого вы хотите восстановить.

3. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.

4. Выберите раздел **Шифрование данных**.

5. Нажмите на кнопку **Выбрать файл** и выберите файл запроса, полученный от пользователя (файл с расширением kesdc).

   Web Console покажет информацию о запросе. В том числе, имя компьютера, на котором пользователь запрашивает доступ к файлу.

6. Нажмите на кнопку **Сохранить ключ** и выберите папку для сохранения файла ключа доступа к зашифрованным данным (файл с расширением kesdr).

В результате вам будет доступен ключ доступа к зашифрованным данным, который нужно будет передать пользователю.

Вход под служебной учетной записью Агента аутентификации

Kaspersky Endpoint Security позволяет добавить служебную учетную запись Агента аутентификации при шифровании диска. Служебная учетная запись нужна для доступа к компьютеру в случаях, когда пользователь, например, забыл пароль. Также вы можете использовать служебную учетную запись в качестве резервной учетной записи. Для добавления учетной записи вам нужно выбрать служебную учетную запись в параметрах шифрования диска и указать имя учетной записи (по умолчанию `ServiceAccount`). Для прохождения аутентификации с помощью агента вам нужен одноразовый пароль.

Как узнать одноразовый пароль в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Устройства**.
3. Откройте свойства компьютера двойным щелчком мыши.
4. В окне свойств компьютера выберите раздел **Задачи**.
5. В списке задач выберите **Управление учетными записями Агента аутентификации** и откройте свойства задачи двойным щелчком мыши.
6. В окне свойств задачи выберите раздел **Настройки**.
7. В списке учетных записей выберите служебную учетную запись Агента аутентификации (например, `WIN10-USER\ServiceAccount`).
8. В раскрывающемся списке **Действие** выберите **Просмотреть учетную запись**.
9. В свойствах учетной записи установите флажок **Показать начальный пароль**.
10. Скопируйте одноразовый пароль для входа под служебной учетной записью.

Как узнать одноразовый пароль в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите просмотреть список учетных записей Агента аутентификации.

   Откроются свойства компьютера.
3. В свойствах компьютера выберите вкладку **Задачи**.
4. В списке задач выберите **Управление учетными записями Агента аутентификации**.
5. В свойствах задачи выберите вкладку **Параметры приложения**.
6. В списке учетных записей выберите служебную учетную запись Агента аутентификации (например, `WIN10-USER\ServiceAccount`).
7. В свойствах учетной записи установите флажок **Показать пароль**.
8. Скопируйте одноразовый пароль для входа под служебной учетной записью.

Kaspersky Endpoint Security автоматически обновляет пароль после каждой аутентификации пользователя под служебной учетной записью. После прохождения аутентификации с помощью агента вам нужно ввести пароль учетной записи Windows. При входе под служебной учетной записью использовать технологию SSO невозможно.

Обновление операционной системы

Обновление операционной системы компьютера, защищенного с помощью полнодискового шифрования (FDE), имеет ряд особенностей. Выполняйте обновление операционной системы последовательно: сначала обновите ОС на одном компьютере, затем на небольшой части компьютеров, затем на всех компьютерах сети.

Если вы используете технологию Шифрование диска Kaspersky, то перед запуском операционной системы загружается Агент аутентификации. С помощью Агента аутентификации пользователь выполняет вход в систему и получает доступ к зашифрованным дискам. Далее начинается загрузка операционной системы. Если запустить обновление операционной системы на компьютере, защищенном с помощью технологии Шифрование диска Kaspersky, мастер обновления ОС может удалить Агент аутентификации. В результате компьютер может быть заблокирован, так как загрузчик ОС не сможет получить доступ к зашифрованному диску.

Особенности обновления операционной системы:

- **Обновление ОС через WSUS**. Вы можете обновлять операционную систему обычным способом.
- **Обновление ОС из ISO**. Для обновления операционной системы необходимо указать папку с драйверами шифрования диска Kaspersky. Приложение автоматически копирует драйверы в отдельную папку. Выполните следующие действия:

  1. Смонтируйте ISO-образ.
  2. Запустите установку обновления системы со следующим ключом:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.3\reflect_drivers
     ```

Автоматическое обновление ОС доступно только если на компьютере установлена операционная система Windows 10 1607 (RS1) и выше. Для обновления более ранних версий операционной системы рекомендуется сначала расшифровать диск, выполнить обновление ОС, затем зашифровать диск.

Если вы используете технологию Шифрование диска BitLocker, для обновления Windows 10 не нужно расшифровывать жесткие диски. Подробнее о BitLocker см. на сайте Microsoft.

Устранение ошибок при обновлении функциональности шифрования

При обновлении с предыдущих версий приложения до Kaspersky Endpoint Security для Windows 14.3 обновляется функциональность полнодискового шифрования.

При запуске обновления функциональности полнодискового шифрования могут возникнуть следующие ошибки:

- Не удалось инициализировать обновление.
- Устройство несовместимо с Агентом аутентификации.

Чтобы устранить ошибки, возникшие при запуске обновления функциональности полнодискового шифрования, в новой версии приложения выполните следующие действия:

1. Расшифруйте жесткие диски.
2. Повторно зашифруйте жесткие диски.

В процессе обновления функциональности полнодискового шифрования могут возникнуть следующие ошибки:

- Не удалось завершить обновление.
- Откат обновления функциональности шифрования завершен с ошибкой.

Чтобы устранить ошибки, возникшие в процессе обновления функциональности полнодискового шифрования,

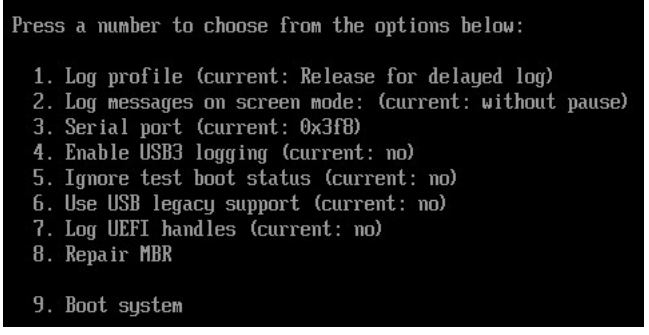
восстановите доступ к зашифрованному устройству с помощью утилиты восстановления.

Трассировка работы Агента аутентификации

Приложение записывает служебную информацию о работе Агента аутентификации, а также информацию о действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.

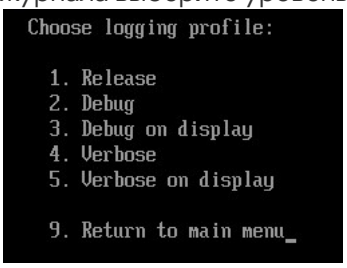
Чтобы включить трассировку работы Агента аутентификации, выполните следующие действия:

1. Включите трассировку работы Kaspersky Endpoint Security.
2. Перезагрузите компьютер.
3. Сразу после запуска компьютера с зашифрованными жесткими дисками по кнопке **F3** вызовите окно для настройки параметров Агента аутентификации.
4. После запуска загрузчика FDE выберите менеджер загрузки **KES (FDE <version>)**.
5. В меню менеджера загрузки перейдите в настройки профиля журнала – **Log profile**.



Меню менеджера загрузки

6. В окне настройки параметров профиля журнала выберите уровень трассировки:



Уровни трассировки работы Агента аутентификации

- **Release**. Если выбран этот вариант, то приложение не записывает информацию о событиях работы Агента аутентификации в файл трассировки.
- **Debug**. Если выбран этот вариант, то приложение записывает информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.
- **Debug on display**. Если выбран этот вариант, то приложение записывает информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки, а также передает ее через COM-порт.

  Если компьютер с зашифрованными жесткими дисками соединен с другим компьютером через COM-порт, то события работы Агента аутентификации можно исследовать с помощью этого компьютера.
- **Verbose**. Если выбран этот вариант, то приложение записывает детальную информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.

  > Уровень детализации записей для этого варианта выше, чем при выборе уровня **Debug**. Высокий уровень детализации записей может замедлять загрузку Агента аутентификации и операционной системы.

- **Verbose on display**. Если выбран этот вариант, то приложение записывает детальную информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки, а также передает ее через COM-порт.

  > Уровень детализации записей для этого варианта выше, чем при выборе уровня **Debug on display**. Высокий уровень детализации записей может замедлять загрузку Агента аутентификации и операционной системы.

После выбора уровня трассировки менеджер загрузки снова покажет меню.

7. В меню менеджера загрузки выберите запуск системы – **Boot system**.

   Загрузчик FDE запустит Агент аутентификации.

   Воспроизведите проблему.

   Запись в файл трассировки Агента аутентификации выполняется в случае, если на компьютере есть зашифрованные жесткие диски или выполняется полнодисковое шифрование.

8. Чтобы остановить процесс трассировки, вернитесь в окно Мониторинга проблем и выключите трассировку.

В результате в папке `%ProgramData%\Kaspersky Lab\KES.14.3\Traces` будут созданы файлы трассировки работы Агента аутентификации KES.SRV. Файл трассировки Агента аутентификации не

передается в "Лабораторию Касперского", как другие файлы трассировки приложения. При необходимости вы можете самостоятельно отправить файл трассировки Агента аутентификации в "Лабораторию Касперского" для анализа.

Изменение справочных текстов Агента аутентификации

Перед изменением справочных текстов Агента аутентификации ознакомьтесь со списком поддерживаемых символов в предзагрузочной среде (см. ниже).

Чтобы изменить справочные тексты Агента аутентификации, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных → Общие настройки шифрования**.
4. В блоке **Шаблоны** нажмите на кнопку **Справка**.
5. В открывшемся окне выполните следующие действия:
   - Выберите вкладку **Аутентификация**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе ввода учетных данных.
   - Выберите вкладку **Смена пароля**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе смены пароля для учетной записи Агента аутентификации.
   - Выберите вкладку **Восстановление пароля**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе восстановления пароля для учетной записи Агента аутентификации.
6. Измените справочные тексты.

   Если вы хотите восстановить исходный текст, нажмите на кнопку **По умолчанию**.

   Вы можете ввести справочный текст, содержащий 16 или менее строк. Максимальная длина строки составляет 64 символа.
7. Сохраните внесенные изменения.

Ограничения поддержки символов в справочных текстах Агента аутентификации

В предзагрузочной среде поддерживаются следующие символы Unicode:

- основная латиница (0000 - 007F);
- дополнительные символы Latin-1 (0080 - 00FF);
- расширенная латиница-A (0100 - 017F);

- расширенная латиница-B (0180 – 024F);
- некомбинируемые протяженные символы-идентификаторы (02B0 – 02FF);
- комбинируемые диакритические знаки (0300 – 036F);
- греческий и коптский алфавиты (0370 – 03FF);
- кириллица (0400 – 04FF);
- иврит (0590 – 05FF);
- арабское письмо (0600 – 06FF);
- дополнительная расширенная латиница (1E00 – 1EFF);
- знаки пунктуации (2000 – 206F);
- символы валют (20A0 – 20CF);
- буквоподобные символы (2100 – 214F);
- геометрические фигуры (25A0 – 25FF);
- формы представления арабских букв-B (FE70 – FEFF).

Символы, не указанные в этом списке, не поддерживаются в предзагрузочной среде. Не рекомендуется использовать такие символы в справочных текстах Агента аутентификации.

Удаление объектов и данных, оставшихся после тестовой работы Агента аутентификации

Если в процессе удаления приложения Kaspersky Endpoint Security обнаруживает объекты и данные, оставшиеся на системном жестком диске после тестовой работы Агента аутентификации, то удаление приложения прерывается и становится невозможным до тех пор, пока эти объекты и данные не будут удалены.

Объекты и данные могут остаться на системном жестком диске после тестовой работы Агента аутентификации только в исключительных ситуациях. Например, если после применения политики Kaspersky Security Center с установленными параметрами шифрования компьютер не перезагружался или после тестовой работы Агента аутентификации приложение не запускается.

Вы можете удалить объекты и данные, оставшиеся на системном жестком диске после тестовой работы Агента аутентификации, следующими способами:

- с помощью политики Kaspersky Security Center;
- с помощью утилиты восстановления.

Чтобы удалить объекты и данные, оставшиеся после тестовой работы Агента аутентификации, с помощью политики Kaspersky Security Center, выполните следующие действия:

1. Примените к компьютеру политику Kaspersky Security Center с установленными параметрами для расшифровки всех жестких дисков компьютера.
2. Запустите Kaspersky Endpoint Security.

Чтобы удалить объекты и данные, оставшиеся после тестовой работы Агента аутентификации, с помощью утилиты восстановления, выполните следующие действия:

1. Запустите исполняемый файл утилиты восстановления fdert.exe, созданный с помощью приложения Kaspersky Endpoint Security.
2. В окне утилиты восстановления выберите нужное устройство.
3. Нажмите на кнопку **Диагностировать**.
4. Если в результате диагностики системного жесткого диска вы получили сообщение об обнаружении объектов и данных, оставшихся после тестовой работы Агента аутентификации, нажмите на кнопку **Удалить объекты и данные АА**.

   Кнопка **Удалить объекты и данные АА** доступна только в случае обнаружения объектов и данных, оставшихся после тестовой работы Агента аутентификации.

Чтобы удалить данные о несовместимости приложения с Агентом аутентификации,

в командной строке введите команду `avp pbatestreset`.

Управление BitLocker

BitLocker – встроенная в операционную систему Windows технология шифрования. Kaspersky Endpoint Security позволяет контролировать и управлять Bitlocker с помощью Kaspersky Security Center. BitLocker шифрует логический том. Шифрование съемных дисков с помощью BitLocker невозможно. Подробнее о BitLocker см. в документации Microsoft.

При шифровании диска BitLocker помещает загрузчик и другие служебные файлы в системный раздел (англ. system partition). Этот раздел не зашифрован. Операционная система создает системный раздел автоматически при установке Windows. Если перед установкой Windows диск полностью размечен, операционная система не сможет создать системный раздел. В этом случае при запуске шифрования диска BitLocker операционная система предложит пользователю разметить диск снова и создать системный раздел. После создания системного раздела операционная система запустит шифрование диска BitLocker.

Алгоритм шифрования BitLocker не зависит от версии установленной библиотеки AES, входящей в состав дистрибутива (AES256 или AES56). Для шифрования используется встроенная в операционную систему библиотека шифрования.

По умолчанию приложение использует алгоритм шифрования BitLocker с длиной ключа 256 бит для шифрования устройств, которые ранее не были зашифрованы. Если устройство было зашифровано до установки приложения, используемый алгоритм шифрования может отличаться. Подробнее о выборе алгоритма шифрования см. на сайте Службы технической поддержки Microsoft. Начиная с версии 12.9 Kaspersky Endpoint Security передает оригинальный ключ восстановления для устройств, ранее зашифрованных сторонним ПО, в Kaspersky Security Center.

BitLocker обеспечивает безопасность хранения ключей доступа с помощью доверенного платформенного модуля. *Доверенный платформенный модуль* (англ. Trusted Platform Module, TPM) – микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины. Использование TPM является самым безопасным способом хранения ключей доступа BitLocker, так как TPM позволяет проверять целостность операционной системы. На компьютерах без TPM вы также можете зашифровать диски. При этом ключ доступа будет зашифрован паролем. Таким образом, BitLocker использует следующие способы аутентификации:

- TPM.
- TPM и PIN-код.
- Пароль.

После шифрования системного жесткого диска для загрузки операционной системы пользователю нужно пройти процедуру аутентификации BitLocker. После прохождения процедуры аутентификации BitLocker будет доступен вход в систему. BitLocker не поддерживает технологию единого входа (SSO).

После шифрования диска BitLocker создает ключ восстановления. Kaspersky Endpoint Security отправляет ключ восстановления в Kaspersky Security Center, чтобы вы имели возможность восстановить доступ к диску, если пользователь, например, забыл пароль.

Если пользователь самостоятельно зашифровал диск с помощью BitLocker, Kaspersky Endpoint Security отправит ключ восстановления и информацию о шифровании диска в Kaspersky Security Center.

Если вы используете групповые политики для Windows, выключите управление BitLocker в параметрах политики. Параметры политики для Windows могут противоречить параметрам политики Kaspersky Endpoint Security. При шифровании диска могут возникнуть ошибки.

Запуск шифрования диска BitLocker

Перед запуском полнодискового шифрования рекомендуется убедиться в том, что компьютер не заражен. Для этого запустите полную проверку или проверку важных областей компьютера. Выполнение полнодискового шифрования на компьютере, зараженном руткитом, может привести к неработоспособности компьютера.

Для работы BitLocker на компьютерах под управлением операционной системы Windows для серверов может потребоваться установить компонент шифрования диска BitLocker. Установите компонент средствами операционной системы (мастер добавления ролей и компонентов). Подробнее об установке компонента шифрования диска BitLocker см. в документации Microsoft.

Как запустить шифрование диска BitLocker через Консоль администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных → Полнодисковое шифрование**.
4. В раскрывающемся списке **Технология шифрования** выберите элемент **Шифрование диска BitLocker**.
5. В раскрывающемся списке **Режим шифрования** выберите элемент **Шифровать все жесткие диски**.

   Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой выполнялось шифрование.

6. Настройте дополнительные параметры шифрования диска BitLocker (см. таблицу ниже).
7. Сохраните внесенные изменения.

Как запустить шифрование диска BitLocker через Web Console

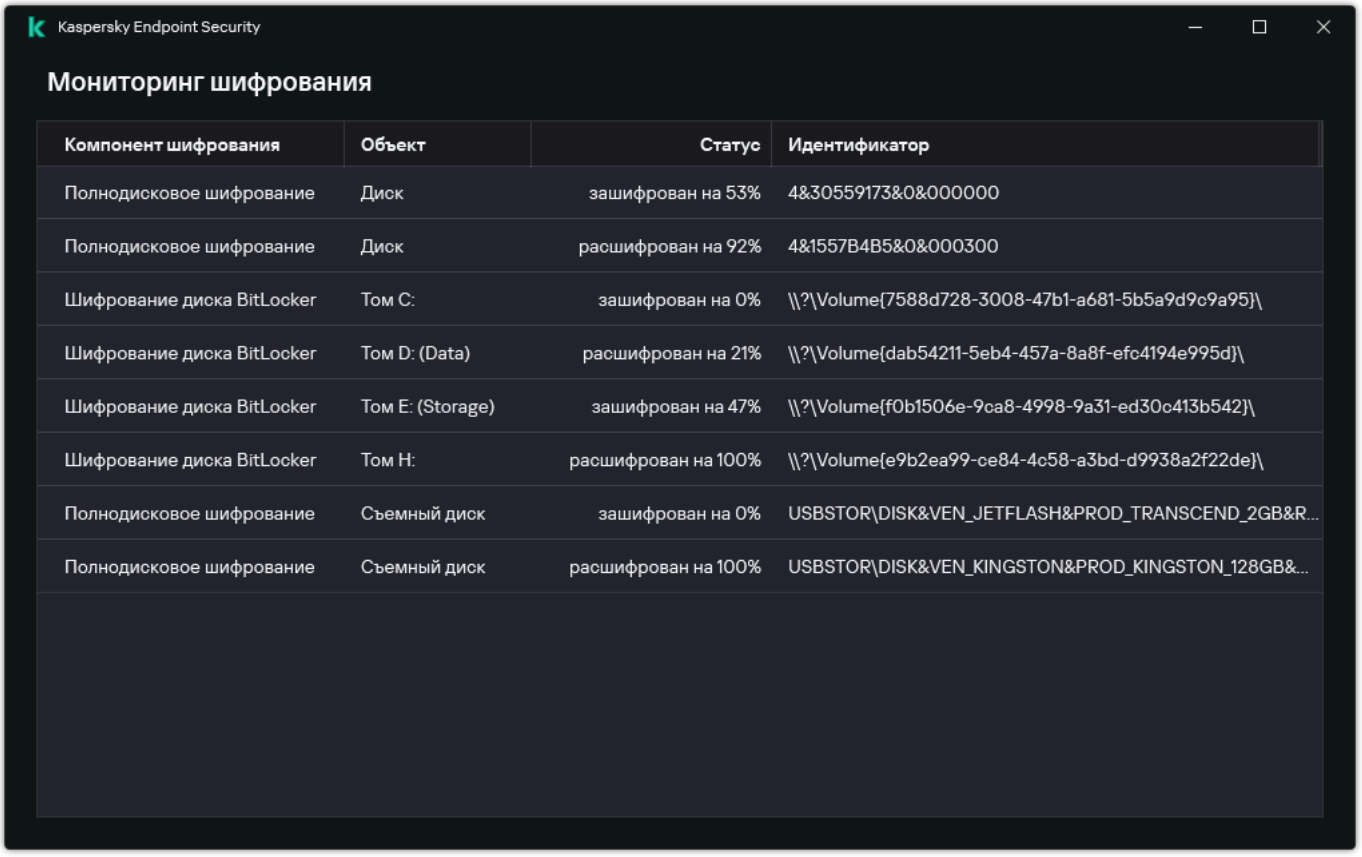
1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Шифрование данных → Полнодисковое шифрование**.
5. Выберите технологию **Шифрование диска BitLocker**.
6. В блоке **Действие с устройствами** выберите элемент **Шифровать все жесткие диски**.

   Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой выполнялось шифрование.

7. Настройте дополнительные параметры шифрования диска BitLocker (см. таблицу ниже).
8. Сохраните внесенные изменения.

Вы можете контролировать процесс шифрования или расшифровки диска на компьютере пользователя с помощью инструмента Мониторинг шифрования. Вы можете запустить инструмент Мониторинг шифрования из главного окна приложения.



Мониторинг шифрования

После применения политики в зависимости от настроек аутентификации приложение покажет следующие запросы:

- Только TPM. Участие пользователя не требуется. Диск будет зашифрован после перезагрузки компьютера.
- TPM + PIN / Пароль. При наличии модуля TPM, появится окно запроса PIN-кода. При отсутствии модуля TPM, появится окно запроса пароля для предзагрузочной аутентификации.
- Только пароль. Появится окно запроса пароля для предзагрузочной аутентификации.

Если в операционной системе включен режим совместимости с Федеральным стандартом обработки информации (FIPS), то в операционных системах Windows 8, а также в более ранних версиях появится окно запроса на подключение запоминающего устройства для сохранения файла ключа восстановления. Вы можете сохранять несколько файлов ключей восстановления на одном запоминающем устройстве.

После установки пароля или PIN-кода BitLocker запросит перезагрузку компьютера для завершения шифрования диска. Далее пользователю нужно пройти процедуру аутентификации BitLocker. После прохождения процедуры аутентификации BitLocker нужно выполнить вход в систему. После загрузки операционной системы BitLocker завершит шифрование диска.

При отсутствии доступа к ключам шифрования пользователь может запросить у администратора локальной сети организации ключ восстановления (если ключ восстановления не был сохранен ранее на запоминающем устройстве или был утерян).

Параметр	Описание
Включить использование проверки подлинности BitLocker, требующей предзагрузочного ввода с клавиатуры на планшетах	Использование аутентификации, требующей ввода данных в предзагрузочной среде, даже если у платформы отсутствует возможность предзагрузочного ввода (например, у сенсорных клавиатур на планшетах). Сенсорная клавиатура планшетов недоступна в предзагрузочной среде. Для прохождения аутентификации BitLocker на планшетах пользователю необходимо подключить, например, USB-клавиатуру. Если флажок установлен, то использование аутентификации, требующей предзагрузочного ввода, разрешено. Рекомендуется использовать этот параметр только для устройств, у которых во время предварительной загрузки, помимо сенсорных клавиатур, имеются альтернативные средства ввода данных, например, USB-клавиатура. Если флажок снят, шифрование диска BitLocker на планшетах невозможно.
Использовать аппаратное шифрование (ОС Windows 8 и выше)	Если флажок установлен, то приложение применяет аппаратное шифрование. Это позволяет увеличить скорость шифрования и сократить использование ресурсов компьютера.
Шифровать только занятое пространство (ОС Windows 8 и выше)	Флажок включает / выключает функцию, ограничивающую область шифрования только занятыми секторами жесткого диска. Это ограничение позволяет сократить время шифрования. Включение / выключение функции **Шифровать только занятое пространство (сокращает время шифрования)** после запуска шифрования не изменяет этого параметра до тех пор, пока жесткие диски не будут расшифрованы. Требуется установить или снять флажок до начала шифрования. Если флажок установлен, то шифруется только та часть жесткого диска, которая занята файлами. Kaspersky Endpoint Security зашифровывает новые данные автоматически по мере их добавления. Если флажок снят, то шифруется весь жесткий диск, в том числе остатки удаленных и отредактированных ранее файлов. Данную функцию рекомендуется применять для новых жестких дисков, данные которых не редактировались и не удалялись. Если вы применяете шифрование на уже используемом жестком диске, рекомендуется зашифровать весь жесткий диск. Это гарантирует защиту всех данных – даже удаленных, но потенциально восстанавливаемых. По умолчанию флажок снят.

Параметр	Описание
Способ аутентификации	**Только пароль (ОС Windows 8 и выше)** Если выбран этот вариант, Kaspersky Endpoint Security запрашивает у пользователя пароль при обращении к зашифрованному диску. Этот вариант действия может быть выбран, если не используется доверенный платформенный модуль (TPM). **Доверенный платформенный модуль (TPM)** Если выбран этот вариант, BitLocker использует доверенный платформенный модуль (TPM). *Доверенный платформенный модуль* (англ. Trusted Platform Module, TPM) – микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины. Для компьютеров под управлением операционных систем Windows 7 и Windows Server 2008 R2 доступно только шифрование с использованием модуля TPM. Если модуль TPM не установлен, шифрование BitLocker невозможно. Использование пароля на этих компьютерах не поддерживается. Устройство, оснащенное доверенным платформенным модулем, может создавать ключи шифрования, которые могут быть расшифрованы только с его помощью. Доверенный платформенный модуль шифрует ключи шифрования собственным корневым ключом хранилища. Корневой ключ хранилища хранится внутри доверенного платформенного модуля. Это обеспечивает дополнительную степень защиты ключей шифрования от попыток взлома. Этот вариант действия выбран по умолчанию. Вы можете установить дополнительную защиту для доступа к ключу шифрования и зашифровать ключ паролем или PIN: • **Использовать PIN для TPM**. Если флажок установлен, пользователь может использовать PIN-код для получения доступа к ключу шифрования, который хранится в доверенном платформенном модуле (TPM). Если флажок снят, пользователю запрещено использовать PIN-код. Для получения доступа к ключу шифрования пользователь использует пароль. • **Доверенный платформенный модуль (TPM), если он недоступен, то пароль**. Если выбран этот вариант, то при отсутствии доверенного платформенного модуля (TPM) пользователь может получить доступ к ключам шифрования с помощью пароля. Если флажок снят и модуль TPM недоступен, то полнодисковое шифрование не запускается. Для выбранного способа аутентификации необходимо настроить требования к паролю или PIN-коду: • **Минимальная длина PIN-а (символов)** (по умолчанию 6). • **Минимальная длина пароля (символов)** (по умолчанию 8). • **Максимальное количество хранимых паролей / PIN** (по умолчанию 5). • **Ограничить срок действия пароля / PIN-а для TPM (дни)** (по умолчанию выключено). • **Использовать расширенный PIN (с буквами и цифрами)**. *Расширенный PIN-код* кроме цифр позволяет использовать другие символы: заглавные и строчные латинские буквы, специальные символы и пробел. По умолчанию выключено.
Автоматически пересоздавать ключ восстановления (дни)	Автоматическое обновление пароля для восстановления доступа к диску, защищенному BitLocker. Если флажок установлен, задайте срок действия пароля ключа восстановления. Эта функция позволяет исключить повторное использование пароля ключа восстановления.

Расшифровка жесткого диска, защищенного BitLocker

Пользователь может самостоятельно расшифровать диск средствами операционной системы (функция *Выключение BitLocker*). После этого Kaspersky Endpoint Security предложит зашифровать диск повторно. Kaspersky Endpoint Security будет предлагать зашифровать диск пока вы не включите расшифровку дисков в политике.

Как расшифровать жесткий диск, защищенный BitLocker, через Консоль администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

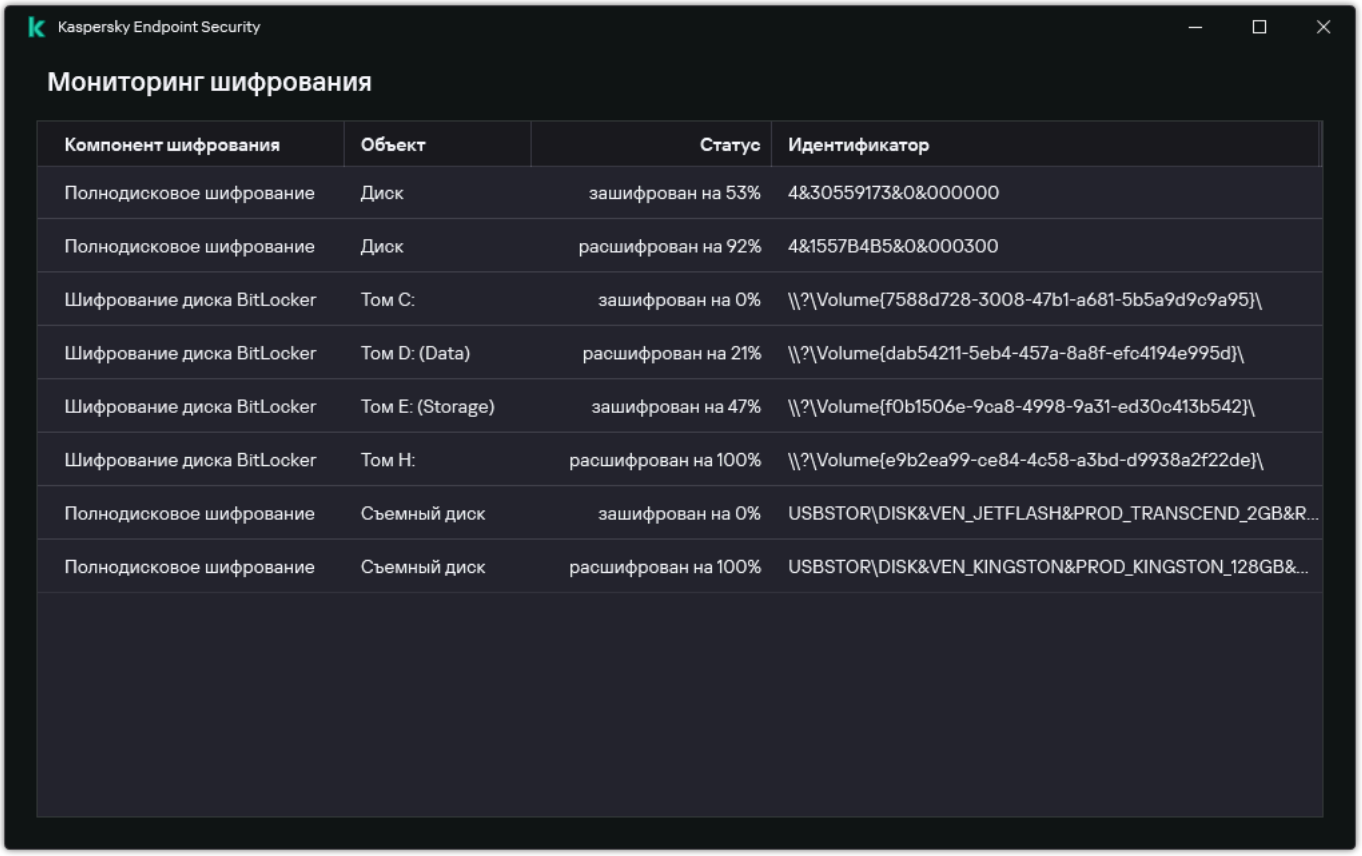
3. В окне политики выберите **Шифрование данных → Полнодисковое шифрование**.
4. В раскрывающемся списке **Технология шифрования** выберите элемент **Шифрование диска BitLocker**.
5. В раскрывающемся списке **Режим шифрования** выберите элемент **Расшифровывать все жесткие диски**.
6. Сохраните внесенные изменения.

Как расшифровать жесткий диск, защищенный BitLocker, через Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Шифрование данных → Полнодисковое шифрование**.
5. Выберите технологию **Шифрование диска BitLocker**.
6. В блоке **Действие с устройствами** выберите элемент **Расшифровывать все жесткие диски**.
7. Сохраните внесенные изменения.

Вы можете контролировать процесс шифрования или расшифровки диска на компьютере пользователя с помощью инструмента Мониторинг шифрования. Вы можете запустить инструмент Мониторинг шифрования из главного окна приложения.



Мониторинг шифрования

Восстановление доступа к диску, защищенному BitLocker

Если пользователь забыл пароль доступа к жесткому диску, зашифрованному BitLocker, нужно запустить процедуру восстановления ("Запрос - Ответ").

Если в операционной системе включен режим совместимости с Федеральным стандартом обработки информации (FIPS), то для операционных систем Windows 8, а также более ранних версий, файл ключа восстановления был сохранен на съемный диск перед шифрованием. Для восстановления доступа к диску вставьте съемный диск и следуйте инструкциям на экране.

Восстановление доступа к жесткому диску, зашифрованному BitLocker, состоит из следующих этапов:

1. Пользователь сообщает администратору идентификатор ключа восстановления (см. рис. ниже).

2. Администратор проверяет идентификатор ключа восстановления в свойствах компьютера в Kaspersky Security Center. Идентификатор, который предоставил пользователь, должен соответствовать идентификатору, который отображается в свойствах компьютера.

3. Если идентификаторы ключа восстановления совпадают, администратор сообщает пользователю ключ восстановления или передает файл ключа восстановления.

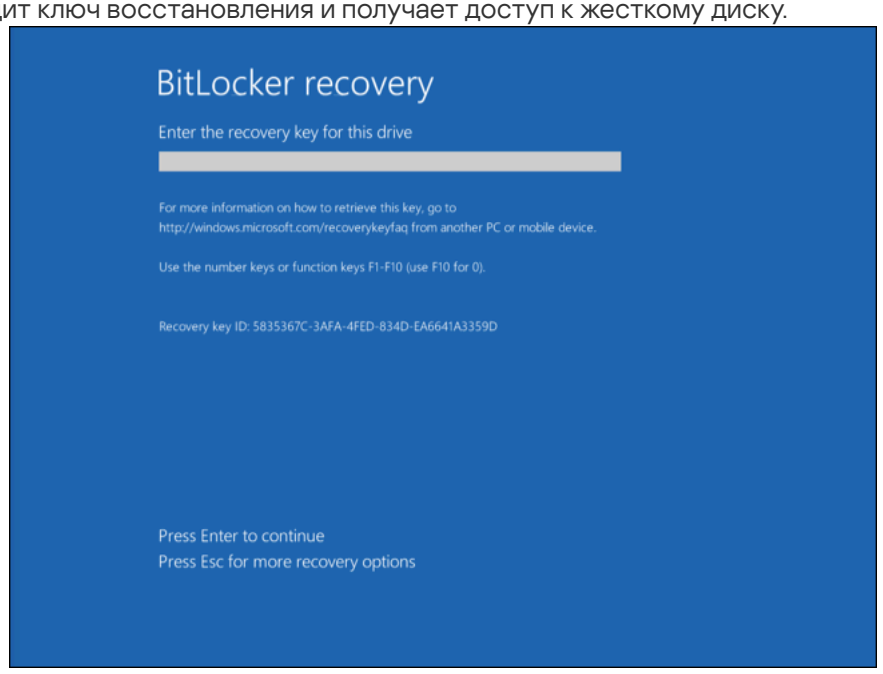
   Файл ключа восстановления используется для компьютеров под управлением следующих операционных систем:

   - Windows 7;
   - Windows 8;
   - Windows Server 2008;
   - Windows Server 2011;
   - Windows Server 2012.

   Для остальных операционных систем используется ключ восстановления.

   Для исключения повторного использования пароля ключа восстановления вы можете настроить автоматическое обновление пароля в параметрах политики.

4. Пользователь вводит ключ восстановления и получает доступ к жесткому диску.



Восстановление доступа к жесткому диску, зашифрованному BitLocker

Восстановление доступа к системному диску

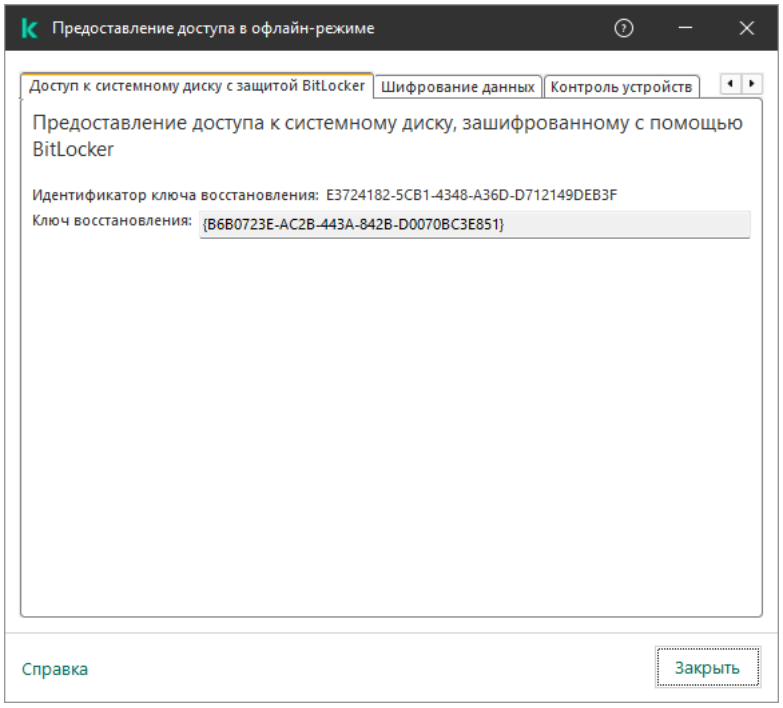
Для запуска процедуры восстановления пользователю нужно на этапе предзагрузочной аутентификации нажать клавишу **Esc**.

Как просмотреть ключ восстановления для системного диска, зашифрованного BitLocker, в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Управляемые устройства**.
3. На вкладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
4. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
5. В открывшемся окне выберите вкладку **Доступ к системному диску с защитой BitLocker**.
6. Запросите у пользователя идентификатор ключа восстановления, указанный в окне ввода пароля BitLocker, и сравните его с идентификатором в поле **Идентификатор ключа восстановления**.

   Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному системному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

В результате вам будет доступен ключ восстановления или файл ключа восстановления, который нужно будет передать пользователю.



Восстановление доступа к диску, зашифрованному с помощью BitLocker

Как просмотреть ключ восстановления для системного диска, зашифрованного BitLocker, в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Установите флажок рядом с именем компьютера, доступ к диску которого вы хотите восстановить.
3. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.
4. В открывшемся окне выберите раздел **BitLocker**.
5. Проверьте идентификатор ключа восстановления. Идентификатор, который предоставил пользователь, должен соответствовать идентификатору, который отображается в параметрах компьютера.

   Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному системному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

6. Нажмите на кнопку **Получить ключ**.

В результате вам будет доступен ключ восстановления или файл ключа восстановления, который нужно будет передать пользователю.

После загрузки операционной системы Kaspersky Endpoint Security предложит пользователю сменить пароль или PIN-код. После установки нового пароля или PIN-кода BitLocker создаст новый ключ восстановления и отправит ключ в Kaspersky Security Center. В результате ключ восстановления и файл ключа восстановления будут обновлены. Если пользователь не сменил пароль, при следующей загрузке операционной системы вы можете использовать старый ключ восстановления.

На компьютерах под управлением Windows 7 сменить пароль или PIN-код невозможно. После ввода ключа восстановления и загрузки операционной системы Kaspersky Endpoint Security не предложит пользователю сменить пароль или PIN-код. Таким образом, установить новый пароль или PIN-код невозможно. Проблема связана с особенностями операционной системы. Для продолжения работы вам нужно перешифровать жесткий диск.

Восстановление доступа к несистемному диску

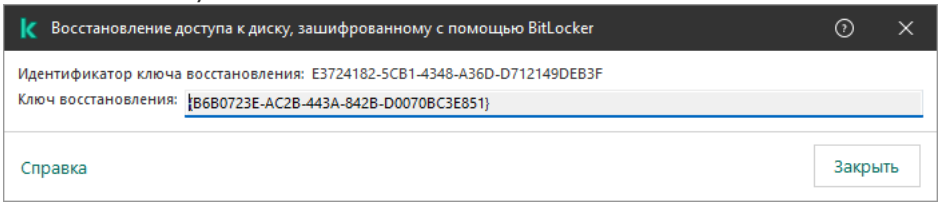
Для запуска процедуры восстановления пользователю нужно в окне предоставления доступа к диску перейти по ссылке **Забыли пароль**. После получения доступа к зашифрованному диску пользователь может включить автоматическую разблокировку диска при аутентификации Windows в параметрах BitLocker.

Как просмотреть ключ восстановления для несистемного диска, зашифрованного BitLocker, в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Дополнительно → Шифрование и защита данных → Зашифрованные жесткие диски**.
3. В рабочей области выберите зашифрованное устройство, для которого вы хотите создать файл ключа доступа, и в контекстном меню устройства выберите пункт **Получить доступ к устройству в Kaspersky Endpoint Security для Windows**.
4. Запросите у пользователя идентификатор ключа восстановления, указанный в окне ввода пароля BitLocker, и сравните его с идентификатором в поле **Идентификатор ключа восстановления**.

   Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

5. Передайте пользователю ключ, указанный в поле **Ключ восстановления**.



Восстановление доступа к диску, зашифрованному с помощью BitLocker

Как просмотреть ключ восстановления для несистемного диска, зашифрованного BitLocker, в Web Console и Cloud Console

1. В главном окне Web Console выберите **Операции → Шифрование и защита данных → Зашифрованные жесткие диски**.
2. Установите флажок рядом с именем компьютера, доступ к диску которого вы хотите восстановить.
3. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.

   Запустится мастер предоставления доступа к устройству.
4. Следуйте указаниям мастера предоставления доступа к устройству:

   a. Выберите плагин **Kaspersky Endpoint Security для Windows**.

   b. Проверьте идентификатор ключа восстановления. Идентификатор, который предоставил пользователь, должен соответствовать идентификатору, который отображается в параметрах компьютера.

   > Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному системному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

   c. Нажмите на кнопку **Получить ключ**.

В результате вам будет доступен ключ восстановления или файл ключа восстановления, который нужно будет передать пользователю.

Приостановка защиты BitLocker для обновления программного обеспечения

Обновление операционной системы, установка пакетов обновлений операционной системы или обновление другого программного обеспечения с включенной защитой BitLocker имеет ряд особенностей. При установке обновлений может потребоваться перезагрузить компьютер несколько раз. После каждой перезагрузки пользователю необходимо проходить аутентификацию BitLocker. Для корректной установки обновлений вы можете временно выключить аутентификацию BitLocker. При этом диск остается зашифрованным и пользователь имеет доступ к данным после входа в систему. Для управления аутентификацией BitLocker предназначена задача *Управление защитой BitLocker*. С помощью задачи вы можете установить количество перезагрузок компьютера, для которых не требуется аутентификация BitLocker. Таким образом, после установки обновлений и завершении работы задачи *Управление защитой BitLocker* аутентификация BitLocker будет автоматически включена. Вы можете включить аутентификацию BitLocker в любой момент.

Как приостановить защиту BitLocker в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.
2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Управление защитой BitLocker**.

Шаг 2. Управление защитой BitLocker

Настройте параметры аутентификации BitLocker. Для приостановки защиты BitLocker выберите **Временно разрешить пропуск аутентификации BitLocker** и установите количество перезагрузок без аутентификации BitLocker (1–15 раз). Если требуется, установите дату и время срока действия задачи. В указанный срок задача автоматически будет выключена и при перезагрузке компьютера пользователю нужно будет проходить аутентификацию BitLocker.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Определение названия задачи

Введите название задачи, например, *Обновление до Windows 10*.

Шаг 5. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как приостановить защиту BitLocker в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows**.
2. В раскрывающемся списке **Тип задачи** выберите **Управление защитой BitLocker**.
3. В поле **Название задачи** введите короткое описание, например, *Обновление до Windows 10*.
4. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Управление защитой BitLocker

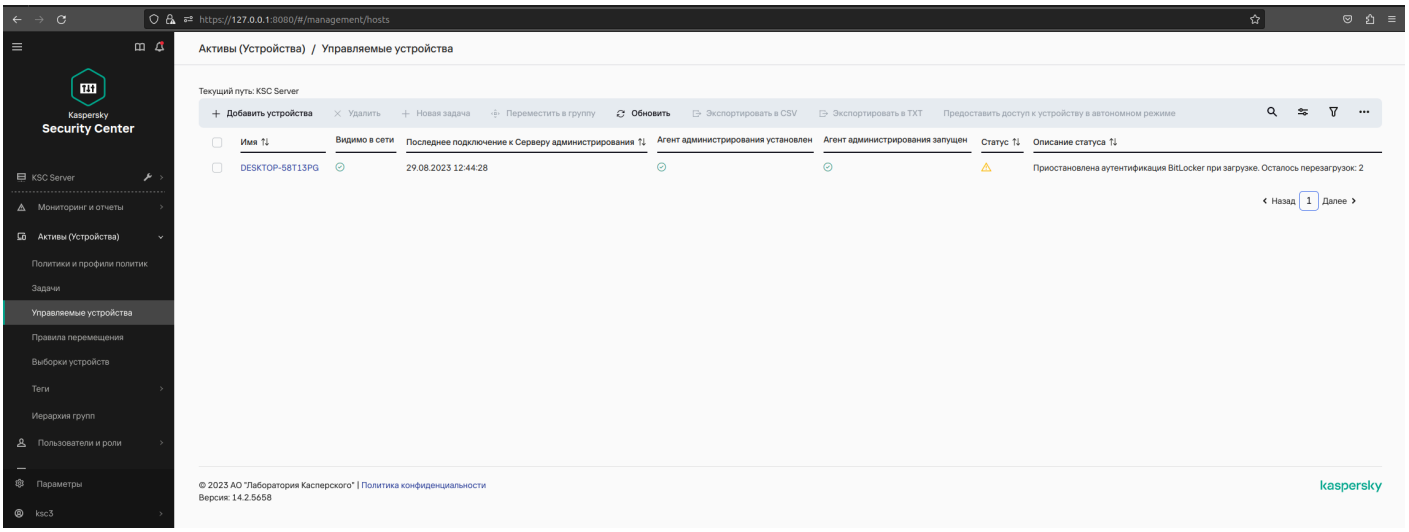
Настройте параметры аутентификации BitLocker. Для приостановки защиты BitLocker выберите **Временно разрешить пропуск аутентификации BitLocker** и установите количество перезагрузок без аутентификации BitLocker (1–15 раз). Если требуется, установите дату и время срока действия задачи. В указанный срок задача автоматически будет выключена и при перезагрузке компьютера пользователю нужно будет проходить аутентификацию BitLocker.

Шаг 3. Завершение создание задачи

Завершите работу мастера. В списке задач отобразится новая задача.

Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку **Запустить**.

В результате после выполнения задачи при следующей перезагрузке компьютера BitLocker не будет запрашивать аутентификацию пользователя. После каждой перезагрузки компьютера Kaspersky Endpoint Security формирует событие о перезагрузке компьютера без аутентификации BitLocker и указывает количество оставшихся перезагрузок. Далее Kaspersky Endpoint Security отправляет событие в Kaspersky Security Center для контроля администратором. Также вы можете узнать количество оставшихся перезагрузок в консоли Kaspersky Security Center в папке **Управляемые устройства** в описании статуса устройства.



Список управляемых устройств

По истечении заданного количества перезагрузок компьютера или срока действия задачи аутентификация BitLocker будет автоматически включена. Для доступа к данным пользователю нужно пройти процедуру аутентификации BitLocker.

На компьютерах под управлением Windows 7 в BitLocker отсутствует возможность подсчета количества перезагрузок компьютера. Подсчет перезагрузок на компьютерах под управлением Windows 7 выполняет Kaspersky Endpoint Security. Таким образом, для автоматического включения аутентификации BitLocker после каждой перезагрузки должен быть выполнен запуск Kaspersky Endpoint Security.

Для досрочного включения аутентификации BitLocker откройте свойства задачи *Управление защитой BitLocker* и установите значение **Запрашивать пароль каждый раз**.

Шифрование файлов на локальных дисках компьютера

Шифрование файлов не поддерживается на компьютерах с Arm-архитектурой.

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов.

Шифрование файлов имеет следующие особенности:

- Kaspersky Endpoint Security шифрует / расшифровывает стандартные папки только для локальных профилей пользователей (англ. local user profiles) операционной системы. Kaspersky Endpoint Security не шифрует и не расшифровывает стандартные папки для перемещаемых профилей пользователей (англ. roaming user profiles), обязательных профилей пользователей (англ. mandatory user profiles), временных профилей пользователей (англ. temporary user profiles), а также перенаправленные папки.

- Kaspersky Endpoint Security не выполняет шифрование файлов, изменение которых может повредить работе операционной системы и установленных приложений. Например, в список исключений из шифрования входят следующие файлы и папки со всеми вложенными в них папками:

  - %WINDIR%;

  - %PROGRAMFILES% и %PROGRAMFILES(X86)%;

  - файлы реестра Windows.

  Список исключений из шифрования недоступен для просмотра и изменения. Файлы и папки из списка исключений из шифрования можно добавить в список для шифрования, но при выполнении шифрования файлов они не будут зашифрованы.

Запуск шифрования файлов на локальных дисках компьютера

Kaspersky Endpoint Security не шифрует файлы, содержимое которых расположено в облачном хранилище OneDrive и других папках с именем OneDrive. Также Kaspersky Endpoint Security блокирует копирование зашифрованных файлов в папки OneDrive, если эти файлы не добавлены в правило расшифровки.

Чтобы зашифровать файлы на локальных дисках компьютера, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Шифрование данных → Шифрование файлов**.

4. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.

5. На вкладке **Шифрование** нажмите на кнопку **Добавить** и в раскрывающемся списке выберите один из следующих элементов:

   a. Выберите элемент **Стандартные папки**, чтобы добавить в правило шифрования файлы из папок локальных профилей пользователей, предложенных специалистами "Лаборатории Касперского".

      - **Документы**. Файлы в стандартной папке операционной системы *Документы*, а также вложенные папки.

      - **Избранное**. Файлы в стандартной папке операционной системы *Избранное*, а также вложенные папки.

      - **Рабочий стол**. Файлы в стандартной папке операционной системы *Рабочий стол*, а также вложенные папки.

- **Временные файлы**. Временные файлы, связанные с работой установленных на компьютере приложений. Например, приложения Microsoft Office создают временные файлы с резервными копиями документов.

  > Рекомендуется не шифровать временные файлы, так как это может привести к потере данных. Например, Microsoft Word создает временные файлы при работе с документом. Если временные файлы зашифрованы, а исходный файл нет, то при попытке сохранить документ пользователь может получить ошибку *Доступ запрещен*. Также Microsoft Word может сохранить файл, но открыть документ в следующий раз будет невозможно, то есть данные будут утеряны.

- **Файлы Outlook**. Файлы, связанные с работой почтового клиента Outlook: файлы данных (PST), автономные файлы данных (OST), файлы автономной адресной книги (OAB) и файлы персональной адресной книги (PAB).

b. Выберите элемент **Папку вручную**, чтобы добавить в правило шифрования папку, путь к которой введен вручную.

   При добавлении пути к папке следует использовать следующие правила:

   - Используйте переменную окружения (например, `%FOLDER%\UserFolder\`). Вы можете использовать переменную окружения только один раз и только в начале пути.
   - Не используйте относительные пути.
   - Не используйте символы `*` и `?`.
   - Не используйте UNC-пути.
   - Используйте `;` или `,` в качестве разделительного символа.

c. Выберите элемент **Файлы по расширению**, чтобы добавить в правило шифрования отдельные расширения файлов. Kaspersky Endpoint Security шифрует файлы с указанными расширениями на всех локальных дисках компьютера.

d. Выберите элемент **Файлы по группам расширений**, чтобы добавить в правило шифрования группы расширений файлов (например, группа *Документы Microsoft Office*). Kaspersky Endpoint Security шифрует файлы с расширениями, перечисленными в группах расширений, на всех локальных дисках компьютера.

6. Сохраните внесенные изменения.

Сразу после применения политики Kaspersky Endpoint Security шифрует файлы, включенные в правило шифрования и не включенные в правило расшифровки.

Шифрование файлов имеет следующие особенности:

- Если один и тот же файл добавлен и в правило шифрования, и в правило расшифровки, то Kaspersky Endpoint Security выполняет следующие действия:
  - Если исходный файл не зашифрован, Kaspersky Endpoint Security не шифрует этот файл.
  - Если исходный файл зашифрован, Kaspersky Endpoint Security расшифровывает этот файл.

- Kaspersky Endpoint Security продолжает шифровать новые файлы, если файлы удовлетворяют критериям правила шифрования. Например, вы изменили свойства незашифрованного файла (путь или расширение), и в результате файл удовлетворяет критериям правила шифрования. Kaspersky Endpoint Security шифрует этот файл.
- Когда пользователь создает новый файл, свойства которого удовлетворяют критериям правила шифрования, Kaspersky Endpoint Security шифрует файл сразу же при открытии файла.
- Kaspersky Endpoint Security откладывает шифрование открытых файлов до тех пор, пока они не будут закрыты.
- Если вы переносите зашифрованный файл в другую папку на локальном диске, файл остается зашифрованным, независимо от того, включена ли эта папка в правило шифрования.
- Если вы расшифровали файл и скопировали файл в другую папку на локальном диске, которая не включена в правило расшифровки, копия файла может быть зашифрована. Для исключения шифрования копии файла, создайте для целевой папки правило расшифровки.

Формирование правил доступа приложений к зашифрованным файлам

По умолчанию все приложения работают с зашифрованными файлами в расшифрованном виде. Если вы постоянно используете отдельные приложения (например, браузеры или текстовые редакторы), то для защиты информации вы можете создать правила доступа к зашифрованным файлам.

Рекомендуется создать правило доступа к зашифрованным файлам для браузеров Microsoft Internet Explorer и Microsoft Edge. Из-за особенностей работы этих браузеров при загрузке зашифрованного файла на веб-сайт (например, облачное хранилище), файл автоматически расшифровывается. Это может привести к утечке информации. Загрузить зашифрованный файл с помощью этих браузеров невозможно. Рекомендуется установить правило **Разрешать доступ к зашифрованным файлам только в виде шифротекста**. Для других браузеров (например, Google Chrome) создавать правило не требуется.

Чтобы сформировать правила доступа приложений к зашифрованным файлам, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных → Шифрование файлов**.
4. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.

   Правила доступа действуют только в режиме **Согласно правилам**. Если после применения правил доступа в режиме **Согласно правилам** вы перейдете в режим **Оставлять без изменений**, то Kaspersky Endpoint Security будет игнорировать все правила доступа. Все приложения будут иметь доступ ко всем зашифрованным файлам.

5. В правой части окна выберите вкладку **Правила для приложений**.

6. Если вы хотите выбрать приложения исключительно из списка Kaspersky Security Center, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Приложения из списка Kaspersky Security Center**.

   a. Задайте фильтры для вывода списка приложений в таблице. Для этого укажите значения параметров **Приложение**, **Производитель**, **Период добавления**, а также флажков из блока **Группа**.

   b. Нажмите на кнопку **Обновить**.

   c. В таблице отобразится список приложений, удовлетворяющих заданным фильтрам.

   d. В графе **Приложение** установите флажки напротив тех приложений в таблице, для которых вы хотите сформировать правила доступа к зашифрованным файлам.

   e. В раскрывающемся списке **Правило для приложений** выберите правило, которое будет определять доступ приложений к зашифрованным файлам.

   f. В раскрывающемся списке **Действие для приложений, выбранных ранее** выберите действие, которое выполняет Kaspersky Endpoint Security над правилами доступа к зашифрованным файлам, сформированными для указанных выше приложений ранее.

   Информация о правиле доступа приложений к зашифрованным файлам отобразится в таблице на вкладке **Правила для приложений**.

7. Если вы хотите выбрать приложения вручную, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Приложения вручную**.

   a. В поле ввода введите имя или список имен исполняемых файлов приложений с их расширениями.

      Вы можете также добавить имена исполняемых файлов приложений из списка Kaspersky Security Center, нажав на кнопку **Добавить из списка Kaspersky Security Center**.

   b. Если требуется, в поле **Описание** введите описание списка приложений.

   c. В раскрывающемся списке **Правило для приложений** выберите правило, которое будет определять доступ приложений к зашифрованным файлам.

   Информация о правиле доступа приложений к зашифрованным файлам отобразится в таблице на вкладке **Правила для приложений**.

8. Сохраните внесенные изменения.

Шифрование файлов, создаваемых и изменяемых отдельными приложениями

Вы можете создать правило, согласно которому Kaspersky Endpoint Security будет шифровать все файлы, создаваемые и изменяемые указанными в правиле приложениями.

Файлы, созданные или измененные указанными приложениями до применения правила шифрования, не будут зашифрованы.

Чтобы настроить шифрование файлов, создаваемых и изменяемых отдельными приложениями, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных → Шифрование файлов**.
4. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.

   Правила шифрования действуют только в режиме **Согласно правилам**. Если после применения правил шифрования в режиме **Согласно правилам** вы перейдете в режим **Оставлять без изменений**, то Kaspersky Endpoint Security будет игнорировать все правила шифрования. Файлы, которые были зашифрованы ранее, по-прежнему останутся зашифрованными.

5. В правой части окна выберите вкладку **Правила для приложений**.
6. Если вы хотите выбрать приложения исключительно из списка Kaspersky Security Center, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Приложения из списка Kaspersky Security Center**.

   a. Задайте фильтры для вывода списка приложений в таблице. Для этого укажите значения параметров **Приложение**, **Производитель**, **Период добавления**, а также флажков из блока **Группа**.

   b. Нажмите на кнопку **Обновить**.

      В таблице отобразится список приложений, удовлетворяющих заданным фильтрам.

   c. В графе **Приложение** установите флажки напротив тех приложений в таблице, создаваемые файлы которых вы хотите шифровать.

   d. В раскрывающемся списке **Правило для приложений** выберите элемент **Шифровать все создаваемые файлы**.

   e. В раскрывающемся списке **Действие для приложений, выбранных ранее** выберите действие, которое выполняет Kaspersky Endpoint Security над правилами шифрования файлов, сформированными для указанных выше приложений ранее.

   Информация о правиле шифрования файлов, создаваемых и изменяемых выбранными приложениями, отобразится в таблице на вкладке **Правила для приложений**.

7. Если вы хотите выбрать приложения вручную, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Приложения вручную**.

   a. В поле ввода введите имя или список имен исполняемых файлов приложений с их расширениями.

      Вы можете также добавить имена исполняемых файлов приложений из списка Kaspersky Security Center, нажав на кнопку **Добавить из списка Kaspersky Security Center**.

   b. Если требуется, в поле **Описание** введите описание списка приложений.

   c. В раскрывающемся списке **Правило для приложений** выберите элемент **Шифровать все создаваемые файлы**.

Информация о правиле шифрования файлов, создаваемых и изменяемых выбранными приложениями, отобразится в таблице на вкладке **Правила для приложений**.

8. Сохраните внесенные изменения.

Формирование правила расшифровки

Чтобы сформировать правило расшифровки, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных → Шифрование файлов**.
4. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.
5. На вкладке **Расшифровка** нажмите на кнопку **Добавить** и в раскрывающемся списке выберите один из следующих элементов:
   a. Выберите элемент **Стандартные папки**, чтобы добавить в правило расшифровки файлы из папок локальных профилей пользователей, предложенных специалистами "Лаборатории Касперского".
   b. Выберите элемент **Папку вручную**, чтобы добавить в правило расшифровки папку, путь к которой введен вручную.
   c. Выберите элемент **Файлы по расширению**, чтобы добавить в правило расшифровки отдельные расширения файлов. Kaspersky Endpoint Security не шифрует файлы с указанными расширениями на всех локальных дисках компьютера.
   d. Выберите элемент **Файлы по группам расширений**, чтобы добавить в правило расшифровки группы расширений файлов (например, группа *Документы Microsoft Office*). Kaspersky Endpoint Security не шифрует файлы с расширениями, перечисленными в группах расширений, на всех локальных дисках компьютера.
6. Сохраните внесенные изменения.

Если один и тот же файл добавлен и в правило шифрования, и в правило расшифровки, то Kaspersky Endpoint Security не шифрует этот файл, если он не зашифрован, и расшифровывает, если он зашифрован.

Расшифровка файлов на локальных дисках компьютера

Чтобы расшифровать файлы на локальных дисках компьютера, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Шифрование данных → Шифрование файлов**.

4. В правой части окна выберите вкладку **Шифрование**.

5. Исключите из списка для шифрования файлы и папки, которые вы хотите расшифровать. Для этого в списке выберите файлы и в контекстном меню кнопки **Удалить** выберите пункт **Удалить правило и расшифровать файлы**.

   Удаленные из списка для шифрования файлы и папки автоматически добавляются в список для расшифровки.

6. Сформируйте список файлов для расшифровки.

7. Сохраните внесенные изменения.

Сразу после применения политики Kaspersky Endpoint Security расшифровывает зашифрованные файлы, добавленные в список для расшифровки.

Kaspersky Endpoint Security расшифровывает зашифрованные файлы, если их параметры (путь к файлу / название файла / расширение файла) изменяются и начинают удовлетворять параметрам объектов, добавленных в список для расшифровки.

Kaspersky Endpoint Security откладывает расшифровку открытых файлов до тех пор, пока они не будут закрыты.

Создание зашифрованных архивов

Для защиты данных при передаче файлов пользователям вне корпоративной сети вы можете использовать зашифрованные архивы. Зашифрованные архивы удобно использовать для передачи файлов большого размера с помощью съемных дисков, так как почтовые клиенты имеют ограничения по размеру файла.

Перед созданием зашифрованных архивов Kaspersky Endpoint Security запросит у пользователя пароль. Для обеспечения надежной защиты данных вы можете включить проверку сложности паролей и выбрать критерии сложности. Таким образом, пользователю будет запрещено использовать короткие и простые пароли, например, `1234`.

Как включить проверку сложности пароля при создании зашифрованных архивов в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Шифрование данных → Общие настройки шифрования**.

4. В блоке **Настройки паролей** нажмите на кнопку **Настройка**.

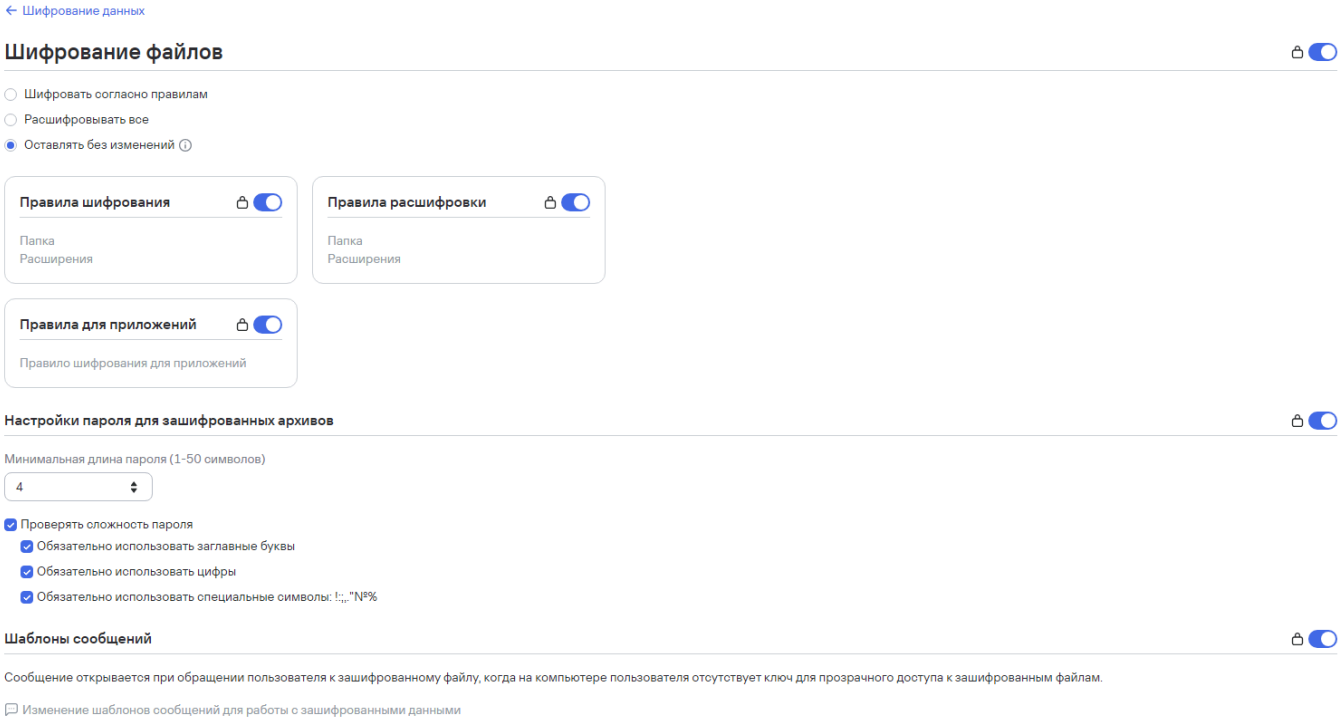
5. В открывшемся окне выберите вкладку **Зашифрованные архивы**.

6. Настройте параметры сложности пароля при создании зашифрованных архивов.

Как включить проверку сложности пароля при создании зашифрованных архивов в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Шифрование данных** → **Шифрование файлов**.
5. В блоке **Настройки пароля для зашифрованных архивов** настройте параметры сложности пароля при создании зашифрованных архивов.



Параметры Шифрования файлов

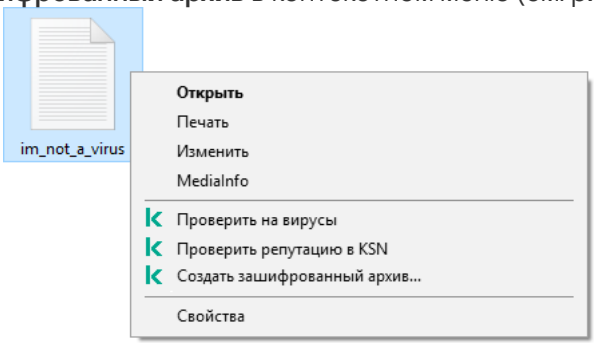
Вы можете создавать зашифрованные архивы на компьютерах с установленным приложением Kaspersky Endpoint Security с функцией шифрования файлов.

При добавлении в зашифрованный архив файла, содержимое которого расположено в облачном хранилище OneDrive, Kaspersky Endpoint Security загружает содержимое этого файла и осуществляет шифрование.

Чтобы создать зашифрованный архив, выполните следующие действия:

1. В любом файловом менеджере выделите файлы или папки, которые вы хотите добавить в зашифрованный архив. По правой клавише мыши откройте их контекстное меню.

2. Выберите пункт **Создать зашифрованный архив** в контекстном меню (см. рис. ниже).



Создание зашифрованного архива

3. В открывшемся окне задайте пароль и повторите его.

   Пароль должен соответствовать критериям сложности, заданным в политике.

4. Нажмите на кнопку **Создать**.

   Запустится процесс создания зашифрованного архива. В процессе создания зашифрованного архива Kaspersky Endpoint Security не выполняет сжатие файлов. По завершении процесса в указанном месте на диске будет создан самораспаковывающийся защищенный паролем зашифрованный архив (исполняемый файл с расширением exe) – .

Для получения доступа к файлам в зашифрованном архиве нужно запустить мастер распаковки архива двойным щелчком мыши и ввести пароль. Если вы забыли пароль, восстановить доступ к файлам в зашифрованном архиве невозможно. Вы можете создать зашифрованный архив повторно.

Восстановление доступа к зашифрованным файлам

При шифровании файлов Kaspersky Endpoint Security получает ключ шифрования, необходимый для прямого доступа к зашифрованным файлам. С помощью ключа шифрования пользователь, работающий под любой из учетных записей Windows, которая была активной во время шифрования файлов, может получать прямой доступ к зашифрованным файлам. Пользователям, работающим под учетными записями Windows, которые были неактивны во время шифрования файлов, требуется связь с Kaspersky Security Center для доступа к зашифрованным файлам.

Зашифрованные файлы могут быть недоступны в следующих случаях:

- На компьютере пользователя присутствуют ключи шифрования, но нет связи с Kaspersky Security Center для работы с ними. В этом случае пользователю требуется запросить доступ к зашифрованным файлам у администратора локальной сети организации.

  При отсутствии связи с Kaspersky Security Center требуется:

  - для доступа к зашифрованным файлам на жестких дисках компьютера запросить один ключ доступа;
  - для доступа к зашифрованным файлам на съемных дисках запросить ключ доступа к зашифрованным файлам для каждого съемного диска.

- С компьютера пользователя удалены компоненты шифрования. В этом случае пользователь может открыть зашифрованные файлы на локальных дисках и съемных дисках, но содержимое файлов отображается как зашифрованное.

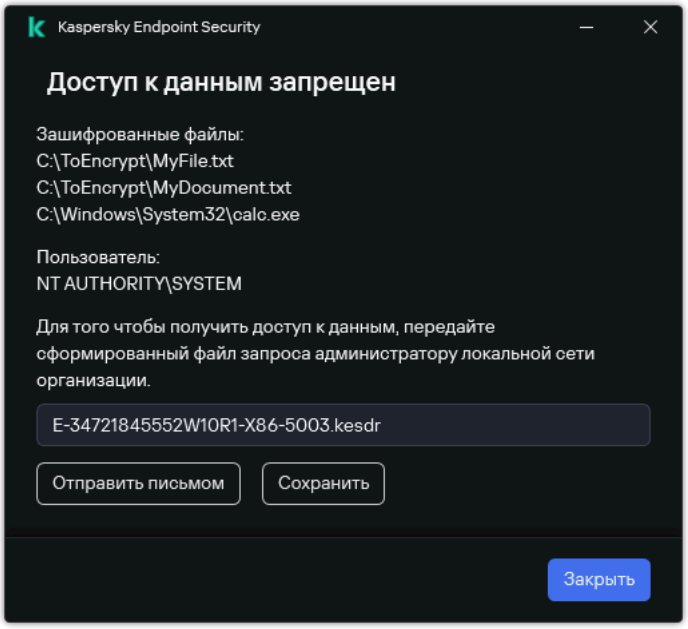
  Пользователь может работать с зашифрованными файлами при следующих условиях:

  - Файлы помещены в зашифрованные архивы, созданные на компьютере с установленным приложением Kaspersky Endpoint Security.
  - Файлы хранятся на съемных дисках, для которых разрешена работа в портативном режиме.

Для получения доступ к зашифрованным файлам пользователю нужно запустить процедуру восстановления ("Запрос - Ответ").

Восстановление доступ к зашифрованным файлам состоит из следующих этапов:

1. Пользователь отправляет администратору файл запроса (см. рис. ниже).
2. Администратор добавляет файл запроса в Kaspersky Security Center, создает файл ключа доступа и отправляет файл пользователю.
3. Пользователь добавляет файл ключа доступа в Kaspersky Endpoint Security и получает доступ к файлам.



Восстановление доступа к зашифрованным файлам

Для запуска процедуры восстановления пользователю нужно обратиться к файлу. В результате Kaspersky Endpoint Security создаст файл запроса (файл с расширением kesdc), который пользователю нужно передать администратору, например, по электронной почте.

Kaspersky Endpoint Security формирует файл запроса доступа ко всем зашифрованным файлам, хранящимся на диске компьютера (локальном диске или съемном диске).

Как получить файл ключа доступа к зашифрованным данным в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Устройства**.

3. На вкладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.

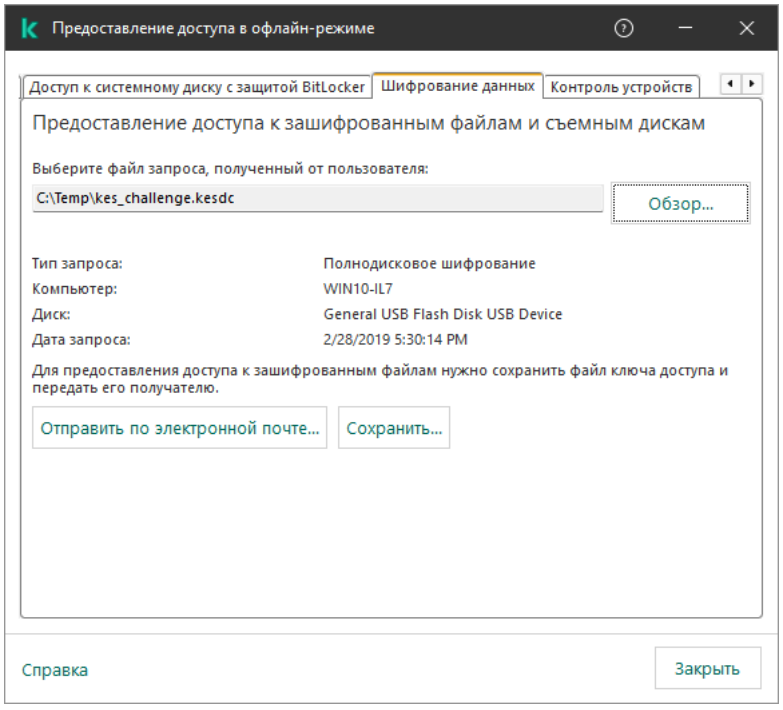
4. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.

5. В открывшемся окне выберите вкладку **Шифрование данных**.

6. На вкладке **Шифрование данных** нажмите на кнопку **Обзор**.

7. В окне выбора файла запроса укажите путь к файлу, полученного от пользователя.

Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.



Предоставление доступа в офлайн-режиме

Как получить файл ключа доступа к зашифрованным данным в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.

2. Установите флажок рядом с именем компьютера, доступ к данным которого вы хотите восстановить.

3. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.

4. Выберите раздел **Шифрование данных**.

5. Нажмите на кнопку **Выбрать файл** и выберите файл запроса, полученный от пользователя (файл с расширением kesdc).

   Web Console покажет информацию о запросе. В том числе, имя компьютера, на котором пользователь запрашивает доступ к файлу.

6. Нажмите на кнопку **Сохранить ключ** и выберите папку для сохранения файла ключа доступа к зашифрованным данным (файл с расширением kesdr).

В результате вам будет доступен ключ доступа к зашифрованным данным, который нужно будет передать пользователю.

После получения файла ключа доступа к зашифрованным данным пользователю нужно запустить файл двойным щелчком мыши. В результате Kaspersky Endpoint Security предоставит доступ ко всем зашифрованным файлам, хранящимся диске. Для получения доступа к зашифрованным файлам, хранящимся на других дисках, требуется получить отдельные ключи доступа для этих дисков.

Восстановление доступа к зашифрованным данным в случае выхода из строя операционной системы

Восстановление доступа к данным в случае выхода из строя операционной системы доступно только при шифровании файлов (FLE). Восстановить доступ к данным при полнодисковом шифровании (FDE) невозможно.

Чтобы восстановить доступ к зашифрованным данным в случае выхода из строя операционной системы, выполните следующие действия:

1. Переустановите операционную систему, не форматируя жесткий диск.
2. Установите Kaspersky Endpoint Security.
3. Установите связь между компьютером и Сервером администрирования Kaspersky Security Center, под управлением которого находился компьютер во время шифрования данных.

Доступ к зашифрованным данным будет предоставлен на тех же условиях, которые действовали до выхода операционной системы из строя.

Изменение шаблонов сообщений для получения доступа к зашифрованным файлам

Чтобы изменить шаблоны сообщений для получения доступа к зашифрованным файлам, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных → Общие настройки шифрования**.
4. В блоке **Шаблоны** нажмите на кнопку **Шаблоны**.

5. В открывшемся окне выполните следующие действия:

- Если вы хотите изменить шаблон сообщения пользователя, выберите вкладку **Сообщение пользователя**. Когда пользователь обращается к зашифрованному файлу при отсутствии на компьютере ключа доступа к зашифрованным файлам, открывается окно (см. рис. ниже). При нажатии на кнопку **Отправить письмом** автоматически формируется сообщение пользователя. Это сообщение отправляется администратору локальной сети организации вместе с файлом запроса доступа к зашифрованным файлам.

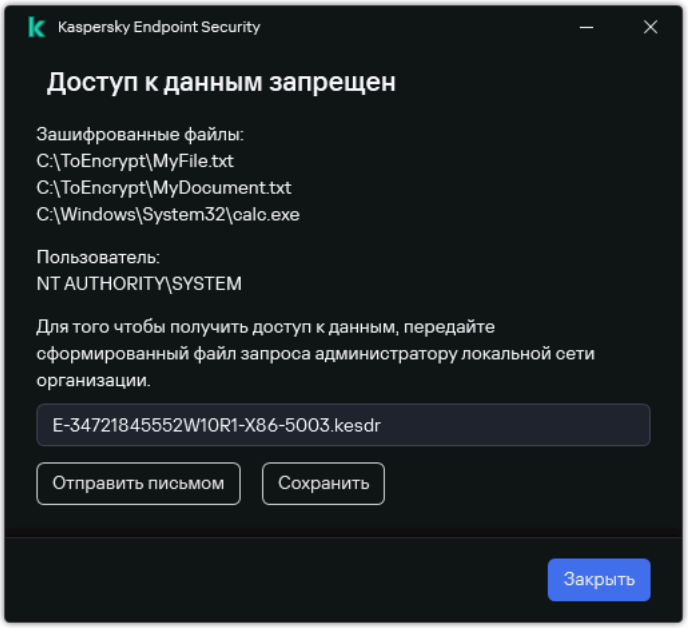
- Если вы хотите изменить шаблон сообщения администратора, выберите вкладку **Сообщение администратора**. Это сообщение приходит к пользователю после предоставления ему доступа к зашифрованным файлам.

6. Измените шаблоны сообщений.

   Для добавления переменной в текст шаблона установите курсор в требуемое место, нажмите на кнопку **Переменная** и выберите нужную переменную из списка доступных.

   Также вы можете восстановить текст шаблона по умолчанию с помощью кнопки **По умолчанию**.

7. Сохраните внесенные изменения.



Восстановление доступа к зашифрованным файлам

Шифрование съемных дисков

Шифрование съемных дисков не поддерживается на компьютерах с Arm-архитектурой.

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов.

Kaspersky Endpoint Security поддерживает шифрование файлов в файловых системах FAT32 и NTFS. Если к компьютеру подключен съемный диск с неподдерживаемой файловой системой, то шифрование этого съемного диска завершается с ошибкой и Kaspersky Endpoint Security устанавливает статус доступа "только чтение" для этого съемного диска.

Для защиты данных на съемных дисках вы можете использовать следующие виды шифрования:

- Полнодисковое шифрование (англ. Full Disk Encryption, FDE).

  Шифрование всего съемного диска, включая файловую систему.

  Получить доступ к зашифрованным данным вне корпоративной сети невозможно. Также невозможно получить доступ к зашифрованным данным внутри корпоративной сети, если компьютер не подключен к Kaspersky Security Center ("гостевой" компьютер).

- Шифрование файлов (англ. File Level Encryption, FLE).

  Шифрование только файлов на съемном диске. Файловая система при этом остается без изменений.

  Шифрование файлов на съемных дисках предоставляет возможность доступа к данным за пределами корпоративной сети с помощью специального режима – *портативный режим*.

Во время шифрования Kaspersky Endpoint Security создает мастер-ключ. Kaspersky Endpoint Security сохраняет мастер-ключ в следующих хранилищах:

- Kaspersky Security Center.
- Компьютер пользователя.

  Мастер-ключ зашифрован секретным ключом пользователя.

- Съемный диск.

  Мастер-ключ зашифрован открытым ключом Kaspersky Security Center.

После завершения шифрования данные на съемном диске доступны внутри корпоративной сети как при использовании обычного съемного диска без шифрования.

Получение доступа к зашифрованным данным

При подключении съемного диска с зашифрованными данными Kaspersky Endpoint Security выполняет следующие действия:

1. Проверяет наличие мастер-ключа в локальном хранилище на компьютере пользователя.

   Если мастер-ключ найден, пользователь получает доступ к данным на съемном диске.

   Если мастер-ключ не найден, Kaspersky Endpoint Security выполняет следующие действия:

   a. Отправляет запрос в Kaspersky Security Center.

      После получения запроса Kaspersky Security Center отправляет ответ, который содержит мастер-ключ.

   b. Kaspersky Endpoint Security сохраняет мастер-ключ в локальном хранилище на компьютере пользователя для дальнейшей работы с зашифрованным съемным диском.

2. Расшифровывает данные.

Особенности шифрования съемных дисков

Шифрование съемных дисков имеет следующие особенности:

- Политика с заданными параметрами шифрования съемных дисков формируется для определенной группы управляемых компьютеров. Поэтому результат применения политики Kaspersky Security Center с настроенным шифрованием / расшифровкой съемных дисков зависит от того, к какому компьютеру подключен съемный диск.
- Kaspersky Endpoint Security не выполняет шифрование / расшифровку файлов со статусом доступа "только чтение", хранящихся на съемных дисках.
- В качестве съемных дисков поддерживаются следующие типы устройств:
  - носители информации, подключаемые по шине USB;
  - жесткие диски, подключаемые по шинам USB и FireWire;
  - SSD-диски, подключаемые по шинам USB и FireWire.

Запуск шифрования съемных дисков

Вы можете расшифровать съемный диск с помощью политики. Политика с заданными параметрами шифрования съемных дисков формируется для определенной группы администрирования. Поэтому результат расшифровки данных на съемных дисках зависит от того, к какому компьютеру подключен съемный диск.

Kaspersky Endpoint Security поддерживает шифрование файлов в файловых системах FAT32 и NTFS. Если к компьютеру подключен съемный диск с неподдерживаемой файловой системой, то шифрование этого съемного диска завершается с ошибкой и Kaspersky Endpoint Security устанавливает статус доступа "только чтение" для этого съемного диска.

Перед шифрованием файлов на съемном диске убедитесь, что диск отформатирован и отсутствуют скрытые разделы (например, системный раздел EFI). Если на диске есть неотформатированные или скрытые разделы, шифрование файлов может завершиться с ошибкой.

Чтобы зашифровать съемные диски, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных** → **Шифрование съемных дисков**.
4. В раскрывающемся списке **Режим шифрования** выберите действие, которое по умолчанию выполняет Kaspersky Endpoint Security со съемными дисками:

   - **Шифровать весь съемный диск** (FDE). Kaspersky Endpoint Security посекторно шифрует содержимое съемного диска. Таким образом, зашифрованными оказываются не только файлы, которые хранятся на съемном диске, но и файловые системы, включая имена файлов и структуры папок на съемном диске.
   - **Шифровать все файлы** (FLE). Kaspersky Endpoint Security шифрует все файлы, которые хранятся на съемных дисках. Приложение не шифрует файловые системы съемных дисков, включая имена файлов и структуры папок.
   - **Шифровать только новые файлы** (FLE). Kaspersky Endpoint Security шифрует только те файлы, которые были добавлены на съемные диски или которые хранились на съемных дисках и были изменены после последнего применения политики Kaspersky Security Center.

   Kaspersky Endpoint Security повторно не шифрует уже зашифрованный съемный диск.

5. Если вы хотите использовать портативный режим для шифрования съемных дисков, установите флажок **Портативный режим**.

   Портативный режим – режим шифрования файлов (FLE) на съемных дисках, который предоставляет возможность доступа к данным за пределами корпоративной сети. Также портативный режим позволяет работать с зашифрованными данными на компьютерах, на которых не установлено приложение Kaspersky Endpoint Security.

6. Если вы хотите зашифровать новый съемный диск, рекомендуется установить флажок **Шифровать только занятое пространство**. Если флажок снят, Kaspersky Endpoint Security зашифрует все файлы, в том числе остатки удаленных или измененных файлов.

7. Если вы хотите настроить шифрование для отдельных съемных дисков, задайте правила шифрования.

8. Если вы хотите использовать полнодисковое шифрование съемных дисков в офлайн-режиме, установите флажок **Разрешать шифрование съемных дисков в офлайн-режиме**.

   Офлайн-режим шифрования – режим шифрования съемных дисков (FDE) при отсутствии связи с Kaspersky Security Center. При шифровании Kaspersky Endpoint Security сохраняет мастер-ключ только на компьютере пользователя. Kaspersky Endpoint Security отправит мастер-ключ в Kaspersky Security Center при следующей синхронизации.

   > Если компьютер, на котором сохранен мастер-ключ, поврежден и данные в Kaspersky Security Center не отправлены, получить доступ к съемному диску невозможно.

   Если флажок **Разрешать шифрование съемных дисков в офлайн-режиме** снят и подключение к Kaspersky Security Center отсутствует, шифрование съемного диска невозможно.

9. Сохраните внесенные изменения.

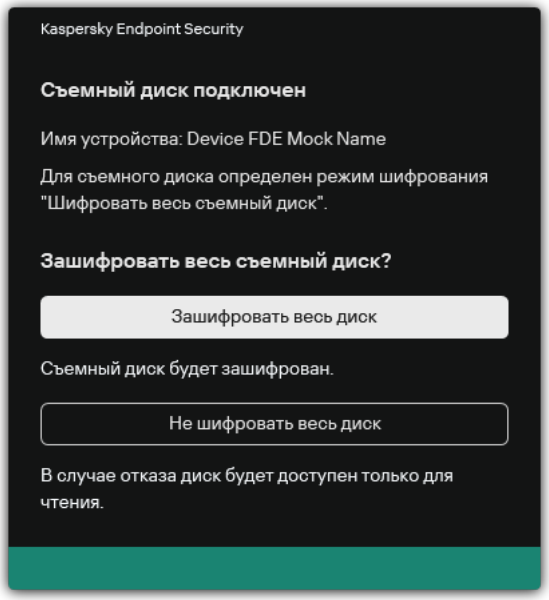
В результате применения политики, если пользователь подключает съемный диск или съемный диск уже подключен, Kaspersky Endpoint Security запрашивает подтверждение для выполнения операции шифрования (см. рис. ниже).

Приложение позволяет выполнить следующие действия:

- Если пользователь подтверждает запрос на шифрование, Kaspersky Endpoint Security шифрует данные.
- Если пользователь отклоняет запрос на шифрование, Kaspersky Endpoint Security оставляет данные без изменений и устанавливает для этого съемного диска право доступа "только чтение".
- Если пользователь не отвечает на запрос на шифрование, Kaspersky Endpoint Security оставляет данные без изменений и устанавливает для этого съемного диска право доступа "только чтение". Приложение повторно запрашивает подтверждение при последующем применении политики или при последующем подключении этого съемного диска.

Если во время шифрования данных пользователь инициирует безопасное извлечение съемного диска, Kaspersky Endpoint Security прерывает шифрование данных и позволяет извлечь съемный диск до завершения операции шифрования. Шифрование данных будет продолжено при следующем подключении съемного диска к этому компьютеру.

Если шифрование съемного диска не удалось, просмотрите отчет **Шифрование данных** в интерфейсе Kaspersky Endpoint Security. Доступ к файлам может быть заблокирован другим приложением. В этом случае попробуйте извлечь и заново подключить съемный диск к компьютеру.



Запрос на шифрование съемного диска

Добавление правила шифрования для съемных дисков

Чтобы добавить правило шифрования для съемных дисков, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных** → **Шифрование съемных дисков**.
4. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите один из следующих элементов:
   - Если вы хотите добавить правила шифрования для съемных дисков, которые находятся в списке доверенных устройств компонента Контроль устройств, выберите элемент **Из списка доверенных устройств данной политики**.
   - Если вы хотите добавить правила шифрования для съемных дисков, которые находятся в списке Kaspersky Security Center, выберите элемент **Из списка устройств Kaspersky Security Center**.
5. В раскрывающемся списке **Режим шифрования для выбранных устройств** выберите действие, которое выполняет Kaspersky Endpoint Security с файлами, хранящимися на выбранных съемных дисках.

6. Установите флажок **Портативный режим**, если вы хотите, чтобы перед шифрованием Kaspersky Endpoint Security выполнял подготовку съемных дисков к работе с зашифрованными на них файлами в портативном режиме.

   Портативный режим позволяет работать с зашифрованными файлами съемных дисков на компьютерах с недоступной функциональностью шифрования.

7. Установите флажок **Шифровать только занятое пространство**, если вы хотите, чтобы Kaspersky Endpoint Security шифровал только те секторы диска, которые заняты файлами.

   Если вы применяете шифрование на уже используемом диске, рекомендуется зашифровать весь диск. Это гарантирует защиту всех данных - даже удаленных, но еще содержащих извлекаемые сведения. Функцию **Шифровать только занятое пространство** рекомендуется использовать для новых, ранее не использовавшихся дисков.

   Если устройство было зашифровано ранее с использованием функции **Шифровать только занятое пространство**, после применения политики в режиме **Шифровать весь съемный диск** секторы, не занятые файлами, по-прежнему не будут зашифрованы.

8. В раскрывающемся списке **Действие для устройств, выбранных ранее** выберите действие, выполняемое Kaspersky Endpoint Security с правилами шифрования, которые были определены для съемных дисков ранее:

   - Если вы хотите, чтобы созданное ранее правило шифрования съемного диска осталось без изменений, выберите элемент **Пропустить**.
   - Если вы хотите, чтобы созданное ранее правило шифрования съемного диска было заменено новым правилом, выберите элемент **Обновить**.

9. Сохраните внесенные изменения.

Добавленные правила шифрования съемных дисков будут применены к съемным дискам, подключенным к любым компьютерам организации.

Экспорт и импорт списка правил шифрования для съемных дисков

Вы можете экспортировать список правил шифрования для съемных дисков в файл в формате XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество правил для однотипных съемных дисков. Также вы можете использовать функцию экспорта / импорта для резервного копирования списка правил или для миграции правил на другой сервер.

Как экспортировать / импортировать список правил шифрования для съемных дисков в Консоли администрирования (MMC)

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Шифрование данных → Шифрование съемных дисков**.

5. В блоке **Правила шифрования выбранных устройств** перейдите по ссылке **<N> правил**.

   Откроется список правил шифрования для съемных дисков.

6. Для экспорта списка правил шифрования для съемных дисков, выполните следующие действия:

   a. Выберите правила, которые вы хотите экспортировать.

   b. Нажмите на кнопку **Экспортировать**.

   c. Подтвердите, что вы хотите экспортировать только выбранные правила, или экспортируйте весь список.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл в папку для загрузки по умолчанию.

7. Для импорта списка исключений, выполните следующие действия:

   a. Нажмите на ссылку **Импортировать**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

   b. Откройте файл.

      Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

8. Сохраните внесенные изменения.

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Шифрование данных → Шифрование съемных дисков**.

4. Для экспорта списка правил шифрования для съемных дисков, выполните следующие действия:

   a. Выберите правила, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

      Если вы не выбрали ни одного правила, Kaspersky Endpoint Security экспортирует все правила.

   b. Нажмите на ссылку **Экспортировать**.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список правил, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл.

5. Для импорта списка правил шифрования для съемных дисков, выполните следующие действия:

   a. Нажмите на ссылку **Импортировать**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

b. Откройте файл.

Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

6. Сохраните внесенные изменения.

Портативный режим для работы с зашифрованными файлами на съемных дисках

Портативный режим – режим шифрования файлов (FLE) на съемных дисках, который предоставляет возможность доступа к данным за пределами корпоративной сети. Также портативный режим позволяет работать с зашифрованными данными на компьютерах, на которых не установлено приложение Kaspersky Endpoint Security.

Портативный режим удобно использовать в следующих случаях:

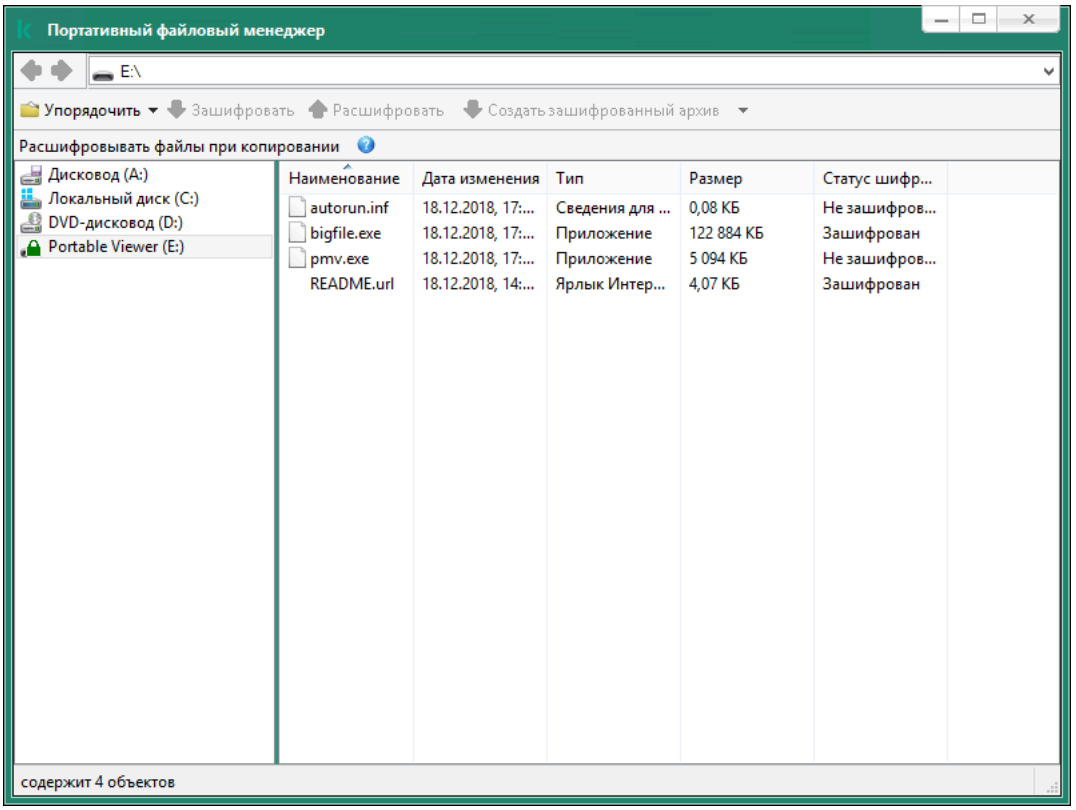
- Нет связи между компьютером и Сервером администрирования Kaspersky Security Center.
- Изменилась инфраструктура со сменой Сервера администрирования Kaspersky Security Center.
- На компьютере не установлено приложение Kaspersky Endpoint Security.

Портативный файловый менеджер

Для работы в портативном режиме Kaspersky Endpoint Security устанавливает на съемный диск специальный модуль шифрования – *портативный файловый менеджер*. Портативный файловый менеджер предоставляет интерфейс для работы с зашифрованными данными, если на компьютере не установлено приложение Kaspersky Endpoint Security (см. рис. ниже). Если на компьютере установлено приложение Kaspersky Endpoint Security, вы можете работать с зашифрованными съемными дисками с помощью обычных файлового менеджера (например, Проводника).

Портативный файловый менеджер хранит ключ для шифрования файлов на съемном диске. Ключ зашифрован паролем пользователя. Пользователь задает пароль перед шифрованием файлов на съемном диске.

Портативный файловый менеджер запускается автоматически при подключении съемного диска к компьютеру, на котором не установлено приложение Kaspersky Endpoint Security. Если на компьютере выключен автозапуск приложения, запустите портативный файловый менеджер вручную. Для этого запустите файл pmv.exe, который хранится на съемном диске.



Портативный файловый менеджер

Поддержка портативного режима для работы с зашифрованным файлами

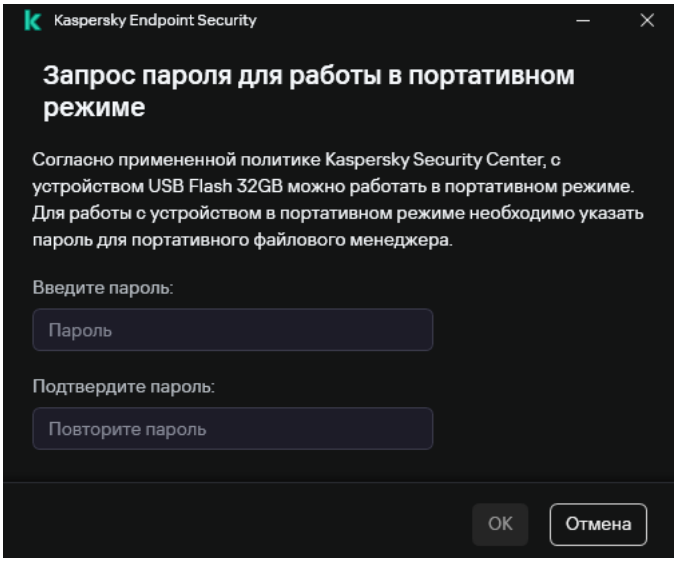
Как включить поддержку портативного режима для работы с зашифрованными файлами на съемных дисках в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных → Шифрование съемных дисков**.
4. В раскрывающемся списке **Режим шифрования для выбранных устройств** выберите элемент **Шифровать все файлы** или элемент **Шифровать только новые файлы**.

   Портативный режим доступен только при шифрования файлов (FLE). Включить поддержку портативного режима для полнодискового шифрования (FDE) невозможно.

5. Установите флажок **Портативный режим**.
6. Если нужно, добавьте правила шифрования для отдельных съемных дисков.
7. Сохраните внесенные изменения.
8. После применения политики подключите съемный диск к компьютеру.
9. Подтвердите операцию шифрования съемного диска.

Откроется окно создания пароля для портативного файлового менеджера.



Запрос пароля для работы в портативном режиме

10. Задайте пароль, соответствующий требованиям к уровню сложности, и подтвердите его.
11. Сохраните внесенные изменения.

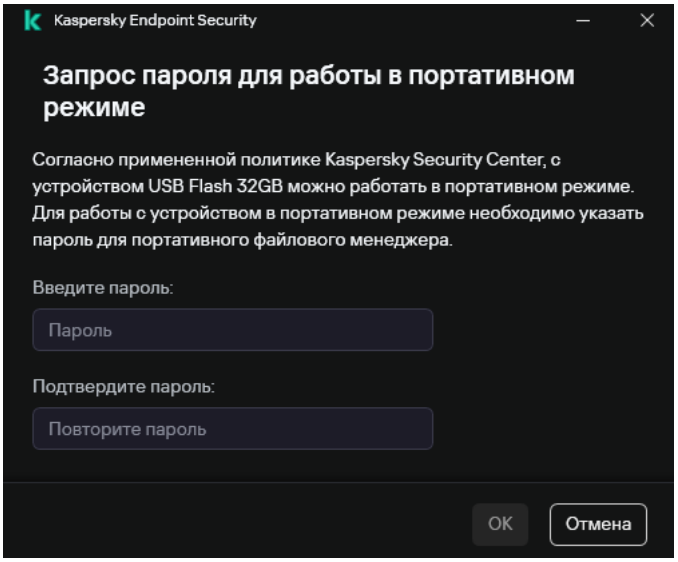
Как включить поддержку портативного режима для работы с зашифрованными файлами на съемных дисках в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Шифрование данных** → **Шифрование съемных дисков**.
5. В блоке **Действие по умолчанию** выберите элемент **Шифровать все файлы** или элемент **Шифровать только новые файлы**.

   Портативный режим доступен только при шифрования файлов (FLE). Включить поддержку портативного режима для полнодискового шифрования (FDE) невозможно.
6. Установите флажок **Портативный режим**.
7. Если нужно, добавьте правила шифрования для отдельных съемных дисков.
8. Сохраните внесенные изменения.
9. После применения политики подключите съемный диск к компьютеру.
10. Подтвердите операцию шифрования съемного диска.

Откроется окно создания пароля для портативного файлового менеджера.



Запрос пароля для работы в портативном режиме

11. Задайте пароль, соответствующий требованиям к уровню сложности, и подтвердите его.

12. Сохраните внесенные изменения.

Kaspersky Endpoint Security зашифрует файлы на съемном диске. Портативный файловый менеджер для работы с зашифрованными файлами будет также добавлен на съемный диск. Если на съемном диске уже есть зашифрованные файлы, то Kaspersky Endpoint Security зашифрует их повторно с помощью собственного ключа. Это позволяет пользователю получить доступ ко всем файлам на съемном диске в портативном режиме.

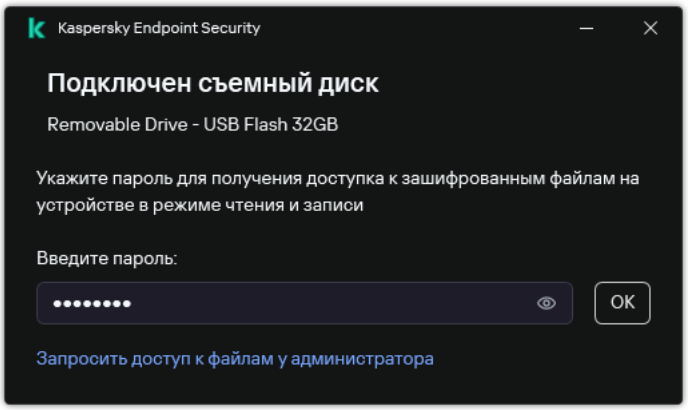
Получение доступа к зашифрованным файлам на съемном диске

После шифрования файлов на съемном диске с поддержкой портативного режима доступны следующие способы доступа к файлам:

- Если на компьютере не установлено приложение Kaspersky Endpoint Security, портативный файловый менеджер предложит ввести пароль. Пароль нужно будет вводить при каждой перезагрузке компьютера или переподключении съемного диска.

- Если компьютер находится за пределами корпоративной сети и на компьютере установлено приложение Kaspersky Endpoint Security, приложение предложит ввести пароль или отправить запрос на доступ к файлам администратору. После получения доступа к файлам на съемном диске Kaspersky Endpoint Security сохранит секретный ключ в хранилище ключей компьютера. Это позволит в дальнейшем получить доступ к файлам без ввода пароля или запроса администратору (см. рис. ниже).

- Если компьютер находится внутри корпоративной сети и на компьютере установлено приложение Kaspersky Endpoint Security, вы получите доступ к устройству без ввода пароля. Kaspersky Endpoint Security получит секретный ключ от Сервера администрирования Kaspersky Security Center к которому подключен компьютер.



Получение доступа к зашифрованным файлам на съемном диске

Восстановление пароля для работы в портативном режиме

Если вы забыли пароль для работы в портативном режиме, вам нужно подключить съемный диск к компьютеру с установленным приложением Kaspersky Endpoint Security внутри корпоративной сети. Вы получите доступ к файлам, так как в хранилище ключей компьютера или на Сервере администрирования сохранен секретный ключ. Расшифруйте и снова зашифруйте файлы с новым паролем.

Особенности работы портативного режима при подключении съемного диска к компьютеру из другой сети

Если компьютер находится за пределами корпоративной сети и на компьютере установлено приложение Kaspersky Endpoint Security, вы можете получить доступ к файлам следующими способами:

- **Доступ по паролю**

  После ввода пароля вы сможете просматривать, изменять и сохранять файлы на съемном диске (*прозрачный доступ*). Kaspersky Endpoint Security может установить для съемного диска право доступа "только чтение", если в параметрах политики для шифрования съемных дисков настроены следующие параметры:

  - Выключена поддержка портативного режима.
  - Выбран режим **Шифровать все файлы** или **Шифровать только новые файлы**.

  В остальных случаях вы получите полный доступ к съемному диску (право "чтение и запись"). Вам будет доступно добавление и удаление файлов.

  Вы можете изменить права доступа к съемному диску, даже если съемный диск подключен к компьютеру. Если права доступа к съемному диску изменились, Kaspersky Endpoint Security заблокирует доступ к файлам и запросит пароль повторно.

  После ввода пароля применить параметры политики шифрования для съемного диска невозможно. Таким образом, расшифровать или перешифровать файлы на съемном диске невозможно.

- **Запрос доступа к файлам у администратора**

  Если вы забыли пароль для работы в портативном режиме, запросите доступ к файлам у администратора. Для доступа к файлам пользователю нужно отправить файл запроса (файл с расширением kesdc) администратору. Пользователь можете отправить файл запроса, например, по электронной почте. Администратор отправит файл доступа к зашифрованным данным (файл с расширением kesdr).

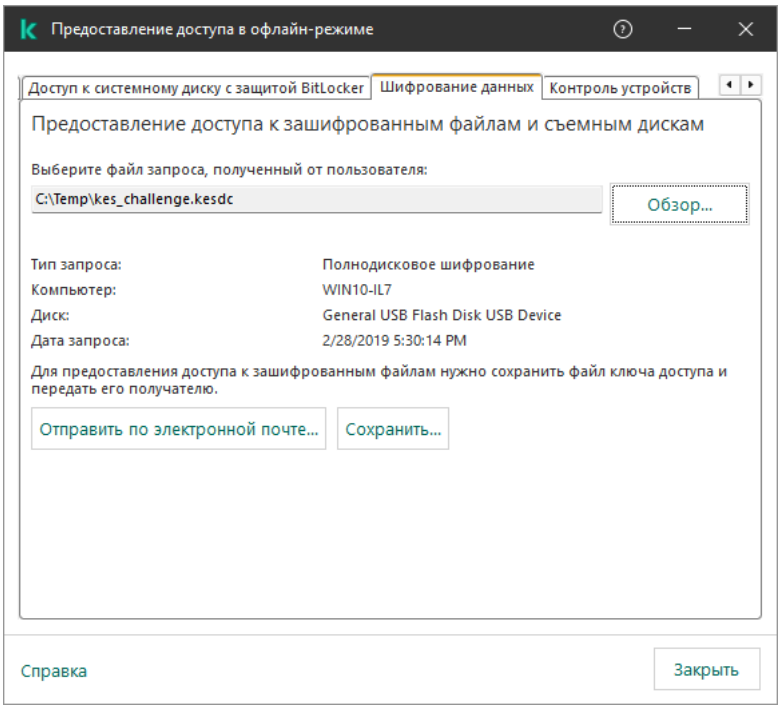
  После прохождения процедуры восстановления пароля ("Запрос - Ответ") вы получите прозрачный доступ к файлам на съемном диске и полный доступ к съемному диску (право "запись и чтение").

  Вы можете применить политику для шифрования съемных дисков и, например, расшифровать файлы. После восстановления пароля или при обновлении политики приложение Kaspersky Endpoint Security предложит подтвердить изменения.

  Как получить файл доступа к зашифрованным данным в Консоли администрирования (MMC)

  1. Откройте Консоль администрирования Kaspersky Security Center.
  2. В дереве консоли выберите папку **Устройства**.
  3. На вкладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
  4. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
  5. В открывшемся окне выберите вкладку **Шифрование данных**.
  6. На вкладке **Шифрование данных** нажмите на кнопку **Обзор**.
  7. В окне выбора файла запроса укажите путь к файлу, полученного от пользователя.

     Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.



Предоставление доступа в офлайн-режиме

Как получить файл доступа к зашифрованным данным в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.
2. Установите флажок рядом с именем компьютера, доступ к данным которого вы хотите восстановить.
3. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.
4. Выберите раздел **Шифрование данных**.
5. Нажмите на кнопку **Выбрать файл** и выберите файл запроса, полученный от пользователя (файл с расширением kesdc).

   Web Console покажет информацию о запросе. В том числе, имя компьютера, на котором пользователь запрашивает доступ к файлу.
6. Нажмите на кнопку **Сохранить ключ** и выберите папку для сохранения файла ключа доступа к зашифрованным данным (файл с расширением kesdr).

В результате вам будет доступен ключ доступа к зашифрованным данным, который нужно будет передать пользователю.

Расшифровка съемных дисков

Вы можете расшифровать съемный диск с помощью политики. Политика с заданными параметрами шифрования съемных дисков формируется для определенной группы администрирования. Поэтому результат расшифровки данных на съемных дисках зависит от того, к какому компьютеру подключен съемный диск.

Чтобы расшифровать съемные диски, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Шифрование данных** → **Шифрование съемных дисков**.
4. Если вы хотите расшифровать все зашифрованные файлы, хранящиеся на съемных дисках, в раскрывающемся списке **Режим шифрования** выберите действие **Расшифровывать весь съемный диск**.

5. Если вы хотите расшифровать данные, хранящиеся на отдельных съемных дисках, измените правила шифрования съемных дисков, данные которых вы хотите расшифровать. Для этого выполните следующие действия:

   a. В списке съемных дисков, для которых определены правила шифрования, выберите запись о нужном вам съемном диске.

   b. Нажмите на кнопку **Задать правило**, чтобы изменить правило шифрования для этого съемного диска.

   c. В контекстном меню кнопки **Задать правило** выберите пункт **Расшифровывать весь съемный диск**.

6. Сохраните внесенные изменения.

В результате, если пользователь подключает съемный диск или он уже подключен, Kaspersky Endpoint Security расшифровывает съемный диск. Приложение предупреждает пользователя, что процедура расшифровки может занять некоторое время. Если во время расшифровки данных пользователь инициирует безопасное извлечение съемного диска, Kaspersky Endpoint Security прерывает расшифровку данных и позволяет извлечь съемный диск до завершения операции расшифровки. Расшифровка данных будет продолжена после следующего подключение съемного диска к компьютеру.

Если расшифровка съемного диска не удалась, просмотрите отчет **Шифрование данных** в интерфейсе Kaspersky Endpoint Security. Доступ к файлам может быть заблокирован другим приложением. В этом случае попробуйте извлечь и заново подключить съемный диск к компьютеру.

Просмотр информации о шифровании данных

В процессе шифрования и расшифровки данных Kaspersky Endpoint Security отправляет на Kaspersky Security Center информацию о статусах применения параметров шифрования на клиентских компьютерах.

Просмотр статусов шифрования

Вы можете контролировать шифрование данных с помощью статуса. Kaspersky Endpoint Security назначает следующие статусы шифрования:

- **Не соответствует политике; отменено пользователем**. Пользователь отменил шифрование данных.
- **Не соответствует политике из-за ошибки**. Ошибка шифрования данных, например, из-за отсутствия лицензии.
- **Применение политики. Требуется перезагрузка**. На компьютере выполняется шифрование данных. Для завершения шифрования данных необходимо перезагрузить компьютер.
- **Не задана политика шифрования**. Шифрование данных выключено в параметрах политики.
- **Не поддерживается**. На компьютере не установлены компоненты шифрования.
- **Применение политики**. На компьютере выполняется шифрование или расшифровка данных.

Чтобы просмотреть статус шифрования данных компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Управляемые устройства**.
3. На вкладке **Устройства** в рабочей области сдвиньте полосу прокрутки до упора вправо. Если графа **Статус шифрования** не отображается, добавьте графу в параметрах консоли Kaspersky Security Center.

   В графе **Статус шифрования** отображаются статусы шифрования данных для компьютеров выбранной группы администрирования. Этот статус формируется на основе информации о шифровании файлов на локальных дисках компьютера и полнодисковом шифровании.
4. Если статус шифрования данных компьютера **В процессе применения политики**, вы можете контролировать панель прогресса шифрования:

   a. Откройте свойства компьютера со статусом **В процессе применения политики** двойным щелчком мыши.

   b. В окне свойств компьютера выберите раздел **Программы**.

   c. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows**.

   d. Нажмите на кнопку **Статистика**.

   e. В блоке **Шифрование устройств** отображается текущее состояние шифрования данных в процентах.

Просмотр статистики шифрования на информационных панелях Kaspersky Security Center

Чтобы просмотреть статусы шифрования на информационных панелях Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите узел **Сервер администрирования**.
3. В рабочей области, расположенной справа от дерева Консоли администрирования, выберите вкладку **Статистика**.
4. Создайте новую страницу с информационными панелями со статистикой шифрования данных. Для этого выполните следующие действия:

   a. На вкладке **Статистика** нажмите на кнопку **Настроить вид**.

   b. В открывшемся окне нажмите на кнопку **Добавить**.

   c. В открывшемся окне в разделе **Общие** введите название страницы.

   d. В разделе **Информационные панели** нажмите на кнопку **Добавить**.

   e. В открывшемся окне в группе **Состояние защиты** выберите элемент **Шифрование устройств**.

f. Нажмите на кнопку **OK**.

g. В открывшемся окне измените при необходимости параметры информационной панели. Для этого воспользуйтесь разделами **Вид** и **Устройства**.

h. Нажмите на кнопку **OK**.

i. Повторите пункты d – h инструкции, при этом в группе **Состояние защиты** выберите элемент **Шифрование съемных дисков**.

Добавленные информационные панели отобразятся в списке **Информационные панели**.

j. Нажмите на кнопку **OK**.

Название созданной на предыдущих шагах страницы с информационными панелями отобразится в списке **Страницы**.

k. Нажмите на кнопку **Закрыть**.

5. На вкладке **Статистика** откройте страницу, созданную на предыдущих шагах инструкции.

Отобразятся информационные панели, на которых вы можете просмотреть статусы шифрования компьютеров и съемных дисков.

Просмотр ошибок шифрования файлов на локальных дисках компьютера

Чтобы просмотреть ошибки шифрования файлов на локальных дисках компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите папку **Управляемые устройства**.

3. На вкладке **Устройства** выделите в списке компьютер и по правой клавише мыши вызовите контекстное меню.

4. В контекстном меню компьютера выберите пункт **Свойства**. В открывшемся окне выберите раздел **Защита**.

5. По ссылке **Просмотреть ошибки шифрования данных** откройте окно **Ошибки шифрования данных**.

В этом окне отображается информация об ошибках шифрования файлов на локальных дисках компьютера. Если ошибка исправлена, то Kaspersky Security Center удаляет информацию о ней из окна **Ошибки шифрования данных**.

Просмотр отчета о шифровании данных

Kaspersky Security Center позволяет создавать отчеты о шифровании данных:

- **Отчет о статусе шифрования управляемых устройств**. Отчет содержит информацию о том, соответствует ли состояние шифрования компьютера политике шифрования.
- **Отчет о статусе шифрования запоминающих устройств**. Отчет содержит информацию о статусе шифрования внешних устройств и запоминающих устройств.
- **Отчет о правах доступа к зашифрованным жестким дискам**. Отчет содержит информацию о состоянии учетных записей, имеющих доступ к зашифрованным дискам.
- **Отчет об ошибках шифрования файлов**. Отчет содержит информацию об ошибках, которые возникли при выполнении задач шифрования или расшифровки данных на компьютерах.
- **Отчет о блокировании доступа к зашифрованным файлам**. Отчет содержит информацию о блокировке доступа приложений к зашифрованным файлам.

Чтобы просмотреть отчет о шифровании данных, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите вкладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**.

   Запустится мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. В окне **Выбор типа шаблона отчета** в разделе **Другое** выберите один из отчетов о шифровании данных.

   После завершения работы мастера создания шаблона отчета в таблице на вкладке **Отчеты** появится новый шаблон отчета.
5. Выберите шаблон отчета, созданный на предыдущих шагах инструкции.
6. В контекстном меню шаблона выберите пункт **Показать отчет**.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Работа с зашифрованными устройствами при отсутствии доступа к ним

Получение доступа к зашифрованным устройствам

Пользователю может потребоваться запросить доступ к зашифрованным устройствам в следующих случаях:

- Жесткий диск был зашифрован на другом компьютере.
- На компьютере нет ключа шифрования для устройства (например, в момент первого обращения к зашифрованному съемному диску на этом компьютере), и связь с Kaspersky Security Center отсутствует.

  После того как пользователь применил ключ доступа к зашифрованному устройству, Kaspersky Endpoint Security сохраняет ключ шифрования на компьютере пользователя и предоставляет доступ к этому устройству при последующих обращениях, даже если связь с Kaspersky Security Center отсутствует.

Получение доступа к зашифрованным устройствам осуществляется следующим образом:

1. Пользователь создает через интерфейс приложения Kaspersky Endpoint Security файл запроса доступа с расширением kesdc и передает его администратору локальной сети организации.
2. Администратор создает в Консоли администрирования Kaspersky Security Center файл ключа доступа с расширением kesdr и передает его пользователю.
3. Пользователь применяет ключ доступа.

Восстановление данных на зашифрованных устройствах

Для работы с зашифрованными устройствами пользователь может использовать утилиту восстановления зашифрованных устройств (далее – "утилита восстановления"). Это может потребоваться в следующих случаях:

- Процедура получения доступа с помощью ключа доступа прошла неуспешно.
- На компьютере с зашифрованным устройством не установлены компоненты шифрования.

Данные, необходимые для восстановления доступа к зашифрованным устройствам с помощью утилиты восстановления, в течение некоторого времени находятся в памяти компьютера пользователя в открытом виде. Чтобы снизить вероятность несанкционированного доступа к этим данным, рекомендуется выполнять восстановление доступа к зашифрованным устройствам на доверенных компьютерах.

Восстановление данных на зашифрованных устройствах осуществляется следующим способом:

1. Пользователь создает с помощью утилиты восстановления файл запроса доступа с расширением fdertc и передает его администратору локальной сети организации.

2. Администратор создает в Консоли администрирования Kaspersky Security Center файл ключа доступа с расширением fdertr и передает его пользователю.

3. Пользователь применяет ключ доступа.

Для восстановления данных на зашифрованных системных жестких дисках пользователь также может указать в утилите восстановления учетные данные Агента аутентификации. Если метаданные учетной записи Агента аутентификации повреждены, то пользователю потребуется пройти процедуру восстановления с помощью файла запроса доступа.

Перед восстановлением данных на зашифрованных устройствах рекомендуется вывести компьютер, на котором будет выполняться процедура, из-под действия политики Kaspersky Security Center или отключить шифрование в параметрах политики Kaspersky Security Center. Это позволяет предотвратить повторное шифрование устройства.

Восстановление данных с помощью утилиты восстановления FDERT

При неисправности жесткого диска файловая система может быть повреждена. Таким образом, данные, защищенные технологией Шифрование диска Kaspersky, будут недоступны. Вы можете расшифровать данные и скопировать данные на новый диск.

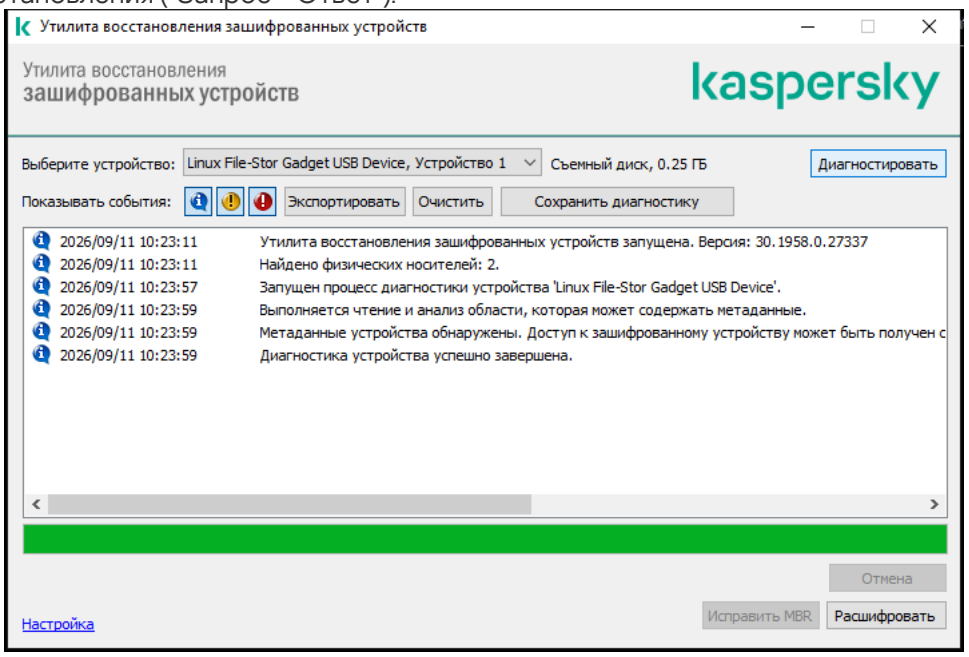
Восстановление данных на диске, защищенные технологией Шифрование диска Kaspersky, состоит из следующих этапов:

1. Создание автономной утилиты восстановления (см. рис. ниже).

2. Подключение диска к компьютеру, на котором отсутствуют компоненты шифрования Kaspersky Endpoint Security.

3. Запуск утилиты восстановления и диагностика жесткого диска.

4. Доступ к данным на диске. Для этого нужно ввести учетные данные Агента аутентификации или запустить процедуру восстановления ("Запрос - Ответ").



Утилита восстановления FDERT

Создание автономной утилиты восстановления

Чтобы создать исполняемый файл утилиты восстановления, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Восстановление зашифрованного устройства**.

   Запустится утилита восстановления зашифрованных устройств.
3. В окне утилиты восстановления нажмите на кнопку **Создать автономную утилиту восстановления**.
4. Сохраните автономную утилиту восстановления в память компьютера.

В результате исполняемый файл утилиты восстановления fdert.exe будет сохранен в указанной папке. Скопируйте утилиту восстановления на компьютер, на котором отсутствуют компоненты шифрования Kaspersky Endpoint Security. Это позволяет предотвратить повторное шифрование диска.

Данные, необходимые для восстановления доступа к зашифрованным устройствам с помощью утилиты восстановления, в течение некоторого времени находятся в памяти компьютера пользователя в открытом виде. Чтобы снизить вероятность несанкционированного доступа к этим данным, рекомендуется выполнять восстановление доступа к зашифрованным устройствам на доверенных компьютерах.

Восстановление данных на жестком диске

Чтобы восстановить доступ к зашифрованному устройству с помощью утилиты восстановления, выполните следующие действия:

1. Запустите исполняемый файл утилиты восстановления fdert.exe, созданный с помощью приложения Kaspersky Endpoint Security.

2. В окне утилиты восстановления выберите зашифрованное устройство, доступ к которому вы хотите восстановить.

3. Нажмите на кнопку **Диагностировать**, чтобы утилита могла определить, какое действие следует выполнить с зашифрованным устройством: разблокировать или расшифровать.

   Если на компьютере доступна функциональность шифрования Kaspersky Endpoint Security, то утилита восстановления предлагает разблокировать устройство. При разблокировке устройство не расшифровывается, но к нему в результате предоставляется прямой доступ. Если на компьютере недоступна функциональность шифрования Kaspersky Endpoint Security, то утилита восстановления предлагает расшифровать устройство.

4. Если вы хотите импортировать диагностическую информацию, нажмите на кнопку **Сохранить диагностику**.

   Утилита сохранит архив с файлами с диагностической информацией.

5. Нажмите на кнопку **Исправить MBR**, если в результате диагностики зашифрованного системного жесткого диска вы получили сообщение о каких-либо проблемах, связанных с главной загрузочной записью (MBR) устройства.

   Исправление главной загрузочной записи устройства может ускорить получение информации, необходимой для разблокировки или расшифровки устройства.

6. Нажмите на кнопку **Разблокировать** или **Расшифровать** в зависимости от результатов диагностики.

7. Если вы хотите восстановить данные с помощью учетной записи Агента аутентификации, выберите вариант **Использовать настройки учетной записи Агента аутентификации** и введите учетные данные Агента аутентификации.

   Этот способ возможен только при восстановлении данных на системном жестком диске. Если системный жесткий диск был поврежден и данные об учетной записи Агента аутентификации потеряны, то для восстановления данных на зашифрованном устройстве необходимо получить ключ доступа у администратора локальной сети организации.

8. Если вы хотите запустить процедуру восстановления, выполните следующие действия:

   a. Выберите вариант **Указать ключ доступа к устройству вручную**.

   b. Нажмите на кнопку **Получить ключ доступа** и сохраните файл запроса в память компьютера (файл с расширением fdertc).

   c. Передайте файл запроса доступа администратору локальной сети организации.

   Не закрывайте окно **Получение ключа доступа к устройству**, пока вы не получите ключ доступа. При повторном открытии этого окна созданный администратором ранее ключ доступа будет невозможно применить.

d. Получите и сохраните файл доступа (файл с расширением fdertr), созданный и переданный вам администратором локальной сети организации (см. инструкцию ниже).

e. Загрузите файл доступа в окне **Получение ключа доступа к устройству**.

9. Если вы выполняете расшифровку устройства, требуется настроить дополнительные параметры расшифровки:

   - Укажите область для расшифровки:

     - Если вы хотите расшифровать все устройство, выберите вариант **Расшифровать все устройство**.

     - Если вы хотите расшифровать часть данных на устройстве, выберите вариант **Расшифровать отдельные области устройства** и задайте границы области для расшифровки.

   - Выберите место записи расшифрованных данных:

     - Если вы хотите, чтобы данные на исходном устройстве были перезаписаны расшифрованными данными, снимите флажок **Расшифровка в файл образа диска**.

     - Если вы хотите сохранить расшифрованные данные отдельно от исходных зашифрованных данных, установите флажок **Расшифровка в файл образа диска** и с помощью кнопки **Обзор** укажите путь, по которому файл формата VHD должен быть сохранен.

10. Нажмите на кнопку **OK**.

Запустится процесс разблокировки / расшифровки устройства.

Как создать файл доступа к зашифрованным данным в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве Консоли администрирования выберите папку **Дополнительно → Шифрование и защита данных → Зашифрованные жесткие диски**.

3. В рабочей области выберите зашифрованное устройство, для которого вы хотите создать файл ключа доступа, и в контекстном меню устройства выберите пункт **Получить доступ к устройству в Kaspersky Endpoint Security для Windows**.

   Если вы не уверены, для какого компьютера был сформирован файл запроса доступа, в дереве Консоли администрирования выберите папку **Дополнительно → Шифрование и защита данных** и в рабочей области нажмите на ссылку **Получить ключ шифрования устройства в Kaspersky Endpoint Security для Windows**.

4. В открывшемся окне выберите используемый алгоритм шифрования: AES256 или AES56.

   Алгоритм шифрования данных зависит от библиотеки шифрования AES, входящей в состав дистрибутива: *Strong encryption (AES256)* или *Lite encryption (AES56)*. Библиотека шифрования AES устанавливается вместе с приложением.

5. Нажмите на кнопку **Обзор** и в открывшемся окне укажите путь к файлу запроса, полученного от пользователя, с расширением fdertc.

6. Нажмите на кнопку **Открыть**.

Отобразится информация о запросе пользователя. Kaspersky Security Center сформирует файл ключа доступа. Отправьте пользователю созданный файл ключа доступа к зашифрованным данным по электронной почте. Или сохраните файл доступа и передайте файл любым доступным способом.

Как создать файл доступа к зашифрованным данным в Web Console

1. В главном окне Web Console выберите **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

2. Установите флажок рядом с именем компьютера, данные на котором вы хотите восстановить.

3. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.

   Запустится мастер предоставления доступа к устройству.

4. Следуйте указаниям мастера предоставления доступа к устройству:

   a. Выберите плагин Kaspersky Endpoint Security для Windows.

   b. Выберите используемый алгоритм шифрования: AES256 или AES56.

      Алгоритм шифрования данных зависит от библиотеки шифрования AES, входящей в состав дистрибутива: *Strong encryption (AES256)* или *Lite encryption (AES56)*. Библиотека шифрования AES устанавливается вместе с приложением.

   c. Выберите файл запроса, полученного от пользователя (файл с расширением fdertc).

   d. Выберите папку для сохранения файла ключа доступа к зашифрованным данным (файл с расширением fdertr).

В результате вам будет доступен ключ доступа к зашифрованным данным, который нужно будет передать пользователю.

Создание диска аварийного восстановления операционной системы

Диск аварийного восстановления операционной системы может быть полезен в ситуации, когда по каким-либо причинам доступ к зашифрованному системному жесткому диску невозможен и операционная система не может быть загружена.

Вы можете загрузить образ операционной системы Windows с помощью диска аварийного восстановления и восстановить доступ к зашифрованному системному диску с помощью утилиты восстановления, включенной в состав образа операционной системы.

Чтобы создать диск аварийного восстановления операционной системы, выполните следующие действия:

1. Создайте исполняемый файл утилиты восстановления зашифрованных устройств.

2. Создайте пользовательский образ среды предустановки Windows. В процессе создания пользовательского образа среды предустановки Windows добавьте в образ исполняемый файл утилиты восстановления зашифрованных устройств.

3. Поместите пользовательский образ среды предустановки Windows на загрузочный носитель, например компакт-диск или съемный диск.

   Инструкцию о создании пользовательского образа среды предустановки Windows вы можете прочитать в справочной документации Microsoft (например, на ресурсе Microsoft TechNet).

Защита от сложных и целевых атак (встроенные агенты)

Решения Detection and Response от "Лаборатории Касперского" представляют собой системы безопасности, предназначенные для обнаружения сложных угроз и признаков атак на разных уровнях инфраструктуры организации. Решения Detection and Response предоставляют вам информацию об обнаруженной угрозе и позволяют управлять действиями по реагированию на обнаружения.

Таким образом, решения Detection and Response выполняют следующие действия:

- Получение данных о работе компьютера, сервера или других устройств (телеметрия).
- Автоматический анализ данных для выявления угроз.
- Формирование деталей алерта в виде граф цепочки развития угрозы для анализа и выбора действий по реагированию на обнаружение.
- Выполнение действий по реагированию на обнаружение (например, сетевая изоляция компьютера).

Kaspersky Endpoint Security обеспечивает работу решений Detection and Response с помощью встроенного в приложение агента. Встроенный агент отправляет телеметрию на серверы решений и выполняет действия по реагированию на обнаружение. Встроенный агент обеспечивает работу следующих решений:

- Kaspersky Managed Detection and Response (MDR);
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum);
- Kaspersky Endpoint Detection and Response Expert (EDR Expert);
- Kaspersky Anti Targeted Attack Platform:
  - Endpoint Detection and Response (EDR) версии 7.1 и ниже;
  - Network Detection and Response (NDR);
  - KATA Sandbox.
- Kaspersky Endpoint Detection and Response Expert (on-premises);
- Kaspersky Sandbox 2.0.

Вы можете использовать Kaspersky Endpoint Security с решениями Detection and Response в различных конфигурациях, например, [EDR Optimum+MDR].

Лицензирование MDR и EDR Optimum

Kaspersky Endpoint Security обеспечивает работу решений Kaspersky Managed Detection and Response (MDR) и Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) от "Лаборатории Касперского". Вы можете использовать Kaspersky Endpoint Security с этими решениями в различных конфигурациях и собрать собственную систему защиты в зависимости от ваших требований. Для этого вам необходимо приобрести лицензию на каждое из решений. При этом лицензия может включать в себя право на использование одного решения (например, только MDR Add-on) или нескольких решений [EDR Optimum+MDR] Add-on.

MDR и EDR Optimum поддерживают следующие способы лицензирования:

- Функциональность MDR или EDR Optimum включена в состав лицензии на использование Kaspersky Endpoint Security для Windows.

  Функциональность будет доступна сразу после активации Kaspersky Endpoint Security для Windows. Вам нужно добавить только один ключ.

- Отдельные лицензии на использование MDR или EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  Функциональность будет доступна после добавления отдельного ключа MDR Add-on, EDR Optimum Add-on или [EDR Optimum+MDR] Add-on. В результате на компьютере будет добавлено два ключа: ключ для Kaspersky Endpoint Security и ключ для MDR или EDR Optimum. Ключ для Kaspersky Endpoint Security следует добавлять в первую очередь.

Kaspersky Endpoint Security позволяет добавлять только один *активный ключ* для лицензирования MDR и EDR Optimum. То есть, если вам нужно активировать оба этих решения, вам нужно добавить один общий ключ [EDR Optimum+MDR] Add-on. Также вы можете добавить один *резервный ключ*.

Если при развертывании MDR вы использовали BLOB-файл, то отдельный ключ для активации MDR не нужен. BLOB-файл уже содержит информацию о лицензии.

Первоначальное лицензирование решений

При первоначальном развертывании MDR и EDR Optimum активация решений ничем не отличается от активации приложения Kaspersky Endpoint Security. Вы можете добавить ключ с помощью задачи *Добавление ключа* или использовать функцию автоматического распространения ключа. Лицензионный ключ будет добавлен в приложение в качестве второго активного ключа или в качестве резервного, если вы установили соответствующий флажок.

Переход с одной лицензии на другую

Если в вашей организации уже развернуто какое-то из этих решений, и соответствующий ключ добавлен в приложение, то лицензирование новой конфигурации имеет особенности. При переходе на другую лицензию приложение не добавляет новый ключ в приложение, а заменяет текущий ключ на новый. Это связано с тем, что приложение позволяет добавлять только один ключ для активации MDR и EDR Optimum.

Например, в вашей организации развернуто решение [EDR Optimum+MDR], и вы решили перейти на конфигурацию MDR Add-on. Для перехода на новую конфигурацию вам нужно заменить ключ [EDR Optimum+MDR] Add-on на ключ MDR Add-on.

Отдельная лицензия на использование EDR Optimum и MDR ([EDR Optimum+MDR] Add-on) больше не доступна. Если вы хотите использовать оба этих решения, вам нужно активировать MDR с помощью BLOB-файла, а EDR Optimum с помощью лицензионного ключа.

При использовании функции автоматического распространения ключа приложение отклоняет лицензионные ключи, распространяющиеся на такое же количество решений. То есть, если у вас добавлен ключ EDR Optimum Add-on, то заменить этот ключ на ключ MDR Add-on невозможно. Но вы можете заменить ключ EDR Optimum Add-on на ключ [EDR Optimum+MDR] Add-on. Также приложение отклоняет ключи, если вы пытаетесь заменить ключ MDR Add-on на ключ EDR Add-on. Для замены ключа вы можете запустить задачу *Добавление ключа*. Задача *Добавление ключа* позволяет заменять ключи от лицензий с любым набором решений.

Если у вас добавлен резервный ключ [EDR Optimum+MDR] Add-on, для корректного добавления активного ключа EDR Optimum Add-on или MDR Add-on вам нужно сначала заменить резервный ключ на ключ EDR Optimum Add-on или MDR Add-on или удалить резервный ключ, а потом заменить активный ключ.

Совместимость со сторонними EDR-решениями

Вы можете использовать приложение Kaspersky Endpoint Security для защиты рабочих станций и серверов совместно с EDR-решениями сторонних поставщиков. Для исключения ложных срабатываний рекомендуется добавить исполняемые файлы приложений Kaspersky Endpoint Security и Агента администрирования в доверенную зону стороннего EDR-решения.

	Kaspersky Endpoint Security для Windows	Агент администрирования Kaspersky Security Center
Рабочая папка	`C:\Program Files (x86)\Kaspersky Lab\KES.14.3.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Исполняемые файлы	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent обеспечивает взаимодействие приложения с другими решениями "Лаборатории Касперского" для обнаружения сложных угроз (например, Kaspersky Sandbox). Решения "Лаборатории Касперского", которые поддерживает Kaspersky Endpoint Agent, зависят от версии Kaspersky Endpoint Agent.

Для работы Kaspersky Endpoint Agent в составе решений "Лаборатории Касперского" необходимо активировать эти решения соответствующим лицензионным ключом.

Полную информацию о Kaspersky Endpoint Agent в составе программного решения, которое вы используете, а также полную информацию о самом решении смотрите в справке соответствующего решения:

- в Справке Kaspersky Anti Targeted Attack Platform;
- в Справке Kaspersky Sandbox;
- в Справке Kaspersky Endpoint Detection and Response Optimum;
- в Справке Kaspersky Managed Detection and Response.

В комплект поставки Kaspersky Endpoint Security версий 11.2.0 – 11.8.0 включено приложение Kaspersky Endpoint Agent. Вы можете выбрать Kaspersky Endpoint Agent во время установки Kaspersky Endpoint Security для Windows. В результате на компьютере будет установлено два приложения: KEA и KES. В Kaspersky Endpoint Security 11.9.0 дистрибутив приложения Kaspersky Endpoint Agent исключен из комплекта поставки Kaspersky Endpoint Security.

Соответствие версий KEA в составе KES

Kaspersky Endpoint Security для Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

"Лаборатория Касперского" переводит все решения Detection and Response на работу со встроенным агентом Kaspersky Endpoint Security вместо Kaspersky Endpoint Agent. "Лаборатория Касперского" постепенно добавляет поддержку этих решений и отказывается от работы с Kaspersky Endpoint Agent (см. таблицу ниже). Начиная с версии 12.1 приложение поддерживает работу со всеми решениями Detection and Response. Кроме того, начиная с версии 12.1 приложение больше несовместимо с Kaspersky Endpoint Agent, и установить оба этих приложения на одном компьютере невозможно.

Внедрение встроенного агента для работы с решениями Detection and Response

Версия Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (компонент Endpoint Detection and Response)	Kaspersky Anti Targeted Attack Platform (компонент Network Detection and Response)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Встроенный агент**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	Kaspersky Endpoint Agent
12.6	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**	**Встроенный агент**

Миграция конфигурации [KES+KEA] на [KES+встроенный агент]

Kaspersky Endpoint Security включает в себя встроенные агенты для работы решений Detection and Response. Теперь вам не нужно отдельное приложение Kaspersky Endpoint Agent для работы этих решений. При развертывании Kaspersky Endpoint Security на компьютеры с установленным Kaspersky Endpoint Agent решения Detection and Response продолжат работу с Kaspersky Endpoint Security. Также приложение Kaspersky Endpoint Agent будет удалено с компьютера.

В комплект поставки Kaspersky Endpoint Security версий 11.2.0 – 11.8.0 включено приложение Kaspersky Endpoint Agent. Вы можете выбрать Kaspersky Endpoint Agent во время установки Kaspersky Endpoint Security для Windows. В результате на компьютере будет установлено два приложения: KEA и KES. В Kaspersky Endpoint Security 11.9.0 дистрибутив приложения Kaspersky Endpoint Agent исключен из комплекта поставки Kaspersky Endpoint Security.

Миграция конфигурации [KES+KEA] на [KES+встроенный агент] состоит из следующих этапов:

1. **Обновление Kaspersky Security Center**

   Обновите все компоненты Kaspersky Security Center до версии 13.2 или выше, включая Агент администрирования на компьютерах пользователей и Web Console.

2. **Обновление веб-плагина Kaspersky Endpoint Security**

   В Kaspersky Security Center Web Console обновите веб-плагин Kaspersky Endpoint Security до версии 11.7.0 или выше. Управление компонентами EDR Optimum и Kaspersky Sandbox доступно только в Web Console.

   Для работы с Kaspersky Anti Targeted Attack Platform (EDR) вам потребуется веб-плагин Kaspersky Endpoint Security версии 12.1 или выше.

   Для работы с Kaspersky Anti Targeted Attack Platform (NDR) вам потребуется веб-плагин Kaspersky Endpoint Security версии 12.7 или выше.

3. **Миграция политики и задач**

   С помощью мастера миграции политик и задач Kaspersky Endpoint Agent перенесите параметры работы Kaspersky Endpoint Agent в приложение Kaspersky Endpoint Security для Windows.

   В результате будет создана новая политика Kaspersky Endpoint Security. Новая политика имеет статус *Неактивна*. Для применения политики откройте свойства политики, примите условия Положения о Kaspersky Security Network и измените статус на *Активна*.

4. **Лицензирование функций**

   Если для активации Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Agent у вас общая лицензия Kaspersky Endpoint Detection and Response Optimum или Kaspersky Optimum Security, после обновления приложения до версии 11.7.0 активация функции EDR Optimum будет выполнена автоматически. Дополнительных действий не требуется.

   Если для активации функциональности EDR Optimum у вас отдельная лицензия Kaspersky Endpoint Detection and Response Optimum Add-on, вам нужно убедиться, что ключ EDR Optimum Add-on добавлен в хранилище Kaspersky Security Center и функция автоматического распространения лицензионного ключа включена. После обновления приложения до версии 11.7.0 активация функции EDR Optimum будет выполнена автоматически.

Если для активации Kaspersky Endpoint Agent у вас лицензия Kaspersky Endpoint Detection and Response Optimum или Kaspersky Optimum Security, а для активации Kaspersky Endpoint Security для Windows у вас другая лицензия, вам нужно заменить ключ для Kaspersky Endpoint Security для Windows на общий ключ Kaspersky Endpoint Detection and Response Optimum или Kaspersky Optimum Security. Вы можете заменить ключ с помощью задачи *Добавление ключа*.

Функциональность Kaspersky Sandbox активировать не требуется. Функциональность Kaspersky Sandbox будет доступна сразу после обновления и активации Kaspersky Endpoint Security для Windows.

Для активации Kaspersky Endpoint Security в составе решения Kaspersky Anti Targeted Attack Platform доступна только лицензия Kaspersky Anti Targeted Attack Platform. После обновления приложения до версии 12.1 активация функции EDR (KATA) будет выполнена автоматически. Дополнительных действий не требуется.

5. **Обновление приложения Kaspersky Endpoint Security**

> Для обновления приложения с миграцией функций EDR Optimum и Kaspersky Sandbox рекомендуется использовать задачу удаленной установки.

Для обновления приложения с помощью задачи удаленной установки вам нужно выполнить следующие настройки:

- Выберите компоненты для решений Detection and Response в параметрах инсталляционного пакета.
- Исключите компонент Kaspersky Endpoint Agent в параметрах инсталляционного пакета (для Kaspersky Endpoint Security для Windows версий 11.2.0 – 11.8.0).
- Если для ограничения доступа к Kaspersky Endpoint Agent включена Защита паролем, введите пароль деинсталляции приложения в параметрах задачи *Удаленная установка приложения*. Вы можете ввести пароль деинсталляции начиная с версии Kaspersky Security Center Linux 15.1.

Также вы можете обновить приложение следующими способами:

- Через службу обновлений "Лаборатории Касперского" (Seamless Update – SMU).
- Локально с помощью мастера установки.

Kaspersky Endpoint Security поддерживает автоматический выбор компонентов при обновлении приложения на компьютере с установленным приложением Kaspersky Endpoint Agent. Автоматический выбор компонентов зависит от прав учетной записи пользователя, который обновляет приложение.

Если вы обновляете Kaspersky Endpoint Security с помощью EXE-файла или с помощью MSI-файла под системной учетной записью (SYSTEM), Kaspersky Endpoint Security получает доступ к действующим лицензиям решений "Лаборатории Касперского". Таким образом, если на компьютере, например, установлено приложение Kaspersky Endpoint Agent и активировано решение EDR Optimum, установщик Kaspersky Endpoint Security автоматически сконфигурирует набор компонентов и выберет компонент EDR Optimum. При этом Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent. Запуск установщика MSI под системной учетной записью (SYSTEM) обычно выполняется при обновлении через службу обновлений "Лаборатории Касперского" (SMU) или при развертывании инсталляционного пакета через Kaspersky Security Center.

Если вы обновляете Kaspersky Endpoint Security с помощью MSI-файла под учетной записью непривилегированного пользователя, у Kaspersky Endpoint Security отсутствует доступ к действующим лицензиям решений "Лаборатории Касперского". При этом Kaspersky Endpoint Security автоматически выбирает компоненты на основании конфигурации Kaspersky Endpoint Agent. Далее Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent.

6. **Перезагрузка компьютера**

   Для завершения обновления приложения со встроенным агентом перезагрузите компьютер. При обновлении приложения установщик удаляет Kaspersky Endpoint Agent до перезагрузки компьютера. После перезагрузки компьютера установщик добавляет встроенный агент. Таким образом, Kaspersky Endpoint Security не выполняет функции EDR и Kaspersky Sandbox до перезагрузки компьютера.

7. **Проверка работы Kaspersky Endpoint Detection and Response Optimum и Kaspersky Sandbox**

   Если после обновления приложения компьютер имеет статус *Критический* в консоли Kaspersky Security Center, выполните следующие действия:

   - Убедитесь, что на компьютере установлен Агент администрирования версии 13.2 или выше.
   - Проверьте статус работы встроенного агента с помощью отчета *Отчет о статусе компонентов приложения*. Если компонент имеет статус *Не установлен*, установите компонент с помощью задачи *Изменение состава компонентов приложения*.
   - Убедитесь, что вы приняли условия Положения о Kaspersky Security Network в новой политике Kaspersky Endpoint Security для Windows.
   - Убедитесь в том, что функция EDR Optimum активирована с помощью отчета *Отчет о статусе компонентов приложения*. Если компонент имеет статус *Не поддерживается лицензией*, убедитесь, что функция автоматического распространения лицензионного ключа EDR Optimum включена.

Миграция политик и задач Kaspersky Endpoint Agent

В Kaspersky Endpoint Security для Windows включен мастер миграции с Kaspersky Endpoint Agent на Kaspersky Endpoint Security. Вы можете перенести параметры политик и задач для следующих решений:

- Kaspersky Sandbox;
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum);
- Kaspersky Anti Targeted Attack Platform.

Мастер миграции с Kaspersky Endpoint Agent на Kaspersky Endpoint Security работает только в Web Console и Cloud Console. В Консоли администрирования (MMC) доступна только миграция параметров для решения Kaspersky Anti Targeted Attack Platform (EDR) с помощью стандартного мастера миграции политик и задач в Kaspersky Security Center.

> Рекомендуем сначала выполнить миграцию с Kaspersky Endpoint Agent на Kaspersky Endpoint Security на одном компьютере, затем на группе компьютеров и далее выполнить миграцию на всех компьютерах организации.

Чтобы перенести параметры политики и задач с Kaspersky Endpoint Agent на Kaspersky Endpoint Security,

в главном окне Web Console выберите **Операции** → **Миграция с Kaspersky Endpoint Agent**.

В результате запустится мастер миграции политик и задач. Следуйте его указаниям.

Шаг 1. Миграция политик

Мастер миграции создает новую политику, в которой будут объединены параметры политик Kaspersky Endpoint Security и Kaspersky Endpoint Agent. В списке политик выберите политики Kaspersky Endpoint Agent, параметры которых вы хотите объединить с политикой Kaspersky Endpoint Security. Нажмите на политику Kaspersky Endpoint Agent, чтобы выбрать политику Kaspersky Endpoint Security, с которой вы хотите объединить параметры. Убедитесь, что политики выбраны верно и перейдите к следующем шагу.

Шаг 2. Миграция задач

Мастер миграции создает новые задачи для Kaspersky Endpoint Security. В списке задач выберите задачи Kaspersky Endpoint Agent, которые вы хотите создать для Kaspersky Endpoint Security. Мастер поддерживает задачи для решений Kaspersky Endpoint Detection and Response Optimum и Kaspersky Sandbox. Перейдите к следующему шагу.

Шаг 3. Завершение работы мастера

Завершите работу мастера. В результате работы мастера будут выполнены следующие действия:

- Создана новая политика Kaspersky Endpoint Security.

  В политике объединены параметры Kaspersky Endpoint Security и Kaspersky Endpoint Agent. Политика называется *<Название политики Kaspersky Endpoint Security> & <Название политики Kaspersky Endpoint Agent>*. Новая политика имеет статус *Неактивна*. Для продолжения работы измените статусы политик Kaspersky Endpoint Agent и Kaspersky Endpoint Security на *Неактивна* и активируйте новую объединенную политику.

  После миграции из Kaspersky Endpoint Agent на Kaspersky Endpoint Security для Windows убедитесь, что в новой политике настроены функции передачи данных на Сервер администрирования: данные о файлах карантина и данные о цепочке развития угрозы. Значения параметров передачи данных не мигрируют из политики Kaspersky Endpoint Agent.

  При миграции с Kaspersky Endpoint Agent на Kaspersky Endpoint Security для решения Kaspersky Anti Targeted Attack Platform (EDR) могут возникнуть ошибки подключения компьютера к серверам Central Node. Это связано с тем, что мастер миграции в Web Console пропускает и не переносит следующие параметры политики:

  - Запрет на изменение параметров **Подключение к серверам KATA** ("замок").

    По умолчанию изменение параметров разрешено ("замок" открыт). Поэтому параметры не будут применены на компьютере. Вам нужно запретить изменение параметров и закрыть "замок".

  - Криптоконтейнер.

    Если вы используете двустороннюю аутентификацию для подключения к серверам Central Node, нужно добавить криптоконтейнер повторно. TLS-сертификат сервера мастер миграции переносит корректно.

Мастер миграции политик и задач в Консоли администрирования (MMC) переносит все параметры для решения Kaspersky Anti Targeted Attack Platform (EDR).

- Созданы новые задачи Kaspersky Endpoint Security.

  Новые задачи представляют собой копии задач Kaspersky Endpoint Agent для решений Kaspersky Endpoint Detection and Response Optimum и Kaspersky Sandbox. При этом мастер оставляет задачи Kaspersky Endpoint Agent без изменений.

Как перенести параметры политик и задач с Kaspersky Endpoint Agent на Kaspersky Endpoint Security в Консоли администрирования (MMC) (только для KATA (EDR))

1. В Консоли администрирования выберите Сервер администрирования и по правой клавише мыши откройте контекстное меню.
2. Выберите пункт **Все задачи** → **Мастер массовой конвертации политик и задач**.

В результате запустится мастер массовой конвертации политик и задач. Следуйте его указаниям.

Шаг 1. Выбор приложения, для которого нужно конвертировать политики и задачи

На этом шаге нужно выбрать приложение Kaspersky Endpoint Security для Windows. Перейдите к следующему шагу.

Шаг 2. Конвертация политик

Мастер миграции создает новую политику Kaspersky Endpoint Security, в которую будут перенесены параметры политики Kaspersky Endpoint Agent. В списке политик выберите политики Kaspersky Endpoint Agent, параметры которых вы хотите перенести в политику Kaspersky Endpoint Security. Перейдите к следующему шагу.

Далее мастер миграции начнет конвертацию политик. При конвертации политик мастер миграции предложит принять Положение о Kaspersky Security Network. Новые политики будут иметь имя *<Название политики> (конвертированная)*.

Шаг 3. Конвертация задач

Пропустите этот шаг. Мастер поддерживает задачи только для решений Kaspersky Endpoint Detection and Response Optimum и Kaspersky Sandbox. Управление этими компонентами доступно только в Web Console. Перейдите к следующему шагу.

Шаг 4. Завершение работы мастера

Завершите работу мастера. В результате работы мастера будет создана новая политика Kaspersky Endpoint Security.

Endpoint Detection and Response агент (EDR-агент)

Начиная с версии Kaspersky Endpoint Security для Windows 12.3 в приложении добавлена конфигурация Endpoint Detection and Response агента (EDR-агент). *Endpoint Detection and Response агент* – приложение, которое устанавливается на отдельные рабочие станции и серверы IT-инфраструктуры организации, для работы следующих решений Detection and Response от "Лаборатории Касперского":

- Kaspersky Managed Detection and Response;
- Kaspersky Anti Targeted Attack Platform (EDR);
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (начиная с версии 12.6);
- Kaspersky Anti Targeted Attack Platform (NDR) (начиная с версии 12.7);
- Kaspersky Endpoint Detection and Response Expert (on-premises) (начиная с версии 12.11).

EDR-агент не поддерживает работу с решением Kaspersky Endpoint Detection and Response Expert (cloud).

EDR-агент осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами. Компоненты защиты и контроля приложения для EDR-агента недоступны.

EDR-агент совместим со сторонними EPP-приложениями. Таким образом, вы можете использовать средства защиты инфраструктуры от сторонних поставщиков совместно с решениями Detection and Response от "Лаборатории Касперского".

Для развертывания EDR-агента на компьютере должен быть установлен Агент администрирования, и компьютер должен быть добавлен в консоли Kaspersky Security Center. Для взаимодействия EDR-агента с Kaspersky Security Center вам нужно установить плагин Kaspersky Endpoint Security для Windows. Вы можете настроить параметры EDR-агента с помощью групповой политики. Для интеграции EDR-агента вам нужно настроить параметры интеграции в соответствующих разделах политики.

Таким образом, для работы решений Detection and Response от "Лаборатории Касперского" в инфраструктуре должны быть установлены следующие приложения от "Лаборатории Касперского":

	• Агент администрирования; • EDR-агент.
Конечная точка	
	Плагин управления Kaspersky Endpoint Security для Windows.
Kaspersky Security Center	
	
Решение Detection and Response: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

Установка EDR-агента

Установка Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агент (EDR-агент) для решений Detection and Response от "Лаборатории Касперского" не отличается.

EDR-агент может быть установлен на компьютер следующими способами:

- удаленно с помощью Kaspersky Security Center;
- локально с помощью мастера установки;
- локально с помощью командной строки (только для KATA (EDR) и EDR Expert (on-premises)).

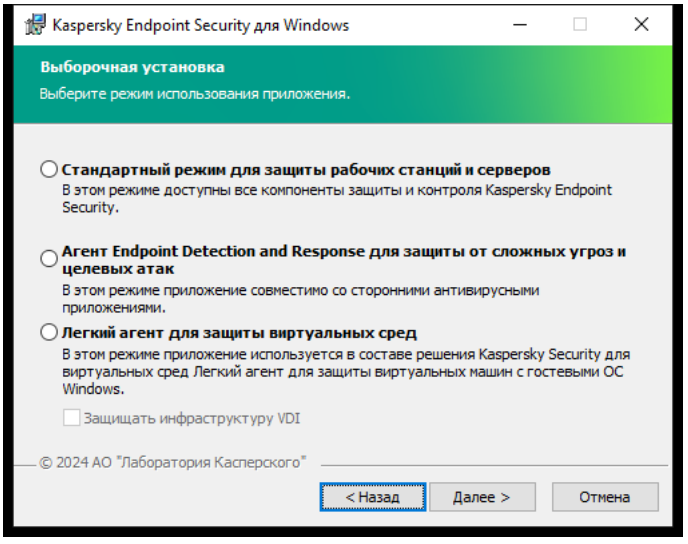
Для установки EDR-агента нужно выбрать соответствующую конфигурацию в параметрах инсталляционного пакета или мастере установки приложения.

Как установить EDR-агент с помощью мастера установки

1. Скопируйте папку комплекта поставки на компьютер пользователя.
2. Запустите файл setup_kes.exe.

   Запустится мастер установки приложения.

Конфигурация Kaspersky Endpoint Security



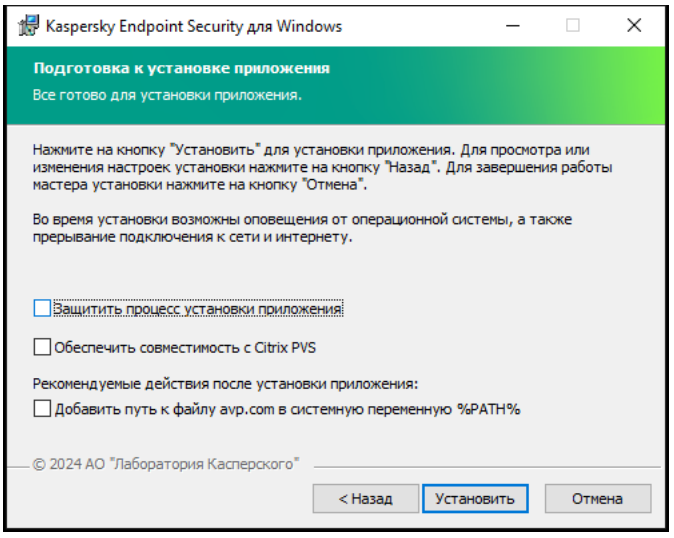
Выбор конфигурации приложения

Выберите конфигурацию **Агент Endpoint Detection and Response**. В этой конфигурации вы можете установить только компоненты для работы решений Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), а также KUMA. Эта конфигурация нужна в том случае, если в вашей организации развернута система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков и решение Detection and Response от "Лаборатории Касперского". Таким образом, Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента может быть совместим со сторонними EPP-приложениями.

Компоненты Kaspersky Endpoint Security

Выберите компоненты, которые вы хотите установить. Вы можете изменить состав компонентов после установки приложения. Для этого вам нужно запустить мастер установки повторно и выбрать операцию изменения состава компонентов.

Дополнительные параметры



Дополнительные параметры установки приложения

Защитить процесс установки приложения. Защита установки включает в себя защиту от подмены дистрибутива вредоносными приложениями, блокирование доступа к папке установки Kaspersky Endpoint Security и блокирование доступа к разделу системного реестра с ключами приложения. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку приложения (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop).

Обеспечить совместимость с Citrix PVS. Вы можете включить поддержку Citrix Provisioning Services для установки Kaspersky Endpoint Security на виртуальную машину.

Добавить путь к файлу avp.com в системную переменную %PATH%. Вы можете добавить путь установки в переменную %PATH% для удобства использования интерфейса командной строки.

Как установить EDR-агент с помощью командной строки (только для KATA (EDR) и EDR Expert (on-premises))

1. Запустите интерпретатор командной строки cmd от имени администратора.

2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security.

3. Выполните команду:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
```

или

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
```

В результате EDR-агент для интеграции с Kaspersky Anti Targeted Attack Platform (EDR) или Kaspersky Endpoint Detection and Response Expert (on-premises) будет установлен на компьютер. Вы можете убедиться, что приложение установлено, и проверить параметры приложения с помощью команды `status`.

Как установить EDR-агент через Консоль администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно → Удаленная установка → Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.
3. Откройте свойства инсталляционного пакета.

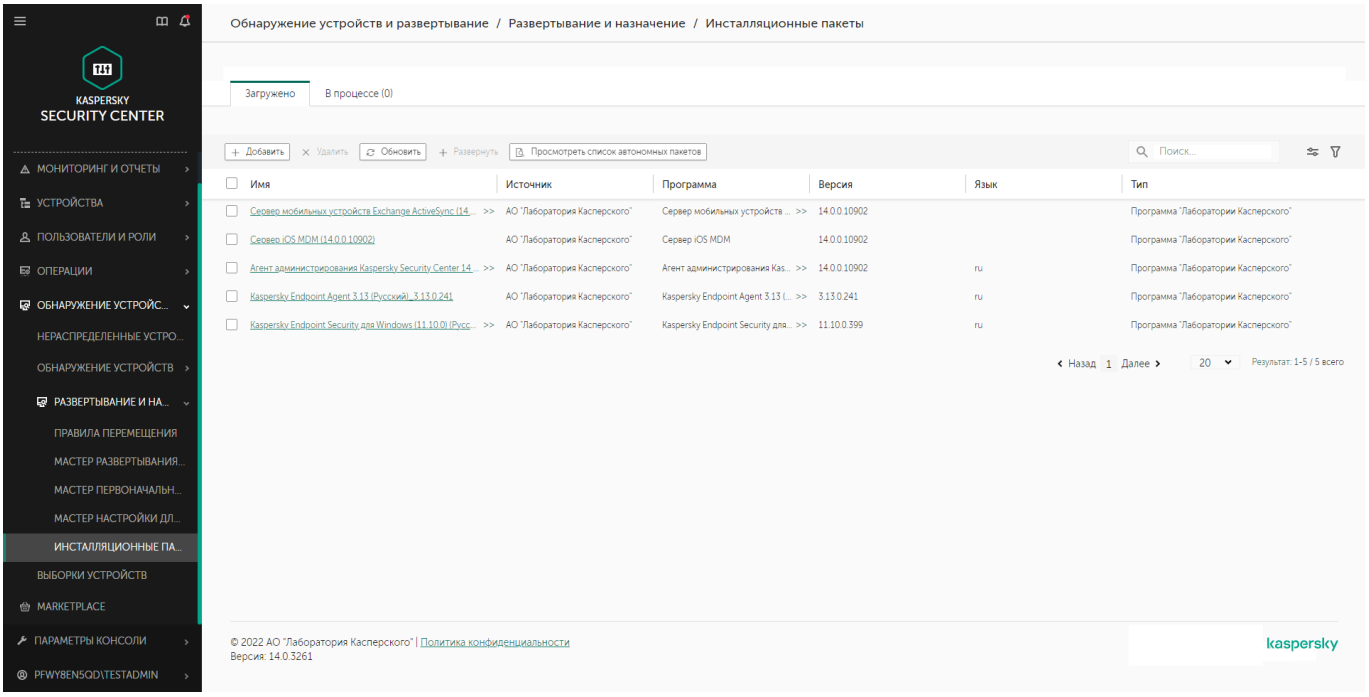
   Если требуется, создайте новый инсталляционный пакет.
4. Перейдите в раздел **Компоненты защиты**.
5. Выберите конфигурацию **Агент Endpoint Detection and Response для защиты от сложных угроз и целевых атак**. В этой конфигурации вы можете установить только компоненты для работы решений Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), а также KUMA. Эта конфигурация нужна в том случае, если в вашей организации развернута система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков и решение Detection and Response от "Лаборатории Касперского". Таким образом, Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента может быть совместим со сторонними EPP-приложениями.
6. Выберите компоненты, которые вы хотите установить.

   Вы можете изменить состав компонентов после установки приложения.
7. Сохраните внесенные изменения.
8. Создайте задачу удаленной установки. В свойствах задачи выберите созданный инсталляционный пакет.

Как установить EDR-агент через Web Console

1. В главном окне Web Console выберите **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.

Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.



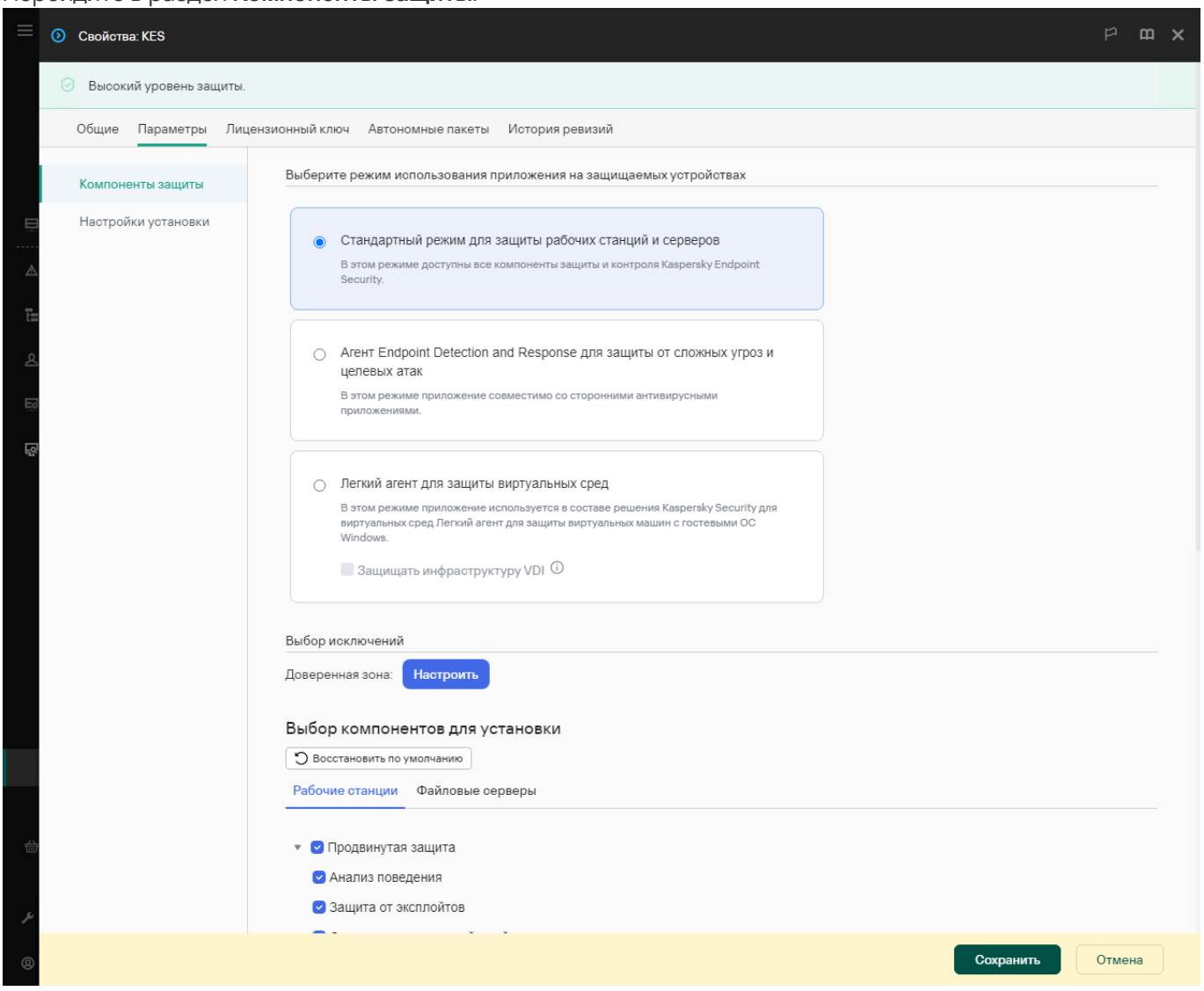
Список инсталляционных пакетов

2. Откройте свойства инсталляционного пакета.

   Если требуется, создайте новый инсталляционный пакет.

3. Выберите вкладку **Параметры**.

4. Перейдите в раздел **Компоненты защиты**.



Состав компонентов в инсталляционном пакете

5. Выберите конфигурацию **Агент Endpoint Detection and Response**. В этой конфигурации вы можете установить только компоненты для работы решений Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), а также KUMA. Эта конфигурация нужна в том случае, если в вашей организации развернута система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков и решение Detection and Response от "Лаборатории Касперского". Таким образом, Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента может быть совместим со сторонними EPP-приложениями.

6. Выберите компоненты, которые вы хотите установить.

   Вы можете изменить состав компонентов после установки приложения.

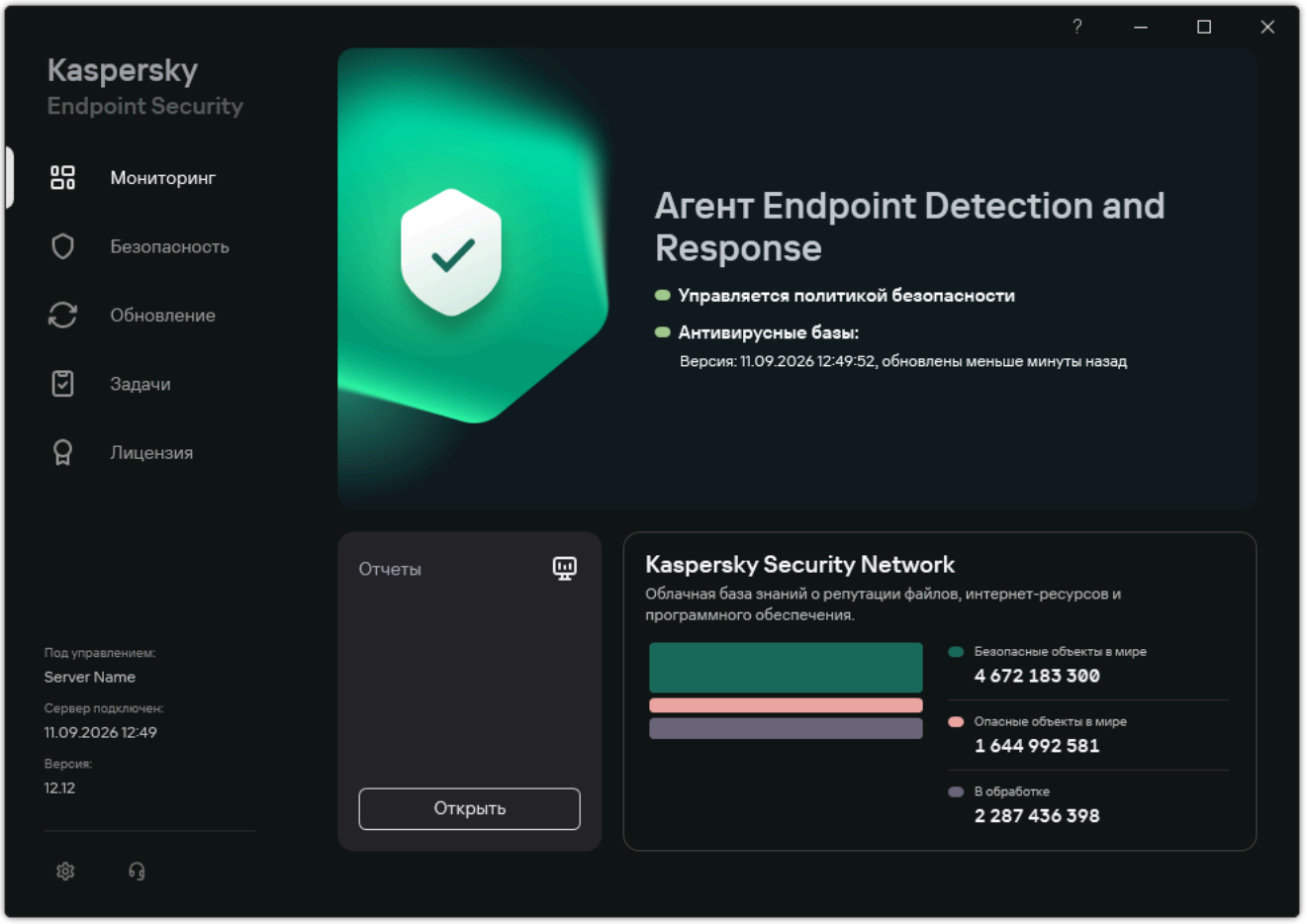
7. Сохраните внесенные изменения.

8. Создайте задачу удаленной установки. В свойствах задачи выберите созданный инсталляционный пакет.

В результате EDR-агент будет установлен на компьютер пользователя. Вам доступен интерфейс приложения, а также значок приложения в области уведомлений .

В консоли Kaspersky Security Center компьютер с установленным приложением в конфигурации EDR-агент будет иметь статус *Критический* – . Компьютер имеет такой статус из-за отсутствия компонента Защита от файловых угроз. Никаких дополнительных действий предпринимать не требуется.

Если вам не удалось установить EDR-агент на компьютер со сторонним EPP-приложением из-за того, что установщик обнаружил на компьютере несовместимое ПО, вы можете пропустить проверку на несовместимое ПО.



Главное окно EDR-агента

Теперь вам нужно настроить интеграцию с решением Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) или Kaspersky Anti Targeted Attack (NDR). Также вы можете настроить дополнительные параметры приложения и, например, сформировать доверенную зону или скрыть интерфейс приложения. Вам доступны следующие разделы параметров:

- Kaspersky Security Network;
- Настройки приложения;
- Настройки сети;
- Исключения;
- Отчеты;

- Интерфейс;
- Управление настройками.

Интеграция EDR-агента с MDR

EDR-агент устанавливается на рабочие станции и серверы в IT-инфраструктуре организации. EDR-агент обрабатывает данные и отправляет их по потокам Kaspersky Security Network в Kaspersky Managed Detection and Response.

Для работы Kaspersky Managed Detection and Response с Сервером администрирования через Kaspersky Security Center Web Console вам нужно установить новое безопасное соединение – *фоновое соединение*. Kaspersky Managed Detection and Response предлагает установить фоновое соединение при развертывании решения. Убедитесь, что фоновое соединение установлено.

Как установить фоновое соединение в Web Console

1. В главном окне Web Console выберите **Параметры** → **Интеграция**.
2. Перейдите в раздел **Интеграция**.
3. Включите переключатель **Фоновое соединение для интеграции Включено**.
4. Сохраните внесенные изменения.

Интеграция с Kaspersky Managed Detection and Response состоит из следующих этапов:

1. **Установка компонента Managed Detection and Response**

   Вы можете выбрать компонент MDR во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

   > Для установки компонента Managed Detection and Response без перезагрузки компьютера с помощью задачи *Изменение состава компонентов приложения* вам необходимо выключить функцию **Проверять на наличие несовместимых приложений сторонних производителей** в настройках задачи.

2. **Настройка Kaspersky Private Security Network**

   > Если вы используете Kaspersky Security Center Cloud Console, этот шаг нужно пропустить. Kaspersky Security Center Cloud Console автоматически настраивает Kaspersky Private Security Network при установке плагина MDR.

   Kaspersky Private Security Network (KPSN) – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров.

   Загрузите конфигурационный файл Kaspersky Security Network в свойствах Сервера администрирования. Конфигурационный файл Kaspersky Security Network находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробнее о настройке Kaspersky Private Security Network см. в справке Kaspersky Security Center. Также вы можете загрузить конфигурационный файл Kaspersky Security Network на компьютер из командной строки (см. инструкцию ниже).

Как настроить Kaspersky Private Security Network из командной строки

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Выполните команду:

   ```
   avp.com KSN /private <file name>
   ```

   где `<file name>` – имя конфигурационного файла с параметрами Kaspersky Private Security Network (формат файла PKCS7 или PEM).

   Пример:
   `avp.com KSN /private C:\kpsn_config.pkcs7`

В результате Kaspersky Endpoint Security будет использовать Kaspersky Private Security Network для определения репутации файлов, приложений и веб-сайтов. В параметрах политики в разделе **Kaspersky Security Network** будет указан статус работы *Инфраструктура: Kaspersky Private Security Network*.

Для работы Managed Detection and Response необходимо включить расширенный режим KSN.

3 Активация Kaspersky Managed Detection and Response

Начиная с версии Kaspersky Endpoint Security для Windows 12.10 для активации функциональности Managed Detection and Response кроме кода активации вы также можете использовать файл ключа.

Вам нужно приобрести отдельную лицензию на использование MDR (Kaspersky Managed Detection and Response Add-on).

Функциональность будет доступна после добавления отдельного ключа Kaspersky Managed Detection and Response Add-on. Лицензирование отдельной функциональности Managed Detection and Response не отличается от лицензирования Kaspersky Endpoint Security.

Убедитесь, что функциональность MDR включена в лицензию и работает в локальном интерфейсе приложения.

4 Включение компонента Managed Detection and Response

Загрузите конфигурационный файл BLOB в политике Kaspersky Endpoint Security (см. инструкцию ниже). BLOB-файл содержит идентификатор клиента и информацию о лицензии Kaspersky Managed Detection and Response. BLOB-файл находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробную информацию о BLOB-файле см. в справке Kaspersky Managed Detection and Response.

Начиная с версии Kaspersky Endpoint Security для Windows 12.6 в Kaspersky Managed Detection and Response без тенантов при наличии действующей лицензии добавлять BLOB-файл не обязательно.

Как включить компонент Managed Detection and Response в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.
4. Установите флажок **Managed Detection and Response (Industrial CyberSecurity)**.

5. В блоке **Настройка** нажмите на кнопку **Загрузить** и выберите BLOB-файл, полученный в Консоли Kaspersky Managed Detection and Response. Файл имеет расширение P7.

   По умолчанию изменение параметров приложения пользователем разрешено (замок открыт). Для применения политики на компьютерах, закройте замки .

6. Сохраните внесенные изменения.

Как включить компонент Managed Detection and Response в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Managed Detection and Response**.
5. Включите переключатель **Managed Detection and Response ВКЛЮЧЕН**.
6. Нажмите на кнопку **Загрузить** и выберите BLOB-файл, полученный в Консоли Kaspersky Managed Detection and Response. Файл имеет расширение P7.

   По умолчанию изменение параметров политики пользователем разрешено (замок открыт). Для применения политики на компьютерах, закройте замки .

7. Сохраните внесенные изменения.

Как включить компонент Managed Detection and Response из командной строки

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Выполните команду:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение **Настройка приложения**.

В результате Kaspersky Endpoint Security проверит BLOB-файл. Проверка BLOB-файла включает в себя проверку цифровой подписи и срока действия лицензии. Если BLOB-файл прошел проверку, Kaspersky Endpoint Security загрузит файл и отправит файл на компьютер при следующей синхронизации с Kaspersky Security Center. Проверьте статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Managed Detection and Response**.

5 Настройка других компонентов приложения для получения телеметрии

Для работы Managed Detection and Response должны быть включены следующие компоненты:

- Kaspersky Security Network (расширенный режим).
- Анализ поведения.
- Защита от эксплойтов.
- Защита от веб-угроз.
- Защита от почтовых угроз.
- Защита от файловых угроз.
- Защита от сетевых угроз.
- Сетевой экран.
- AMSI-защита.
- Фоновая проверка.

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Managed Detection and Response**.
5. Включите переключатель **Managed Detection and Response ВКЛЮЧЕН**.
6. Сохраните внесенные изменения.

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Установите флажок **Managed Detection and Response (Industrial CyberSecurity)**.
5. Сохраните внесенные изменения.

Интеграция EDR-агента с EDR (KATA)

EDR-агент устанавливается на рабочие станции и серверы в IT-инфраструктуре организации. На этих компьютерах EDR-агент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправляет данные наблюдения на сервер с компонентом Central Node.

Для интеграции с EDR (KATA) вам нужно включить компонент Endpoint Detection and Response (KATA) и настроить параметры EDR-агента.

Для работы Endpoint Detection and Response (KATA) должны быть выполнены следующие условия:

- Kaspersky Anti Targeted Attack Platform версии 5.0 – 7.1.
- Kaspersky Security Center версии 14.2 или выше. В более ранних версиях Kaspersky Security Center невозможно активировать функциональность Endpoint Detection and Response (KATA).

https://rutube.ru/video/b0331e73f0fc30baed824121f9b00c35/

Интеграция с Endpoint Detection and Response (KATA) состоит из следующих этапов:

1. **Активация Endpoint Detection and Response (KATA)**

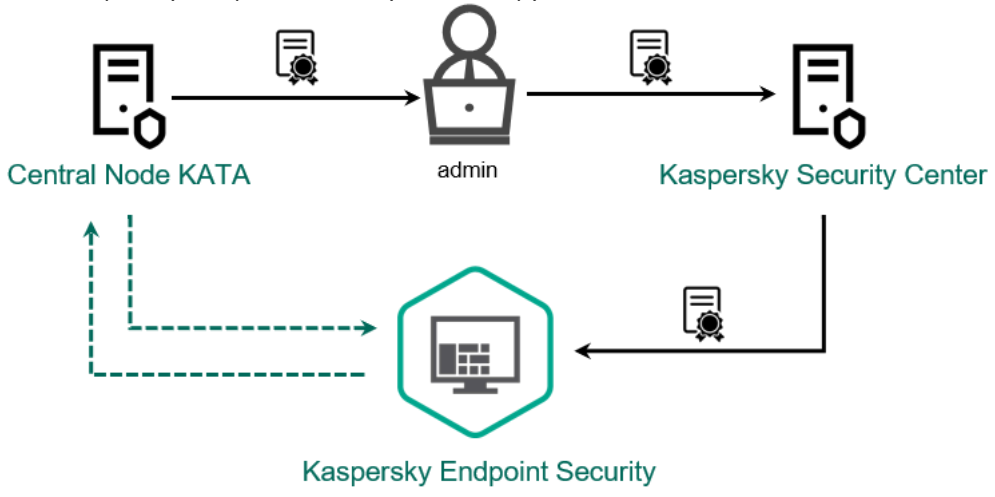
   Вам нужно приобрести отдельную лицензию на использование EDR (KATA) (Kaspersky Endpoint Detection and Response (KATA) Add-on).

   Функциональность будет доступна после добавления отдельного ключа Kaspersky Endpoint Detection and Response (KATA). Лицензирование отдельной функциональности Endpoint Detection and Response (KATA) не отличается от лицензирования Kaspersky Endpoint Security.

   Убедитесь, что функциональность EDR (KATA) включена в лицензию и работает в локальном интерфейсе приложения.

2. **Подключение к Central Node**

   Для работы Kaspersky Anti Targeted Attack Platform необходимо установить доверенное соединение между Kaspersky Endpoint Security и компонентом Central Node. Для настройки доверенного соединения вам нужен TLS-сертификат. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). Далее вам нужно добавить TLS-сертификат в Kaspersky Endpoint Security (см. инструкцию ниже).



Добавление TLS-сертификата в Kaspersky Endpoint Security

По умолчанию Kaspersky Endpoint Security проверяет только TLS-сертификат Central Node. Чтобы сделать соединение более безопасным, вы можете включить дополнительную проверку компьютера в Central Node (двусторонняя аутентификация). Для включения такой проверки вам нужно включить двустороннюю аутентификацию в параметрах Central Node и Kaspersky Endpoint Security. Также для двусторонней аутентификации вам нужен криптоконтейнер. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

Как подключить компьютер с Kaspersky Endpoint Security к Central Node в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Detection and Response → Endpoint Detection and Response Expert (on-premises)**.
5. Установите флажок **Endpoint Detection and Response Expert (on-premises)**.
6. Нажмите на кнопку **Настройки подключения к серверам**.
7. Настройте параметры подключения к серверам:
   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу Central Node.
   - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).
   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

     Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.
8. Нажмите на кнопку **OK**.
9. Добавьте серверы Central Node. Для этого укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.

   Вы можете добавить несколько адресов сервера Central Node. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.

10. Если требуется, настройте параметры отправки телеметрии.

11. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как подключить компьютер с Kaspersky Endpoint Security к Central Node в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response Expert (on-premises)**.

5. Включите переключатель: **Endpoint Detection and Response Expert (on-premises) ВКЛЮЧЕН**.

6. Для настройки EDR (KATA) в списке решений выберите **Endpoint Detection and Response Expert (версия 7.1 и ниже)**.

7. Нажмите на кнопку **Настройки подключения**.

8. Настройте параметры подключения к серверам:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу Central Node.

   - **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

     Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

9. Нажмите на кнопку **ОК**.

10. Добавьте серверы Central Node. Для этого укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.

    Вы можете добавить несколько адресов сервера Central Node. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.

11. Если требуется, настройте параметры отправки телеметрии.

12. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

В результате компьютер будет добавлен в консоли Kaspersky Anti Targeted Attack Platform. Проверьте статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Endpoint Detection and Response Expert (on-premises)**.

Интеграция EDR-агента с NDR (KATA)

EDR-агент устанавливается на рабочие станции и серверы в IT-инфраструктуре организации. На этих компьютерах EDR-агент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправляет данные наблюдения на сервер с компонентом Central Node.

Для интеграции с NDR (KATA) вам нужно включить компонент Network Detection and Response (KATA) и настроить параметры EDR-агента.

Для работы Network Detection and Response (KATA) должны быть выполнены следующие условия:

- Kaspersky Anti Targeted Attack Platform версии 7.0 или выше.
- Kaspersky Security Center версии 14.2 или выше. В более ранних версиях Kaspersky Security Center невозможно активировать функциональность Network Detection and Response (KATA).

https://rutube.ru/video/a6f9b4964e130bdb4ae5ea597d25f5ef/

Интеграция с Network Detection and Response (KATA) состоит из следующих этапов:

1. **Активация Network Detection and Response (KATA)**

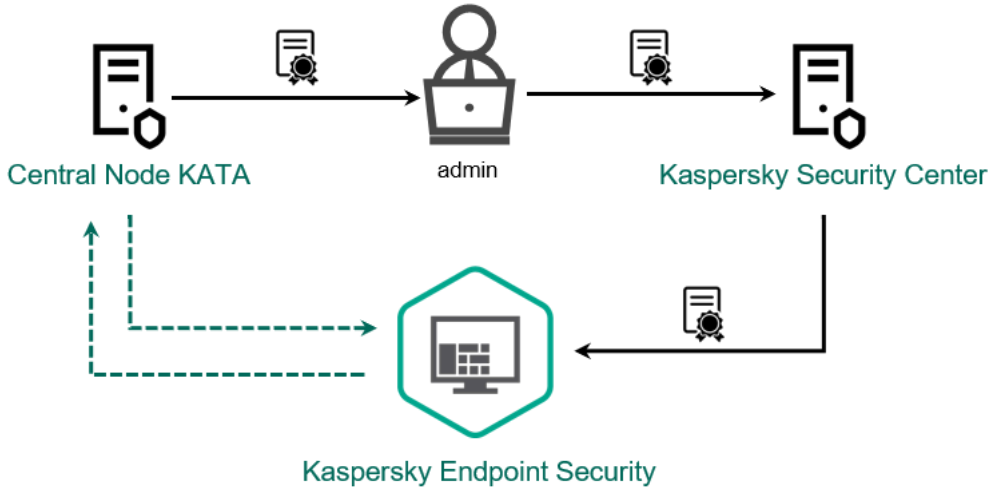
   Вам нужно приобрести отдельную лицензию на использование NDR (KATA) (Kaspersky Network Detection and Response (KATA) Add-on).

   Функциональность будет доступна после добавления отдельного ключа Kaspersky Network Detection and Response (KATA). Лицензирование отдельной функциональности Network Detection and Response (KATA) не отличается от лицензирования Kaspersky Endpoint Security.

   Убедитесь, что функциональность NDR (KATA) включена в лицензию и работает в локальном интерфейсе приложения.

2. **Подключение к Central Node**

Для работы Kaspersky Anti Targeted Attack Platform необходимо установить доверенное соединение между Kaspersky Endpoint Security и компонентом Central Node. Для настройки доверенного соединения вам нужен TLS-сертификат. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). Далее вам нужно добавить TLS-сертификат в Kaspersky Endpoint Security (см. инструкцию ниже).



Добавление TLS-сертификата в Kaspersky Endpoint Security

По умолчанию Kaspersky Endpoint Security проверяет только TLS-сертификат Central Node. Чтобы сделать соединение более безопасным, вы можете включить дополнительную проверку компьютера в Central Node (двусторонняя аутентификация). Для включения такой проверки вам нужно включить двустороннюю аутентификацию в параметрах Central Node и Kaspersky Endpoint Security. Также для двусторонней аутентификации вам нужен криптоконтейнер. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

Как подключить компьютер с Kaspersky Endpoint Security к Central Node в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Detection and Response** → **Network Detection and Response (KATA)**.
4. Установите флажок **Network Detection and Response (KATA)**.
5. Нажмите на кнопку **Настройки подключения**.
6. Настройте параметры подключения к серверам:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу Central Node.
   - **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

- **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

  Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

7. Нажмите на кнопку **OK**.
8. Добавьте серверы Central Node. Для этого укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.
9. Вы можете добавить несколько адресов сервера Central Node. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.
10. Если требуется, настройте параметры отправки телеметрии.
11. Сохраните внесенные изменения.

Как подключить компьютер с Kaspersky Endpoint Security к Central Node в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Network Detection and Response (KATA)**.
5. Включите переключатель **Network Detection and Response (KATA) ВКЛЮЧЕН**.
6. Нажмите на кнопку **Настройки подключения**.
7. Настройте параметры подключения к серверам:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу Central Node.
   - **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

- **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

  Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

8. Нажмите на кнопку **OK**.
9. Добавьте серверы Central Node. Для этого укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.
10. Вы можете добавить несколько адресов сервера Central Node. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.
11. Если требуется, настройте параметры отправки телеметрии.
12. Сохраните внесенные изменения.

В результате компьютер будет добавлен в консоли Kaspersky Anti Targeted Attack Platform. Проверьте статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Network Detection and Response (KATA)**.

Интеграция EDR-агента с EDR Expert (on-premises)

EDR-агент устанавливается на рабочие станции и серверы в IT-инфраструктуре организации. На этих компьютерах EDR-агент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправляет данные наблюдения на сервер EDR Expert (on-premises).

Для интеграции с EDR Expert (on-premises) вам нужно включить компонент Endpoint Detection and Response Expert (on-premises) и настроить параметры EDR-агента.

Интеграция с Endpoint Detection and Response Expert (on-premises) состоит из следующих этапов:

1. **Активация Endpoint Detection and Response Expert (on-premises)**

   Вам нужно приобрести отдельную лицензию на использование EDR Expert (on-premises) (Kaspersky Endpoint Detection and Response Expert (on-premises) Add-on).

   Функциональность будет доступна после добавления отдельного ключа Kaspersky Endpoint Detection and Response Expert (on-premises). Лицензирование отдельной функциональности Endpoint Detection and Response Expert (on-premises) не отличается от лицензирования Kaspersky Endpoint Security.

Убедитесь, что функциональность EDR Expert (on-premises) включена в лицензию и работает в локальном интерфейсе приложения.

2 Подключение к серверу сбора телеметрии и серверу реагирования

Для работы Kaspersky Endpoint Detection and Response Expert (on-premises) необходимо установить доверенное соединение между Kaspersky Endpoint Security и двумя серверами:

- *Сервер сбора телеметрии* – сервер, входящий в состав SIEM, который предназначен для сбора, нормализации, корреляции, анализа и хранения данных о событиях на компьютере.
- *Сервер реагирования* – сервер, который предназначен для приема и проверки данных, исследования поведения объектов, а также публикации результатов исследования.

Для обеспечения безопасности соединения вам необходимы следующие сертификаты:

- Сертификат сервера. TLS-сертификат, предназначенный для установки доверенного соединения с сервером. При ручной настройке подключения к серверу вам необходимо добавить сертификат в настройках компонента Endpoint Detection and Response Expert (on-premises). Если вы выбрали сервер из списка, сертификат будет загружен автоматически.
- Сертификат клиента. По умолчанию серверы OSMP запрашивают клиентский сертификат для выполнения двусторонней аутентификации. При ручной настройке подключения к серверу вам необходимо включить двустороннюю аутентификацию в настройках компонента Endpoint Detection and Response Expert (on-premises) и добавить сертификат клиента (криптоконтейнер с сертификатом и закрытым ключом). Если вы выбрали сервер из списка, сертификат будет загружен автоматически.

Вы можете получить сертификаты в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).

Как подключить компьютер с Kaspersky Endpoint Security к EDR Expert (on-premises) в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response Expert (on-premises)**.
5. Включите переключатель **Endpoint Detection and Response Expert (on-premises) ВКЛЮЧЕН**.
6. Для настройки EDR Expert (on-premises) в списке решений выберите **Endpoint Detection and Response Expert (версия 8.0 и выше)**.

7. Настройте подключение к *серверам сбора телеметрии*.

a. В блоке **Подключение к серверам сбора телеметрии** перейдите по ссылке **Настройки подключения**.

b. Настройте параметры подключения:

- **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу.
- **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером. Вы можете получить TLS-сертификат в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).
- **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером. По умолчанию серверы OSMP запрашивают клиентский сертификат для выполнения двусторонней аутентификации. Включите функцию двусторонней аутентификации и загрузите защищенный паролем криптоконтейнер. Вы можете получить криптоконтейнер в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).

  Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

c. Нажмите на кнопку **OK**.

d. Выберите сервер сбора телеметрии из списка доступных серверов или добавьте сервер вручную. Выбор сервера доступен, если компьютер находится под управлением OSMP.

e. Если вы хотите добавить сервер из списка, нажмите на кнопку **Добавить** и в выпадающем списке выберите **Выбрать сервер**. В открывшемся окне выберите нужный сервер сбора телеметрии.

Если вы ранее добавили TLS-сертификат, он будет заменен TLS-сертификатом выбранного сервера.

f. Для добавления сервера вручную нажмите на кнопку **Добавить** и в выпадающем списке выберите **Новый сервер**.

Если выбор серверов недоступен, выпадающий список отображаться не будет. Для добавления сервера вручную нажмите на кнопку **Добавить**.

Откроется форма добавления сервера.

g. Выберите протокол для подключения к серверу:

- **TCP** – отправка необработанного потока данных о событиях по протоколу TCP.
- **TCP / TLS** – отправка необработанного потока данных о событиях с использованием шифрования TLS.
- **HTTP/HTTPS** – отправка данных о событиях в формате HTTP-сообщений по протоколу TCP. Для HTTPS используется TLS-шифрование.

h. Введите адрес сервера (IPv4, IPv6, FQDN), а также порт подключения к серверу (по умолчанию 443).

При вводе адреса сервера учитывайте следующие особенности:

- **TCP**. Вы можете указывать как IP-адрес, так и FQDN-имя сервера.
- **TCP / TLS**. Необходимо указывать только FQDN-имя сервера.
- **HTTP/HTTPS**. Вам необходимо вручную указать протокол (HTTP или HTTPS) в адресе сервера (например, `https://server.com` или `http://10.10.10.100`).

i. При использовании протоколов TCP или TCP/TLS, вы можете настроить метод сжатия передаваемых данных:

- **Выключено** – отправка данных без сжатия;
- **GZIP** – сжатие передаваемых данных с использованием метода GZIP.

> Сжатие телеметрии для протоколов TCP и TCP/TLS доступно для Kaspersky Endpoint Security версии 14.3 и выше. Для более ранних версий приложения мы рекомендуем также настроить подключение к данном серверу с использованием протокола HTTPS, так как некоторые данные телеметрии могут быть потеряны.

j. Нажмите на кнопку **OK**.

Вы можете добавить несколько серверов. Kaspersky Endpoint Security пытается установить соединение с первым сервером из списка. Если установить соединение не удалось, выполняется попытка подключения ко второму серверу и так далее по списку.

k. Если требуется, настройте параметры отправки телеметрии.

8. Настройте подключение к *серверам реагирования*:

a. В блоке **Подключение к серверам реагирования** настройте параметр **Отправлять запрос на синхронизацию на сервер каждые (мин.)**. Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Endpoint Security получает задачи по реагированию на угрозы и отправляет результаты выполнения задач.

b. Перейдите по ссылке **Настройки подключения**.

c. Настройте параметры подключения:

- **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу.
- **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером. Вы можете получить TLS-сертификат в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером. По умолчанию серверы OSMP запрашивают клиентский сертификат для выполнения двусторонней аутентификации. Включите функцию двусторонней аутентификации и загрузите защищенный паролем криптоконтейнер. Вы можете получить криптоконтейнер в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).

  Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

d. Нажмите на кнопку **OK**.

e. Выберите сервер реагирования из списка доступных серверов или добавьте сервер вручную. Список серверов доступен, если компьютер находится под управлением OSMP.

f. Если вы хотите добавить сервер из списка, нажмите на кнопку **Добавить** и в выпадающем списке выберите **Выбрать сервер**. В открывшемся окне выберите нужный сервер реагирования.

   Если вы ранее добавили TLS-сертификат, он будет заменен TLS-сертификатом выбранного сервера.

g. Для добавления нового сервера вручную нажмите на кнопку **Добавить** и в выпадающем списке выберите **Новый сервер**.

   Если выбор серверов недоступен, выпадающий список отображаться не будет. Для добавления сервера нажмите на кнопку **Добавить**.

   Откроется форма добавления сервера.

h. Укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.

   Вы можете добавить несколько серверов реагирования. Kaspersky Endpoint Security пытается установить соединение с первым сервером из списка. Если установить соединение не удалось, Kaspersky Endpoint Security подключается ко второму серверу и так далее по списку.

9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Вы можете проверить статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Endpoint Detection and Response Expert (on-premises)**.

Совместимость со сторонними EPP-приложениями

EDR-агент предназначен для работы решений Detection and Response от "Лаборатории Касперского". Компоненты защиты и контроля для EDR-агента недоступны. Эта конфигурация позволяет устанавливать EPP-приложения от сторонних поставщиков и развернуть решения Detection and Response от "Лаборатории Касперского" в инфраструктуре организации.

EDR-агент совместим с EPP-приложениями от следующих поставщиков:

- **Dr.Web**

  EDR-агент совместим с Агентом Dr.Web для Windows версии 13 и Сервером Dr.Web (x64) 13.0.0.10200.

- **Dallas Lock**

  EDR-агент совместим с СЗИ Dallas Lock 8.0-C версии 843.2.

  > Для работы EDR-агента на компьютере, на котором развернуто программное обеспечение Dallas Lock, необходимо в параметрах модуля Межсетевой экран разрешить соединения с внешними службами "Лаборатории Касперского".

- **Secret Net Studio**

  EDR-агент совместим с СЗИ Secret Net Studio версии 8.11 (20851).

  > Невозможно установить приложение на компьютер, на котором развернуто программное обеспечение Secret Net Studio с компонентом Антивирус. Для совместной работы приложений вам нужно удалить компонент Антивирус из состава Secret Net Studio.

- **Trend Micro**

  EDR-агент совместим с Trend Micro Vision One (включая Security Agent 14.0.20731).

  EDR-агент совместим с Trend Micro Deep Security версии 20.0.3-18160 (включая Security Agent).

- **Windows Defender**

- **Sophos**

  EDR-агент совместим с Sophos Intercept X версии 2024.1.2 (включая Endpoint Agent) и Sophos Core Agent версии 2026.2.1.3.

- **Bitdefender**

  EDR-агент совместим с Bitdefender Endpoint Security Tools версии 8.26.7.647.

- **ESET**

  EDR-агент совместим с ESET Endpoint Security версии 13.0.2044.0 и ESET Management Agent версии 13.2.1189.0.

> На компьютерах под управлением Windows 11 для Arm64 EDR-агент не совместим с Bitdefender Endpoint Security Tools.

Следует устанавливать приложения в следующем порядке: сначала установите EPP-приложение, затем Агент администрирования Kaspersky Security Center, далее EDR-агент. Это связано с тем, что установщик EPP-приложения может определить EDR-агент и Агент администрирования как несовместимое ПО и удалить приложения. Также следует проверять работу EDR-агента и Агента администрирования после обновления стороннего EPP-приложения, так как установщик повторно проверяет компьютер на несовместимое ПО и может удалить приложения.

Если вам не удалось установить EDR-агент на компьютер со сторонним EPP-приложением из-за того, что установщик обнаружил на компьютере несовместимое ПО, вы можете пропустить проверку на несовместимое ПО.

Managed Detection and Response



Kaspersky Endpoint Security для Windows поддерживает работу с решением Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* – решение, которое автоматически обнаруживает и анализирует инциденты безопасности в вашей инфраструктуре. Для этого MDR использует данные телеметрии, полученные от конечных точек, и машинное обучение. Данные об инцидентах MDR передает экспертам "Лаборатории Касперского". Далее эксперты могут самостоятельно обработать инцидент и, например, добавить новую запись в антивирусные базы. Или эксперты могут дать рекомендации по обработке инцидента и, например, предложить изолировать компьютер от сети. Подробную информацию о работе решения см. в справке Kaspersky Managed Detection and Response.

Конфигурации Kaspersky Endpoint Security для работы с MDR

Для работы с MDR предусмотрены следующие конфигурации:

- **[KES+встроенный агент]**. В этой конфигурации Kaspersky Endpoint Security является и приложением, которое обеспечивает безопасность компьютера, и приложением для работы с MDR.
- **[стороннее EPP+EDR-агент]**. В этой конфигурации безопасность IT-инфраструктуры обеспечивает система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков. Работу с MDR обеспечивает Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента (EDR-агент). В этой конфигурации EDR-агента совместим со сторонними EPP-приложениями.

Интеграция встроенного агента с MDR

Для интеграции с Kaspersky Managed Detection and Response вам нужно включить компонент Managed Detection and Response и настроить параметры Kaspersky Endpoint Security.

Для работы Kaspersky Managed Detection and Response с Сервером администрирования через Kaspersky Security Center Web Console вам нужно установить новое безопасное соединение – *фоновое соединение*. Kaspersky Managed Detection and Response предлагает установить фоновое соединение при развертывании решения. Убедитесь, что фоновое соединение установлено.

Как установить фоновое соединение в Web Console

1. В главном окне Web Console выберите **Параметры** → **Интеграция**.
2. Перейдите в раздел **Интеграция**.
3. Включите переключатель **Фоновое соединение для интеграции Включено**.
4. Сохраните внесенные изменения.

Интеграция с Kaspersky Managed Detection and Response состоит из следующих этапов:

1. **Установка компонента Managed Detection and Response**

Вы можете выбрать компонент MDR во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

Для установки компонента Managed Detection and Response без перезагрузки компьютера с помощью задачи *Изменение состава компонентов приложения* вам необходимо выключить функцию **Проверять на наличие несовместимых приложений сторонних производителей** в настройках задачи.

2 Настройка Kaspersky Private Security Network

Если вы используете Kaspersky Security Center Cloud Console, этот шаг нужно пропустить. Kaspersky Security Center Cloud Console автоматически настраивает Kaspersky Private Security Network при установке плагина MDR.

Kaspersky Private Security Network (KPSN) – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров.

Загрузите конфигурационный файл Kaspersky Security Network в свойствах Сервера администрирования. Конфигурационный файл Kaspersky Security Network находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробнее о настройке Kaspersky Private Security Network см. в справке Kaspersky Security Center. Также вы можете загрузить конфигурационный файл Kaspersky Security Network на компьютер из командной строки (см. инструкцию ниже).

Как настроить Kaspersky Private Security Network из командной строки

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Выполните команду:

```
avp.com KSN /private <file name>
```

где `<file name>` – имя конфигурационного файла с параметрами Kaspersky Private Security Network (формат файла PKCS7 или PEM).

Пример:
```
avp.com KSN /private C:\kpsn_config.pkcs7
```

В результате Kaspersky Endpoint Security будет использовать Kaspersky Private Security Network для определения репутации файлов, приложений и веб-сайтов. В параметрах политики в разделе **Kaspersky Security Network** будет указан статус работы *Инфраструктура: Kaspersky Private Security Network*.

Для работы Managed Detection and Response необходимо включить расширенный режим KSN.

3 Активация Kaspersky Managed Detection and Response

Начиная с версии Kaspersky Endpoint Security для Windows 12.10 для активации функциональности Managed Detection and Response кроме кода активации вы также можете использовать файл ключа.

Kaspersky Managed Detection and Response поддерживает следующие способы лицензирования:

- Функциональность Managed Detection and Response включена в состав лицензии на использование Kaspersky Endpoint Security для Windows.

  Функциональность будет доступна сразу после активации Kaspersky Endpoint Security для Windows.

- Отдельная лицензия на использование MDR (Kaspersky Managed Detection and Response Add-on).

  Функциональность будет доступна после добавления отдельного ключа Kaspersky Managed Detection and Response Add-on. В результате на компьютере будет добавлено два ключа: ключ для Kaspersky Endpoint Security и ключ для Kaspersky Managed Detection and Response.

  Лицензирование отдельной функциональности Managed Detection and Response не отличается от лицензирования Kaspersky Endpoint Security.

Убедитесь, что функциональность MDR включена в лицензию и работает в локальном интерфейсе приложения.

4. **Включение компонента Managed Detection and Response**

Загрузите конфигурационный файл BLOB в политике Kaspersky Endpoint Security (см. инструкцию ниже). BLOB-файл содержит идентификатор клиента и информацию о лицензии Kaspersky Managed Detection and Response. BLOB-файл находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробную информацию о BLOB-файле см. в справке Kaspersky Managed Detection and Response.

Начиная с версии Kaspersky Endpoint Security для Windows 12.6 в Kaspersky Managed Detection and Response без тенантов при наличии действующей лицензии добавлять BLOB-файл не обязательно.

Как включить компонент Managed Detection and Response в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Установите флажок **Managed Detection and Response (Industrial CyberSecurity)**.
5. В блоке **Настройка** нажмите на кнопку **Загрузить** и выберите BLOB-файл, полученный в Консоли Kaspersky Managed Detection and Response. Файл имеет расширение P7.

   По умолчанию изменение параметров приложения пользователем разрешено (замок открыт). Для применения политики на компьютерах, закройте замки.

6. Сохраните внесенные изменения.

Как включить компонент Managed Detection and Response в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Встроенные агенты → Managed Detection and Response**.
5. Включите переключатель **Managed Detection and Response ВКЛЮЧЕН**.
6. Нажмите на кнопку **Загрузить** и выберите BLOB-файл, полученный в Консоли Kaspersky Managed Detection and Response. Файл имеет расширение P7.

   По умолчанию изменение параметров политики пользователем разрешено (замок открыт). Для применения политики на компьютерах, закройте замки .
7. Сохраните внесенные изменения.

Как включить компонент Managed Detection and Response из командной строки

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Выполните команду:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение **Настройка приложения**.

В результате Kaspersky Endpoint Security проверит BLOB-файл. Проверка BLOB-файла включает в себя проверку цифровой подписи и срока действия лицензии. Если BLOB-файл прошел проверку, Kaspersky Endpoint Security загрузит файл и отправит файл на компьютер при следующей синхронизации с Kaspersky Security Center. Проверьте статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Managed Detection and Response**.

5 Настройка других компонентов приложения для получения телеметрии

Для работы Managed Detection and Response должны быть включены следующие компоненты:

- Kaspersky Security Network (расширенный режим).
- Анализ поведения.
- Защита от эксплойтов.
- Защита от веб-угроз.
- Защита от почтовых угроз.
- Защита от файловых угроз.
- Защита от сетевых угроз.
- Сетевой экран.
- AMSI-защита.

- Фоновая проверка.

  1. В главном окне Web Console выберите **Управление активами** → **Политики**.
  2. Нажмите на название политики Kaspersky Endpoint Security.

     Откроется окно свойств политики.
  3. Выберите вкладку **Параметры приложения**.
  4. Перейдите в раздел **Встроенные агенты** → **Managed Detection and Response**.
  5. Включите переключатель **Managed Detection and Response ВКЛЮЧЕН**.
  6. Сохраните внесенные изменения.

  1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
  2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
  3. В окне политики выберите **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
  4. Установите флажок **Managed Detection and Response (Industrial CyberSecurity)**.
  5. Сохраните внесенные изменения.

Руководство по миграции с KEA на KES для MDR

В Kaspersky Endpoint Security для Windows включен встроенный агент для работы решения Kaspersky Managed Detection and Response. Теперь вам не нужно отдельное приложение Kaspersky Endpoint Agent для работы MDR. Все функции Kaspersky Endpoint Agent будет выполнять Kaspersky Endpoint Security.

При развертывании Kaspersky Endpoint Security на компьютеры с установленным приложением Kaspersky Endpoint Agent решение Kaspersky Managed Detection and Response продолжит работу с Kaspersky Endpoint Security. Также приложение Kaspersky Endpoint Agent будет удалено с компьютера. Такое же поведение в системе будет при обновлении Kaspersky Endpoint Security до версии 11.6.0 или выше.

> Kaspersky Endpoint Security несовместим с Kaspersky Endpoint Agent. Установить оба этих приложения на одном компьютере невозможно.

Для работы Kaspersky Endpoint Security в составе Kaspersky Managed Detection and Response должны быть выполнены следующие условия:

- Kaspersky Security Center версии 13.2 или выше (включая Агент администрирования). В более ранних версиях Kaspersky Security Center невозможно активировать функциональность Managed Detection and Response.
- Установлено фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования. Для работы MDR с Сервером администрирования через Kaspersky Security Center Web Console вам нужно установить новое безопасное соединение – *фоновое соединение*.

Этапы миграции конфигурации [KES+KEA] на [KES+встроенный агент] для MDR

1. **Обновление плагина управления Kaspersky Endpoint Security**

   Управление компонентом MDR доступно с помощью плагина управления Kaspersky Endpoint Security версии 11.6 или выше. В зависимости от консоли Kaspersky Security Center, которую вы используете, обновите плагин управления в Консоли администрирования (MMC) или веб-плагин в Web Console.

2. **Миграция политик и задач**

   Перенесите параметры работы Kaspersky Endpoint Agent в приложение Kaspersky Endpoint Security для Windows. Вам доступны следующие способы:

   - Мастер миграции с Kaspersky Endpoint Agent. Мастер миграции с Kaspersky Endpoint Agent работает только в Web Console.

     Как перенести параметры политик и задач с помощью Мастера миграции с Kaspersky Endpoint Agent в Web Console

     В главном окне Web Console выберите **Операции** → **Миграция с Kaspersky Endpoint Agent**.

     В результате запустится мастер миграции политик и задач. Следуйте его указаниям.

     Шаг 1. Миграция политик

     Мастер миграции создает новую политику, в которой будут объединены параметры политик Kaspersky Endpoint Security и Kaspersky Endpoint Agent. В списке политик выберите политики Kaspersky Endpoint Agent, параметры которых вы хотите объединить с политикой Kaspersky Endpoint Security. Нажмите на политику Kaspersky Endpoint Agent, чтобы выбрать политику Kaspersky Endpoint Security, с которой вы хотите объединить параметры. Убедитесь, что политики выбраны верно и перейдите к следующем шагу.

     Шаг 2. Миграция задач

     Мастер миграции не поддерживает задачи MDR. Пропустите этот шаг.

     Шаг 3. Завершение работы мастера

     Завершите работу мастера. В результате работы мастера будет создана новая политика Kaspersky Endpoint Security. В политике объединены параметры Kaspersky Endpoint Security и Kaspersky Endpoint Agent. Политика называется *<Название политики Kaspersky Endpoint Security> & <Название политики Kaspersky Endpoint Agent>*. Новая политика имеет статус *Неактивна*. Для продолжения работы измените статусы политик Kaspersky Endpoint Agent и Kaspersky Endpoint Security на *Неактивна* и активируйте новую объединенную политику.

   - Стандартный Мастер массовой конвертации политик и задач. Мастер массовой конвертации политик и задач доступен в Консоли администрирования (MMC). Подробнее о Мастере массовой конвертации политик и задач см. в справке Kaspersky Security Center.

3 Лицензирование функций MDR

Для активации Kaspersky Endpoint Security в составе решения Kaspersky Managed Detection and Response вам потребуется отдельная лицензия Kaspersky Managed Detection and Response Add-on. Вы можете добавить ключ с помощью задачи *Добавление ключа*. Таким образом, в приложение будет добавлено два ключа: *Kaspersky Endpoint Security* и *Kaspersky Managed Detection and Response*.

4 Установка / Обновление версии приложения Kaspersky Endpoint Security

Для миграции функций MDR во время установки или обновления приложения рекомендуется использовать задачу удаленной установки. При создании задачи удаленной установки вам нужно выбрать компонент MDR в параметрах инсталляционного пакета.

Также вы можете обновить приложение следующими способами:

- Через службу обновлений "Лаборатории Касперского".
- Локально с помощью мастера установки.

Kaspersky Endpoint Security поддерживает автоматический выбор компонентов при обновлении приложения на компьютере с установленным приложением Kaspersky Endpoint Agent. Автоматический выбор компонентов зависит от прав учетной записи пользователя, который обновляет приложение.

Если вы обновляете Kaspersky Endpoint Security с помощью EXE-файла или с помощью MSI-файла под системной учетной записью (SYSTEM), Kaspersky Endpoint Security получает доступ к действующим лицензиям решений "Лаборатории Касперского". Таким образом, если на компьютере установлено приложение Kaspersky Endpoint Agent и активировано решение MDR, установщик Kaspersky Endpoint Security автоматически сконфигурирует набор компонентов и выберет компонент MDR. При этом Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent. Запуск установщика MSI под системной учетной записью (SYSTEM) обычно выполняется при обновлении через службу обновлений "Лаборатории Касперского" или при развертывании инсталляционного пакета через Kaspersky Security Center.

Если вы обновляете Kaspersky Endpoint Security с помощью MSI-файла под учетной записью непривилегированного пользователя, у Kaspersky Endpoint Security отсутствует доступ к действующим лицензиям решений "Лаборатории Касперского". При этом Kaspersky Endpoint Security автоматически выбирает компоненты на основании состава компонентов Kaspersky Endpoint Agent. Далее Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent.

Kaspersky Endpoint Security поддерживает обновление без перезагрузки компьютера. Вы можете выбрать режим обновления приложения в параметрах политики.

5 Проверка работы приложения

Если после установки или обновления приложения компьютер имеет статус *Критический* в консоли Kaspersky Security Center, выполните следующие действия:

- Убедитесь, что на компьютере установлен Агент администрирования версии 13.2 или выше.
- Проверьте статус работы встроенного агента с помощью отчета *Отчет о статусе компонентов приложения*. Если компонент имеет статус *Не установлен*, установите компонент с помощью задачи *Изменение состава компонентов приложения*. Если компонент имеет статус *Не поддерживается лицензией*, убедитесь, что вы активировали функцию встроенного агента.
- Убедитесь, что вы приняли условия Положения о Kaspersky Security Network в новой политике Kaspersky Endpoint Security для Windows.

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security для Windows поддерживает работу с решением Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* – решение для кибербезопасности бизнеса, которое включает в себя приложения "Лаборатории Касперского", с помощью которых организация получает возможность защититься от большинства киберрисков и покрыть основные сценарии распространения угроз. Компоненты EDR Expert (on-premises) развернуты на единой платформе управления Open Single Management Platform (OSMP). Платформа обеспечивает выполнение кросс-программных сценариев в рамках единого интерфейса и позволяет интегрировать приложения "Лаборатории Касперского" и приложения сторонних производителей в единую систему безопасности.

Один из центральных элементов решения – *SIEM*. SIEM позволяет отслеживать события, полученные от всех компонентов, и выполняет взаимную корреляцию этих событий с помощью готовых и пользовательских правил. На основании журналов и телеметрии, полученных от инфраструктуры организации, EDR Expert (on-premises) автоматически выявляет атаки и позволяет проводить расследование инцидентов с помощью единого графа расследования, который комбинирует все собираемые в EDR Expert (on-premises) события – как от приложений "Лаборатории Касперского", так и от сторонних ИБ-продуктов.

Для реагирования на сложные инциденты EDR Expert (on-premises) использует предустановленные и пользовательские сценарии. Также доступны действия по реагированию от приложений сторонних производителей и сценарии реагирования, в которых задействовано несколько приложений.

Средства анализа угроз

Kaspersky Endpoint Detection and Response использует следующие средства анализа угроз (Threat Intelligence):

- Интеграция с Kaspersky Threat Intelligence Portal, который содержит и отображает информацию о репутации файлов и веб-адресов.
- База угроз "Лаборатории Касперского" Kaspersky Threats.
- Инфраструктура облачных служб Kaspersky Security Network (далее также "KSN"), предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Принцип работы решения

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами.

Kaspersky Endpoint Security, установленное в стандартном режиме в инфраструктуре VDI, поддерживает работу с EDR Expert (on-premises). При этом работоспособность остальных функций приложения не гарантируется. Для защиты виртуальных машин в инфраструктуре VDI рекомендуется использовать Kaspersky Endpoint Security в режиме Легкого агента.

Данные о событиях на компьютере (телеметрия) отправляются на сервер EDR Expert (on-premises). Приложение Kaspersky Endpoint Security также передает на сервер сбора телеметрии данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

Настройка интеграции с EDR Expert (on-premises) выполняется в консоли Kaspersky Security Center. Дальнейшее управление встроенным агентом осуществляется в единой платформе управления OSMP, включая запуск задач, управление объектами на карантине, просмотр отчетов и другие действия.

Конфигурации Kaspersky Endpoint Security для работы с EDR Expert (on-premises)

Для работы с EDR Expert (on-premises) предусмотрены следующие конфигурации:

- **[KES+встроенный агент]**. В этой конфигурации Kaspersky Endpoint Security является и приложением, которое обеспечивает безопасность компьютера, и приложением для работы с EDR Expert (on-premises). Встроенный агент для EDR Expert (on-premises) доступен в Kaspersky Endpoint Security для Windows версии 12.11 и выше.

- **[стороннее EPP+EDR-агент]**. В этой конфигурации безопасность IT-инфраструктуры обеспечивает система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков. Работу с EDR Expert (on-premises) обеспечивает Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента (EDR-агент). В этой конфигурации EDR-агент совместим со сторонними EPP-приложениями. EDR-агент для EDR Expert (on-premises) доступен в Kaspersky Endpoint Security для Windows версии 12.11 и выше.

Интеграция встроенного агента с EDR Expert (on-premises)

Для интеграции с решением Kaspersky Endpoint Detection and Response Expert (on-premises) вам нужно добавить компонент Endpoint Detection and Response Expert (on-premises) и настроить параметры Kaspersky Endpoint Security.

> Компоненты Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), Endpoint Detection and Response Expert (on-premises) несовместимы между собой.

Для работы Endpoint Detection and Response Expert (on-premises) должны быть выполнены следующие условия:

- Установлена единая платформа управления OSMP (Open Single Management Platform).
- Приложение активировано и функциональность входит в лицензию.
- Компонент Endpoint Detection and Response Expert (on-premises) включен.
- Компоненты приложения, которые обеспечивают работу EDR Expert (on-premises), включены и работают. Работу EDR Expert (on-premises) обеспечивают следующие компоненты:
  - Защита от файловых угроз.
  - Защита от веб-угроз.
  - Защита от почтовых угроз.

- Защита от эксплойтов.
- Анализ поведения.
- Предотвращение вторжений.
- Откат вредоносных действий.
- Адаптивный контроль аномалий.

Интеграция с EDR Expert (on-premises) состоит из следующих этапов:

1. **Установка компонента EDR Expert (on-premises)**

   Вы можете выбрать компонент EDR Expert (on-premises) во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

   > Для завершения обновления приложения с новым компонентом нужно перезагрузить компьютер.

2. **Активация Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Вам нужно приобрести отдельную лицензию на использование EDR Expert (on-premises) (Kaspersky Endpoint Detection and Response Expert (on-premises) Add-on).

   Функциональность будет доступна после добавления отдельного ключа Kaspersky Endpoint Detection and Response Expert (on-premises). В результате на компьютере будет добавлено два ключа: ключ для Kaspersky Endpoint Security и ключ для Kaspersky Endpoint Detection and Response Expert (on-premises).

   Лицензирование отдельной функциональности Endpoint Detection and Response Expert (on-premises) не отличается от лицензирования Kaspersky Endpoint Security.

   Убедитесь, что функциональность EDR Expert (on-premises) включена в лицензию и работает в локальном интерфейсе приложения.

3. **Подключение к серверу сбора телеметрии и серверу реагирования**

   Для работы Kaspersky Endpoint Detection and Response Expert (on-premises) необходимо установить доверенное соединение между Kaspersky Endpoint Security и двумя серверами:

   - *Сервер сбора телеметрии* – сервер, входящий в состав SIEM, который предназначен для сбора, нормализации, корреляции, анализа и хранения данных о событиях на компьютере.
   - *Сервер реагирования* – сервер, который предназначен для приема и проверки данных, исследования поведения объектов, а также публикации результатов исследования.

   Для обеспечения безопасности соединения вам необходимы следующие сертификаты:

   - Сертификат сервера. TLS-сертификат, предназначенный для установки доверенного соединения с сервером. При ручной настройке подключения к серверу вам необходимо добавить сертификат в настройках компонента Endpoint Detection and Response Expert (on-premises). Если вы выбрали сервер из списка, сертификат будет загружен автоматически.
   - Сертификат клиента. По умолчанию серверы OSMP запрашивают клиентский сертификат для выполнения двусторонней аутентификации. При ручной настройке подключения к серверу вам необходимо включить двустороннюю аутентификацию в настройках компонента Endpoint Detection and Response Expert (on-premises) и добавить сертификат клиента (криптоконтейнер с сертификатом и закрытым ключом). Если вы выбрали сервер из списка, сертификат будет загружен автоматически.

   Вы можете получить сертификаты в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).

Как подключить компьютер с Kaspersky Endpoint Security к EDR Expert (on-premises) в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response Expert (on-premises)**.
5. Включите переключатель **Endpoint Detection and Response Expert (on-premises) ВКЛЮЧЕН**.
6. Для настройки EDR Expert (on-premises) в списке решений выберите **Endpoint Detection and Response Expert (версия 8.0 и выше)**.
7. Настройте подключение к *серверам сбора телеметрии*.

   a. В блоке **Подключение к серверам сбора телеметрии** перейдите по ссылке **Настройки подключения**.

   b. Настройте параметры подключения:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу.
   - **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером. Вы можете получить TLS-сертификат в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).
   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером. По умолчанию серверы OSMP запрашивают клиентский сертификат для выполнения двусторонней аутентификации. Включите функцию двусторонней аутентификации и загрузите защищенный паролем криптоконтейнер. Вы можете получить криптоконтейнер в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).

     Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

   c. Нажмите на кнопку **OK**.

   d. Выберите сервер сбора телеметрии из списка доступных серверов или добавьте сервер вручную. Выбор сервера доступен, если компьютер находится под управлением OSMP.

   e. Если вы хотите добавить сервер из списка, нажмите на кнопку **Добавить** и в выпадающем списке выберите **Выбрать сервер**. В открывшемся окне выберите нужный сервер сбора телеметрии.

   Если вы ранее добавили TLS-сертификат, он будет заменен TLS-сертификатом выбранного сервера.

   f. Для добавления сервера вручную нажмите на кнопку **Добавить** и в выпадающем списке выберите **Новый сервер**.

Если выбор серверов недоступен, выпадающий список отображаться не будет. Для добавления сервера вручную нажмите на кнопку **Добавить**.

Откроется форма добавления сервера.

g. Выберите протокол для подключения к серверу:

- **TCP** – отправка необработанного потока данных о событиях по протоколу TCP.
- **TCP / TLS** – отправка необработанного потока данных о событиях с использованием шифрования TLS.
- **HTTP/HTTPS** – отправка данных о событиях в формате HTTP-сообщений по протоколу TCP. Для HTTPS используется TLS-шифрование.

h. Введите адрес сервера (IPv4, IPv6, FQDN), а также порт подключения к серверу (по умолчанию 443).

При вводе адреса сервера учитывайте следующие особенности:

- **TCP**. Вы можете указывать как IP-адрес, так и FQDN-имя сервера.
- **TCP / TLS**. Необходимо указывать только FQDN-имя сервера.
- **HTTP/HTTPS**. Вам необходимо вручную указать протокол (HTTP или HTTPS) в адресе сервера (например, `https://server.com` или `http://10.10.10.100`).

i. При использовании протоколов TCP или TCP/TLS, вы можете настроить метод сжатия передаваемых данных:

- **Выключено** – отправка данных без сжатия;
- **GZIP** – сжатие передаваемых данных с использованием метода GZIP.

Сжатие телеметрии для протоколов TCP и TCP/TLS доступно для Kaspersky Endpoint Security версии 14.3 и выше. Для более ранних версий приложения мы рекомендуем также настроить подключение к данном серверу с использованием протокола HTTPS, так как некоторые данные телеметрии могут быть потеряны.

j. Нажмите на кнопку **OK**.

Вы можете добавить несколько серверов. Kaspersky Endpoint Security пытается установить соединение с первым сервером из списка. Если установить соединение не удалось, выполняется попытка подключения ко второму серверу и так далее по списку.

k. Если требуется, настройте параметры отправки телеметрии.

8. Настройте подключение к *серверам реагирования*:

   a. В блоке **Подключение к серверам реагирования** настройте параметр **Отправлять запрос на синхронизацию на сервер каждые (мин.)**. Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Endpoint Security получает задачи по реагированию на угрозы и отправляет результаты выполнения задач.

   b. Перейдите по ссылке **Настройки подключения**.

   c. Настройте параметры подключения:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу.
   - **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером. Вы можете получить TLS-сертификат в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).
   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером. По умолчанию серверы OSMP запрашивают клиентский сертификат для выполнения двусторонней аутентификации. Включите функцию двусторонней аутентификации и загрузите защищенный паролем криптоконтейнер. Вы можете получить криптоконтейнер в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).

     Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

   d. Нажмите на кнопку **OK**.

   e. Выберите сервер реагирования из списка доступных серверов или добавьте сервер вручную. Список серверов доступен, если компьютер находится под управлением OSMP.

   f. Если вы хотите добавить сервер из списка, нажмите на кнопку **Добавить** и в выпадающем списке выберите **Выбрать сервер**. В открывшемся окне выберите нужный сервер реагирования.

   Если вы ранее добавили TLS-сертификат, он будет заменен TLS-сертификатом выбранного сервера.

   g. Для добавления нового сервера вручную нажмите на кнопку **Добавить** и в выпадающем списке выберите **Новый сервер**.

   Если выбор серверов недоступен, выпадающий список отображаться не будет. Для добавления сервера нажмите на кнопку **Добавить**.

   Откроется форма добавления сервера.

h. Укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.

Вы можете добавить несколько серверов реагирования. Kaspersky Endpoint Security пытается установить соединение с первым сервером из списка. Если установить соединение не удалось, Kaspersky Endpoint Security подключается ко второму серверу и так далее по списку.

9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Вы можете проверить статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Endpoint Detection and Response Expert (on-premises)**.

Настройка отправки телеметрии EDR Expert (on-premises)

Телеметрия – список событий, которые произошли на защищаемом компьютере. Kaspersky Endpoint Security анализирует данные телеметрии и отправляет их на серверы сбора телеметрии во время синхронизации. Подробную информацию об отправляемых событиях телеметрии см. в справке Kaspersky Endpoint Detection and Response Expert (on-premises).

События телеметрии поступают на сервер почти непрерывно. Kaspersky Endpoint Security выполняет синхронизацию с сервером при выполнении любого из следующих условий:

- Истек период синхронизации.
- Количество событий в буфере превысило максимальное значение.

Таким образом, по умолчанию приложение выполняет синхронизацию каждые 30 секунд или при накоплении в буфере 1024 события. Вы можете настроить параметры синхронизации в политике Kaspersky Endpoint Security и выбрать оптимальные значения исходя из нагрузки на сеть (см. инструкцию ниже).

Если соединение между Kaspersky Endpoint Security и сервером отсутствует, то приложение ставит новые события в очередь. При восстановлении соединения Kaspersky Endpoint Security отправляет события из очереди на сервер по порядку. При этом, чтобы не перегрузить сервер, Kaspersky Endpoint Security может отправлять не все события. Для этого вы можете оптимизировать параметры отправки событий и, например, задать максимальное количество событий в час (см. инструкцию ниже).

Чтобы настроить параметры отправки телеметрии, выполните следующие действия:

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты → Endpoint Detection and Response Expert (on-premises)**.
5. Для настройки EDR Expert (on-premises) в списке решений выберите **Endpoint Detection and Response Expert (версия 8.0 и выше)**.
6. В блоке **Настройка передачи данных** убедитесь, что установлен флажок **Отправлять телеметрию на серверы сбора телеметрии**.

7. Если требуется, установите флажок **Отправлять телеметрию только с IOA**. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию *потоковой проверки*, которая позволяет отслеживать такие события в режиме реального времени.

8. Если требуется, в блоке **Настройка передачи данных** настройте параметры синхронизации с сервером:

   - **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд.

   - **Максимальное количество пакетов событий**. Приложение выполняет синхронизацию с сервером при заполнении буфера событиями. По умолчанию установлено значение 1024 события.

9. Если требуется, в блоке **Регулирование количества запросов** снимите флажок **Включить регулирование количества запросов**.

   Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события. По умолчанию функция включена.

10. Настройте параметры оптимизации отправки событий на сервер:

    - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

    - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Endpoint Security восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.

11. В блоке **Подключение к серверам реагирования** введите значение для параметра **Отправлять запрос на синхронизацию на сервер каждые (мин.)**.

12. Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Endpoint Security передает данные об изменениях в параметрах приложения и задачах.

13. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Фильтрация событий телеметрии EDR Expert (on-premises)

Для повышения производительности и оптимизации отправки данных на Сервер сбора телеметрии вы можете добавить исключения из телеметрии. Например, вы можете отменить обработку данных о сетевых коммуникациях для отдельных приложений.

Использование слишком большого количества правил может привести к увеличению нагрузки на Сервер сбора телеметрии и снижению производительности компьютера. Рекомендуется добавлять только необходимые правила.

Чтобы создать исключение из телеметрии в Web Console и Cloud Console, выполните следующие действия:

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки телеметрии**.
5. Выберите вкладку **Телеметрия EDR Expert (on-premises)**.
6. В блоке **Общие исключения** нажмите на кнопку **Добавить**.

   Откроется окно **Добавление правила исключения**.
7. При необходимости измените статус правила. По умолчанию правило включено.
8. Введите имя правила.
9. Выберите действие, которое будет выполнено при срабатывании правила:
   - **Не собирать**. Отфильтрованное событие будет исключено из отправляемой телеметрии.
   - **Исключить IOA**. Из отправляемой телеметрии будет исключено событие о срабатывании IOA-правила.
10. Если выбран вариант **Исключить IOA**, укажите IOA-правила, которые необходимо добавить в исключения:
    - **Исключить все**. При выполнении заданного условия приложение будет исключать из телеметрии события, формируемые на основе всех IOA-правил.
    - **Исключить по GUID**. Укажите GUID IOA-правила. Вы можете указать несколько GUID через `,`. Подробную информацию об IOA-правилах см. в справке EDR Expert (on-premises).
11. Задайте условие фильтрации:
    a. Выберите название поля, по которому будет выполняться фильтрация.
    b. Выберите оператор (см. таблицу ниже), и укажите значение, с которым будет сравниваться значение поля из события.

Перечень операторов условий

Оператор	Описание
<	Если значение поля меньше значения, заданного в условии, событие будет отфильтровано.
≤	Если значение поля меньше или равно значению, заданному в условии, событие будет отфильтровано.
=	Если значение поля равно значению, заданному в условии, событие будет отфильтровано.
≥	Если значение поля больше или равно значению, заданному в условии, событие будет отфильтровано.
>	Если значение поля больше значения, заданного в условии, событие будет отфильтровано.
≠	Если значение поля не равно значению, заданному в условии, событие будет отфильтровано.
похоже	Если значение поля подходит под маску, указанную в условии, событие будет отфильтровано. Приложение поддерживает символы `*` и `?` для ввода маски.
не похоже	Если значение поля не подходит под маску, указанную в условии, событие будет отфильтровано. Приложение поддерживает символы `*` и `?` для ввода маски.

Оператор	Описание
одно из	Если значение поля совпадает с одним из значений из заданного в условии списка, событие считается отфильтрованным.
ни одного из	Если значение поля не совпадает ни с одним из значений из заданного в условии списка, событие считается отфильтрованным.
похоже на одно из	Если значение поля подходит под одну из масок, заданных в условии, событие будет отфильтровано. Приложение поддерживает символы `*` и `?` для ввода маски.
не похоже ни на одно из	Если значение поля не подходит ни под одну из масок, заданных в условии, событие будет отфильтровано. Приложение поддерживает символы `*` и `?` для ввода маски.
существует	Если указанное в условии поле содержится в событии, событие будет отфильтровано.
не существует	Если указанное в условии поле не содержится в событии, событие будет отфильтровано.
содержит	Если значение, заданное в условии, содержится в значении поля, событие будет отфильтровано.
равно	Если значение поля равно значению, заданному в условии, событие будет отфильтровано. Проверка выполняется без учета регистра.
И (побитовый)	Если результат операции "Побитовое И" (&) для значения поля и значения, указанного в условии, равен 1, событие будет отфильтровано.

12. При необходимости вы можете формировать сложные критерии фильтрации, добавляя несколько условий фильтрации и групп условий. Также в группу условий вы можете добавлять вложенные условия и группы условий. Вы можете использовать следующие операторы:

    - **И** – фильтр отбирает события, которые соответствуют всем указанным условиям.
    - **ИЛИ** – фильтр отбирает события, которые соответствуют одному из указанных условий.
    - **НЕ** (для использования данного оператора выберите вариант **Добавить НЕ перед**) – фильтр отбирает события, которые не соответствуют всем указанным условиям.

    Условия и группы условий первого уровня объединены с помощью оператора **И**.

13. Если компьютер находится под управлением OSMP, вам доступна проверка созданного правила фильтрации. Для выполнения проверки нажмите на кнопку **Проверить правило**.

    В открывшемся окне отобразится таблица событий, отфильтрованных с помощью созданного правила. Подробнее см. в справке EDR Expert (on-premises).

14. Если требуется, в блоке **Все типы событий** добавьте исключения из телеметрии по типу событий:

    a. Нажмите на название типа события.

    b. В открывшемся окне нажмите на кнопку **Настроить вручную**.

    c. При необходимости настройте отправку телеметрии по выбранному типу событий с помощью переключателя **Отправлять событие**. По умолчанию включена отправка телеметрии по всем типам событий.

    d. В блоке **Правила исключения** нажмите на кнопку **Добавить**.

    Откроется окно **Добавление правила исключения**.

    e. Выполните действия, описанные в шагах 7-13, для каждого добавляемого правила.

15. Для некоторых типов событий вы также можете добавить правила включения для расширения собираемой телеметрии:

    a. В блоке **Правила включения** нажмите на кнопку **Добавить**.

    Откроется окно **Добавление правила включения**.

    b. Введите имя правила.

    c. В блоке **Условие** введите значения для отображаемых полей. Тип доступных полей зависит от выбранного события.

    Для отправки событий чтения реестра Windows вам необходимо создать включающие фильтры с типом **Registry Query**, указав в поле **RegKeyName** название раздела реестра, а в поле **RegValueName** – название параметра. Использование масок не поддерживается. Для указания параметра `(Default)` вам необходимо в поле **RegValueName** ввести `/`.
    Включение отправки событий с типом **Registry Query** может снижать производительность приложения. Не рекомендуется создавать более 200 включающих фильтров для данного типа событий.

    Правила исключения имеют приоритет над правилами включения.

16. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Экспорт и импорт фильтров событий EDR Expert (on-premises)

Вы можете экспортировать список исключений в файл в формате JSON. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество идентификаторов событий. Также вы можете использовать функцию экспорта / импорта для резервного копирования фильтров событий или для миграции списка на другой сервер.

Использование слишком большого количества правил может привести к увеличению нагрузки на Сервер сбора телеметрии и снижению производительности компьютера. Рекомендуется добавлять только необходимые правила.

Как экспортировать / импортировать фильтры событий в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Общие настройки → Исключения и типы объектов**.
5. В блоке **Настройки телеметрии → Телеметрия EDR Expert (on-premises)** нажмите на кнопку **Настройка**.

6. Для экспорта фильтров событий выполните следующие действия:

   a. Нажмите на кнопку **Экспортировать**.

      В открывшемся окне введите имя файла формата JSON, в который вы хотите экспортировать фильтры событий, а также выберите папку, в которой вы хотите сохранить этот файл.

   b. Сохраните файл.

      Kaspersky Endpoint Security экспортирует фильтры событий в JSON-файл.

7. Для импорта фильтров событий выполните следующие действия:

   a. Нажмите на кнопку **Импортировать**.

   b. В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать фильтры событий.

   c. Откройте файл.

      Если на компьютере уже есть правила фильтрации событий, Kaspersky Endpoint Security заменит их при импорте.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как экспортировать / импортировать фильтры событий в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки → Настройки телеметрии**.

5. Выберите вкладку **Телеметрия EDR Expert (on-premises)**.

6. Для экспорта фильтров событий выполните следующие действия:

   a. Нажмите на кнопку **Экспортировать**.

   b. В открывшемся окне введите имя файла формата JSON, в который вы хотите экспортировать фильтры событий, а также выберите папку, в которой вы хотите сохранить этот файл.

   c. Сохраните файл.

      Kaspersky Endpoint Security экспортирует фильтры событий в JSON-файл.

7. Для импорта фильтров событий выполните следующие действия:

   a. Нажмите на кнопку **Импортировать**.

   b. В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать фильтры событий.

c. Выберите способ импорта правил фильтрации событий: добавить к существующим правилам или заменить существующие правила на новые.

d. Откройте файл.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Также вы можете экспортировать и импортировать фильтры событий из командной строки.

Особенности использования профилей политик для настройки интеграции с EDR Expert (on-premises) и EDR (KATA)

Для того, чтобы в рамках единой политики для одних групп администрирования настроить интеграцию с EDR (KATA), а для других – с EDR Expert (on-premises), вам необходимо использовать профили политики. Настройки интеграции с EDR (KATA) необходимо задавать в свойствах политики, а интеграцию с EDR Expert (on-premises) для выбранных групп администрирования следует настраивать в свойствах профилей политики.

Использование профилей политики для настройки интеграции с EDR Expert (on-premises) имеет следующие ограничения:

- Если вы настроите интеграцию с EDR Expert (on-premises) в свойствах политики, то эти настройки будут применяться для всех групп администрирования, настройки интеграции из профилей политики применяться не будут.

- При использовании профилей политики для настройки интеграции с EDR Expert (on-premises) вы не можете использовать Консоль администрирования (MMC) для работы с политиками. При открытии свойств политики в Консоли администрирования настройки интеграции с EDR Expert (on-premises) в профилях политики будут переопределены настройками из политики, компонент будет работать некорректно. Вам потребуется сбросить настройки компонента Endpoint Detection and Response Expert (on-premises) согласно инструкции ниже.

- При использовании профилей политики для настройки интеграции с EDR Expert (on-premises) вы не можете использовать дочерние политики.

Если у вас уже есть политика, настроенная в предыдущей версии веб-плагина, для применения на управляемых устройствах настроек интеграции с EDR Expert (on-premises) из профилей политики вам необходимо сбросить настройки компонента Endpoint Detection and Response Expert (on-premises).

Чтобы сбросить настройки компонента, выполните следующие действия:

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response Expert (on-premises)**.

5. Измените режим работы компонента с **Endpoint Detection and Response Expert (версия 7.1 и ниже)** на **Режим Endpoint Detection and Response Expert (версия 8.0 и выше)**.

6. Переключитесь обратно на **Endpoint Detection and Response Expert (версия 7.1 и ниже)**.

7. Сохраните внесенные изменения.

Endpoint Detection and Response Expert (cloud)

Интеграция Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (cloud) временно недоступна. Поддержка функциональности запланирована на конец 2026 года. Следите за нашими Release Notes, чтобы быть в курсе обновлений приложения и новых возможностей.



Kaspersky Endpoint Security поддерживает работу с решением Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* – облачное решение для кибербезопасности бизнеса, которое включает в себя приложения "Лаборатории Касперского", с помощью которых организация получает возможность защититься от большинства киберрисков и покрыть основные сценарии распространения угроз. Компоненты EDR Expert (cloud) развернуты на единой платформе управления Open Single Management Platform (OSMP). Платформа обеспечивает выполнение кросс-программных сценариев в рамках единого интерфейса и позволяет интегрировать приложения "Лаборатории Касперского" и приложения сторонних производителей в единую систему безопасности.

Один из центральных элементов решения – *SIEM*. SIEM позволяет отслеживать события, полученные от всех компонентов, и выполняет взаимную корреляцию этих событий с помощью готовых и пользовательских правил. На основании журналов и телеметрии, полученных от инфраструктуры организации, EDR Expert (cloud) автоматически выявляет атаки и позволяет проводить расследование инцидентов с помощью единого графа расследования, который комбинирует все собираемые в EDR Expert (cloud) события – как от приложений "Лаборатории Касперского", так и от сторонних ИБ-продуктов.

Для реагирования на сложные инциденты EDR Expert (cloud) использует предустановленные и пользовательские сценарии. Также доступны действия по реагированию от приложений сторонних производителей и сценарии реагирования, в которых задействовано несколько приложений.

Средства анализа угроз

Kaspersky Endpoint Detection and Response использует следующие средства анализа угроз (Threat Intelligence):

- Интеграция с Kaspersky Threat Intelligence Portal, который содержит и отображает информацию о репутации файлов и веб-адресов.
- База угроз "Лаборатории Касперского" Kaspersky Threats.
- Инфраструктура облачных служб Kaspersky Security Network (далее также "KSN"), предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Принцип работы решения

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами.

Данные о событиях на компьютере (телеметрия) отправляются на сервер EDR Expert (cloud). Приложение Kaspersky Endpoint Security также передает на сервер сбора телеметрии данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

Настройка интеграции с EDR Expert (cloud) выполняется в консоли Kaspersky Security Center. Дальнейшее управление встроенным агентом осуществляется в единой платформе управления OSMP, включая запуск задач, управление объектами на карантине, просмотр отчетов и другие действия.

Интеграция встроенного агента с EDR Expert (cloud)

Для интеграции с решением Kaspersky Endpoint Detection and Response Expert (cloud) вам нужно установить компонент Endpoint Detection and Response Expert (cloud) и настроить параметры Kaspersky Endpoint Security.

> Компоненты Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), Endpoint Detection and Response Expert (on-premises) несовместимы между собой.

Условия работы EDR Expert (cloud)

Для работы EDR Expert (cloud) должны быть выполнены следующие условия:

- Инфраструктура Kaspersky Endpoint Detection and Response Expert (cloud) доступна в вашем регионе. Для получения информации о доступности инфраструктуры EDR Expert (cloud) в вашем регионе обратитесь в Службу технической поддержки.
- Установлена единая платформа управления OSMP (Open Single Management Platform).
- Приложение Kaspersky Endpoint Security установлено в стандартном режиме.
- Приложение Kaspersky Endpoint Security активировано и функциональность входит в лицензию.
- Вы приняли условия Соглашения об обработке данных Kaspersky Endpoint Detection and Response Expert (cloud).
- Компонент Endpoint Detection and Response Expert (cloud) включен.
- Компоненты приложения, которые обеспечивают работу EDR Expert (cloud), включены и работают:
  - Защита от файловых угроз.
  - Защита от веб-угроз.

- Защита от почтовых угроз.
- Защита от эксплойтов.
- Анализ поведения.
- Предотвращение вторжений.
- Откат вредоносных действий.
- Адаптивный контроль аномалий.

Этапы интеграции с EDR Expert (cloud)

Интеграция с EDR Expert (cloud) состоит из следующих этапов:

1. **Установка компонента Endpoint Detection and Response Expert (cloud)**

   Вы можете выбрать компонент Endpoint Detection and Response Expert (cloud) во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

   > Для завершения обновления приложения с новым компонентом нужно перезагрузить компьютер.

2. **Активация Kaspersky Endpoint Detection and Response Expert (cloud)**

   Вам нужно приобрести отдельную лицензию на использование Kaspersky Endpoint Detection and Response Expert (cloud).

   Функциональность будет доступна после добавления отдельного ключа Kaspersky Endpoint Detection and Response Expert (cloud). В результате на компьютере будет добавлено два ключа: ключ для Kaspersky Endpoint Security и ключ для Kaspersky Endpoint Detection and Response Expert (cloud).

   Лицензирование отдельной функциональности Endpoint Detection and Response Expert (cloud) не отличается от лицензирования Kaspersky Endpoint Security.

   Убедитесь, что функциональность EDR Expert (cloud) включена в лицензию и работает в локальном интерфейсе приложения.

3. **Подключение к серверу сбора телеметрии и серверу реагирования**

   Для работы Kaspersky Endpoint Detection and Response Expert (cloud) необходимо установить доверенное соединение между Kaspersky Endpoint Security и двумя серверами:

   - *Сервер сбора телеметрии* – сервер, входящий в состав SIEM, который предназначен для сбора, нормализации, корреляции, анализа и хранения данных о событиях на компьютере.
   - *Сервер реагирования* – сервер, который предназначен для приема и проверки данных, исследования поведения объектов, а также публикации результатов исследования.

   Как подключить компьютер с Kaspersky Endpoint Security к EDR Expert (cloud) в Web Console

   1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
   2. Нажмите на название политики Kaspersky Endpoint Security.

      Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Встроенные агенты → Endpoint Detection and Response Expert (cloud)**.

5. Включите компонент с помощью переключателя **Endpoint Detection and Response Expert (cloud) ВЫКЛЮЧЕН**.

6. Если текущая политика является дочерней, и в родительской политике установлен запрет на изменение параметров интеграции с EDR Expert (cloud) ("замок" закрыт), вы можете настроить наследование параметров в блоке **Наследование**:

   - **Наследовать настройки подключения из политики** (значение по умолчанию). Параметры подключения будут унаследованы из родительской политики. Редактирование параметров будет недоступно.

   - **Использовать собственные настройки подключения**. Вы можете настроить параметры подключения самостоятельно.

7. На вкладке **Сервер реагирования** отображаются автоматически полученные полное доменное имя и порт сервера реагирования. Если политика безопасности в вашей инфраструктуре не позволяет подключаться к серверам EDR Expert (cloud) напрямую, вы можете настроить подключение через TCP-туннель:

   a. Установите флажок **Использовать TCP-туннель для реагирования**.

   b. Укажите адрес сервера (IPv4, IPv6), а также порт подключения к туннелю.

8. Если необходимо, настройте период отправки запросов на синхронизацию с сервером в поле **Отправлять запрос на синхронизацию на сервер каждые (мин.)**. Во время синхронизации Kaspersky Endpoint Security получает задачи по реагированию на угрозы и отправляет результаты выполнения задач.

9. Перейдите на вкладку **Сервер сбора телеметрии**.

10. Настройте параметры подключения к серверу сбора телеметрии:

    a. Нажмите на ссылку **Изменить**.

    b. В открывшемся окне выберите сервер сбора телеметрии из списка. Роль сервера сбора телеметрии в EDR Expert (cloud) выполняет коллектор KUMA. Подробнее см. в справке Kaspersky Unified Monitoring and Analysis Platform.

    Если при подключении к серверу сбора телеметрии возникла ошибка, выберите другой сервер. Если вам не удалось выполнить подключение к серверу сбора телеметрии, обратитесь в Службу технической поддержки.

    c. При необходимости вы можете вы можете настроить подключение к серверу сбора телеметрии через TCP-туннель, как для сервера реагирования.

11. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Вы можете проверить статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Endpoint Detection and Response Expert (cloud)**.

Настройка отправки телеметрии EDR Expert (cloud)

Телеметрия – список событий, которые произошли на защищаемом компьютере. Kaspersky Endpoint Security анализирует данные телеметрии и отправляет их на серверы сбора телеметрии во время синхронизации. События телеметрии поступают на сервер почти непрерывно. Kaspersky Endpoint Security выполняет синхронизацию с сервером при выполнении любого из следующих условий:

- Истек период синхронизации.
- Количество событий в буфере превысило максимальное значение.

Таким образом, по умолчанию приложение выполняет синхронизацию каждые 30 секунд или при накоплении в буфере 1024 события. Вы можете настроить параметры синхронизации в политике Kaspersky Endpoint Security и выбрать оптимальные значения исходя из нагрузки на сеть (см. инструкцию ниже).

Если соединение между Kaspersky Endpoint Security и сервером отсутствует, то приложение ставит новые события в очередь. При восстановлении соединения Kaspersky Endpoint Security отправляет события из очереди на сервер по порядку. При этом, чтобы не перегрузить сервер, Kaspersky Endpoint Security может отправлять не все события. Для этого вы можете оптимизировать параметры отправки событий и, например, задать максимальное количество событий в час (см. инструкцию ниже).

Чтобы настроить параметры отправки телеметрии, выполните следующие действия:

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response Expert (cloud)**.
5. В открывшемся окне перейдите на вкладку **Настройка передачи данных**.
6. Убедитесь, что установлен флажок **Отправка телеметрии ВКЛЮЧЕНА**.
7. Если требуется, включите функцию **Отправлять телеметрию только с IOA**. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию *потоковой проверки*, которая позволяет отслеживать такие события в режиме реального времени. По умолчанию функция выключена.
8. Если требуется, настройте параметры синхронизации с сервером:

   - **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд.
   - **Максимальное количество пакетов событий**. Приложение выполняет синхронизацию с сервером при заполнении буфера событиями. По умолчанию установлено значение 1024 события.
9. Перейдите на вкладку **Регулирование количества запросов**.

10. Если требуется, выключите регулирование количества запросов с помощью переключателя **Регулирование количества запросов ВКЛЮЧЕНО**.

    Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события. По умолчанию функция включена.

11. Настройте параметры оптимизации отправки событий на сервер:

    - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

    - **Процент превышения лимита событий (%)**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Endpoint Security восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.

12. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Исключения из телеметрии EDR Expert (cloud)

Для повышения производительности и оптимизации отправки данных на Сервер сбора телеметрии вы можете добавить исключения из телеметрии. Например, вы можете отменить обработку данных о сетевых коммуникациях для отдельных приложений.

> Использование слишком большого количества правил может привести к увеличению нагрузки на Сервер сбора телеметрии и снижению производительности компьютера. Рекомендуется добавлять только необходимые правила.

Чтобы создать исключение из телеметрии в Web Console и Cloud Console, выполните следующие действия:

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки → Настройки телеметрии**.

5. Выберите вкладку **Телеметрия EDR Expert (cloud)**.

6. В блоке **Общие исключения** нажмите на кнопку **Добавить**.

   Откроется окно **Добавление правила исключения**.

7. При необходимости измените статус правила. По умолчанию правило включено.

8. Введите имя правила.

9. Выберите действие, которое будет выполнено при срабатывании правила:

   - **Не собирать**. Отфильтрованное событие будет исключено из отправляемой телеметрии.
   - **Исключить IOA**. Из отправляемой телеметрии будет исключено событие о срабатывании IOA-правила.

10. Если выбран вариант **Исключить IOA**, укажите IOA-правила, которые необходимо добавить в исключения:

    - **Исключить все**. При выполнении заданного условия приложение будет исключать из телеметрии события, формируемые на основе всех IOA-правил.
    - **Исключить по GUID**. Укажите GUID IOA-правила. Вы можете указать несколько GUID через `,`. Подробную информацию об IOA-правилах см. в справке EDR Expert (cloud).

11. Задайте условие фильтрации:

    a. Выберите название поля, по которому будет выполняться фильтрация.

    b. Выберите оператор (см. таблицу ниже), и укажите значение, с которым будет сравниваться значение поля из события.

Перечень операторов условий

Оператор	Описание
<	Если значение поля меньше значения, заданного в условии, событие будет отфильтровано.
≤	Если значение поля меньше или равно значению, заданному в условии, событие будет отфильтровано.
=	Если значение поля равно значению, заданному в условии, событие будет отфильтровано.
≥	Если значение поля больше или равно значению, заданному в условии, событие будет отфильтровано.
>	Если значение поля больше значения, заданного в условии, событие будет отфильтровано.
≠	Если значение поля не равно значению, заданному в условии, событие будет отфильтровано.
похоже	Если значение поля подходит под маску, указанную в условии, событие будет отфильтровано. Приложение поддерживает символы `*` и `?` для ввода маски.
не похоже	Если значение поля не подходит под маску, указанную в условии, событие будет отфильтровано. Приложение поддерживает символы `*` и `?` для ввода маски.
одно из	Если значение поля совпадает с одним из значений из заданного в условии списка, событие считается отфильтрованным.
ни одного из	Если значение поля не совпадает ни с одним из значений из заданного в условии списка, событие считается отфильтрованным.
похоже на одно из	Если значение поля подходит под одну из масок, заданных в условии, событие будет отфильтровано. Приложение поддерживает символы * и ? для ввода маски.
не похоже ни на одно из	Если значение поля не подходит ни под одну из масок, заданных в условии, событие будет отфильтровано. Приложение поддерживает символы * и ? для ввода маски.
существует	Если указанное в условии поле содержится в событии, событие будет отфильтровано.
не существует	Если указанное в условии поле не содержится в событии, событие будет отфильтровано.
содержит	Если значение, заданное в условии, содержится в значении поля, событие будет отфильтровано.
равно	Если значение поля равно значению, заданному в условии, событие будет отфильтровано. Проверка выполняется без учета регистра.
И (побитовый)	Если результат операции "Побитовое И" (&) для значения поля и значения, указанного в условии, равен 1, событие будет отфильтровано.

12. При необходимости вы можете формировать сложные критерии фильтрации, добавляя несколько условий фильтрации и групп условий. Также в группу условий вы можете добавлять вложенные условия и группы условий. Вы можете использовать следующие операторы:

    - **И** – фильтр отбирает события, которые соответствуют всем указанным условиям.
    - **ИЛИ** – фильтр отбирает события, которые соответствуют одному из указанных условий.
    - **НЕ** (для использования данного оператора выберите вариант **Добавить НЕ перед**) – фильтр отбирает события, которые не соответствуют всем указанным условиям.

    Условия и группы условий первого уровня объединены с помощью оператора **И**.

13. Для проверки работы созданного правила фильтрации нажмите на кнопку **Проверить правило**.

    В открывшемся окне отобразится таблица событий, отфильтрованных с помощью созданного правила. Подробнее см. в справке EDR Expert (cloud).

14. Если требуется, в блоке **Все типы событий** добавьте исключения из телеметрии по типу событий:

    a. Нажмите на название типа события.

    b. В открывшемся окне нажмите на кнопку **Настроить вручную**.

    c. При необходимости настройте отправку телеметрии по выбранному типу событий с помощью переключателя **Отправлять событие**. По умолчанию включена отправка телеметрии по всем типам событий.

    d. В блоке **Правила исключения** нажмите на кнопку **Добавить**.

    Откроется окно **Добавление правила исключения**.

    e. Выполните действия, описанные в шагах 7-13, для каждого добавляемого правила.

15. Для некоторых типов событий вы также можете добавить правила включения для расширения собираемой телеметрии:

    a. В блоке **Правила включения** нажмите на кнопку **Добавить**.

    Откроется окно **Добавление правила включения**.

    b. Введите имя правила.

    c. В блоке **Условие** введите значения для отображаемых полей. Тип доступных полей зависит от выбранного события.

    > Правила исключения имеют приоритет над правилами включения.

16. Для применения политики на компьютерах убедитесь, что закрыты замки, и сохраните внесенные изменения.

Как экспортировать / импортировать фильтры событий EDR Expert (cloud)

Вы можете экспортировать список исключений в файл в формате JSON. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество идентификаторов событий. Также вы можете использовать функцию экспорта / импорта для резервного копирования фильтров событий или для миграции списка на другой сервер.

Использование слишком большого количества правил может привести к увеличению нагрузки на Сервер сбора телеметрии и снижению производительности компьютера. Рекомендуется добавлять только необходимые правила.

Чтобы экспортировать / импортировать фильтры событий в Web Console, выполните следующие действия:

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки телеметрии**.
5. Выберите вкладку **Телеметрия EDR Expert (cloud)**.
6. Для экспорта фильтров событий выполните следующие действия:
   a. Нажмите на кнопку **Экспортировать**.
   b. В открывшемся окне введите имя файла формата JSON, в который вы хотите экспортировать фильтры событий, а также выберите папку, в которой вы хотите сохранить этот файл.
   c. Сохраните файл.

      Kaspersky Endpoint Security экспортирует фильтры событий в JSON-файл.
7. Для импорта фильтров событий выполните следующие действия:
   a. Нажмите на кнопку **Импортировать**.
   b. В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать фильтры событий.
   c. Выберите способ импорта правил фильтрации событий: добавить к существующим правилам или заменить существующие правила на новые.
   d. Откройте файл.

8. Для применения политики на компьютерах убедитесь, что закрыты замки, и сохраните внесенные изменения.

    1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

    2. Нажмите на название политики Kaspersky Endpoint Security.

       Откроется окно свойств политики.

    3. Выберите вкладку **Параметры приложения**.

    4. Перейдите в раздел **Общие настройки** → **Настройки телеметрии**.

    5. Выберите вкладку **Телеметрия EDR Expert (cloud)**.

    6. Для экспорта фильтров событий выполните следующие действия:

        a. Нажмите на кнопку **Экспортировать**.

        b. В открывшемся окне введите имя файла формата JSON, в который вы хотите экспортировать фильтры событий, а также выберите папку, в которой вы хотите сохранить этот файл.

        c. Сохраните файл.

           Kaspersky Endpoint Security экспортирует фильтры событий в JSON-файл.

    7. Для импорта фильтров событий выполните следующие действия:

        a. Нажмите на кнопку **Импортировать**.

        b. В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать фильтры событий.

        c. Выберите способ импорта правил фильтрации событий: добавить к существующим правилам или заменить существующие правила на новые.

        d. Откройте файл.

    8. Для применения политики на компьютерах убедитесь, что закрыты замки, и сохраните внесенные изменения.

Endpoint Detection and Response Optimum / Expert



В Kaspersky Endpoint Security для Windows включен встроенный агент для работы решения Kaspersky Endpoint Detection and Response Optimum (далее также "EDR Optimum"). Начиная с версии Kaspersky Endpoint Security для Windows 11.8.0 в приложение добавлен встроенный агент для работы решения Kaspersky Endpoint Detection and Response Expert (далее также "EDR Expert"). *Решения Kaspersky Endpoint Detection and Response* – решения, предназначенные для защиты IT-инфраструктуры организации от сложных кибернетических угроз. Функционал решений сочетает автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для противодействия сложным атакам, в том числе новым эксплойтам (exploits), программам-вымогателям (ransomware), бесфайловым атакам (fileless attacks), а также методам, использующим законные системные инструменты. EDR Expert предлагает пользователю больше функций для мониторинга и реагирования на угрозы информационной безопасности, чем EDR Optimum. Подробнее о решениях см. в справке Kaspersky Endpoint Detection and Response Optimum и в справке Kaspersky Endpoint Detection and Response Expert.

Средства анализа угроз

Kaspersky Endpoint Detection and Response использует следующие средства анализа угроз (Threat Intelligence):

- Интеграция с Kaspersky Threat Intelligence Portal, который содержит и отображает информацию о репутации файлов и веб-адресов.
- База угроз "Лаборатории Касперского" Kaspersky Threats.
- Инфраструктура облачных служб Kaspersky Security Network (далее также "KSN"), предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.
- Технология Cloud Sandbox, которая позволяет запускать обнаруженные файлы в изолированной среде и определять их репутацию.

Принцип работы решения

Kaspersky Endpoint Detection and Response выполняет обзор и анализ развития угрозы и предоставляет *Сотруднику службы безопасности* или *Администратору* информацию о потенциальной атаке, необходимую для принятия своевременных действий по реагированию. Kaspersky Endpoint Detection and Response показывает детали алерта в отдельном окне. *Алерт* – это событие в ИТ-инфраструктуре организации, которое приложение отметило как необычное или подозрительное и которое может представлять угрозу безопасности ИТ-инфраструктуры организации. *Детали алерта* – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum и в справке Kaspersky Endpoint Detection and Response Expert.

Поддержка предыдущих версий Kaspersky Endpoint Security

Если вы используете Kaspersky Endpoint Security 11.2.0-11.6.0 для взаимодействия с Kaspersky Endpoint Detection and Response Optimum, в состав приложения включено приложение Kaspersky Endpoint Agent. Вы можете установить Kaspersky Endpoint Agent совместно с Kaspersky Endpoint Security. В Kaspersky Endpoint Security 11.9.0 дистрибутив приложения Kaspersky Endpoint Agent исключен из комплекта поставки Kaspersky Endpoint Security.

Решение Kaspersky Endpoint Detection and Response Expert не поддерживает работу с Kaspersky Endpoint Agent. Решение Kaspersky Endpoint Detection and Response Expert использует для работы Kaspersky Endpoint Security со встроенным агентом (версия 11.8.0 и выше).

Интеграция встроенного агента с EDR Optimum / EDR Expert

Для интеграции с Kaspersky Endpoint Detection and Response вам нужно добавить компонент Endpoint Detection and Response Optimum или компонент Endpoint Detection and Response Expert (cloud) и настроить параметры Kaspersky Endpoint Security.

Компоненты Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), Endpoint Detection and Response Expert (on-premises) несовместимы между собой.

Для работы Endpoint Detection and Response должны быть выполнены следующие условия:

- Kaspersky Security Center версии 13.2 или выше. В более ранних версиях Kaspersky Security Center невозможно активировать функциональность Endpoint Detection and Response.
- Плагин управления Kaspersky Endpoint Detection and Response.

  Начиная с Kaspersky Endpoint Security версии 12.6 отображение деталей алерта перенесено из плагина управления Kaspersky Endpoint Security в плагин управления EDR. Плагин управления EDR является единым плагином для работы с агентами на операционных системах Windows, Mac и Linux. Теперь для работы с EDR Optimum вам нужен плагин управления Kaspersky Endpoint Security для создания задач реагирования на угрозы и плагин управления EDR для просмотра деталей алерта.
- Компонент Endpoint Detection and Response Optimum в составе Kaspersky Endpoint Security поддерживает работу с решением Kaspersky Endpoint Detection and Response Optimum версии 2.0. Работа с решением Kaspersky Endpoint Detection and Response Optimum версии 1.0 не поддерживается.
- Управление EDR Optimum доступно в Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console.

  Управление EDR Expert доступно только в Kaspersky Security Center Cloud Console. Управлять функциональностью в Консоли администрирования (MMC) невозможно.
- Приложение активировано и функциональность входит в лицензию.
- Компонент Endpoint Detection and Response включен.
- Компоненты приложения, которые обеспечивают работу Endpoint Detection and Response, включены и работают. Работу Endpoint Detection and Response обеспечивают следующие компоненты:
  - Защита от файловых угроз.
  - Защита от веб-угроз.
  - Защита от почтовых угроз.
  - Защита от эксплойтов.
  - Анализ поведения.
  - Предотвращение вторжений.

- Откат вредоносных действий.
- Адаптивный контроль аномалий.

Интеграция с Kaspersky Endpoint Detection and Response состоит из следующих этапов:

1. **Установка компонентов Endpoint Detection and Response**

   Вы можете выбрать компонент Endpoint Detection and Response Optimum или компонент Endpoint Detection and Response Expert (cloud) во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

   > Для завершения обновления приложения с новыми компонентами нужно перезагрузить компьютер.

2. **Активация Kaspersky Endpoint Detection and Response**

   Вы можете приобрести лицензию на использование Kaspersky Endpoint Detection and Response следующими способами:

   - Функциональность Endpoint Detection and Response включена в состав лицензии на использование Kaspersky Endpoint Security для Windows.

     Функциональность будет доступна сразу после активации Kaspersky Endpoint Security для Windows.

   - Приобретение отдельной лицензии на использование EDR Optimum или EDR Expert (Kaspersky Endpoint Detection and Response Add-on).

     Функциональность будет доступна после добавления отдельного ключа Kaspersky Endpoint Detection and Response. В результате на компьютере будет добавлено два ключа: ключ для Kaspersky Endpoint Security и ключ для Kaspersky Endpoint Detection and Response.

     Лицензирование отдельной функциональности Endpoint Detection and Response не отличается от лицензирования Kaspersky Endpoint Security.

   Убедитесь, что функциональность EDR Optimum или EDR Expert включена в лицензию и работает в локальном интерфейсе приложения.

   Подробнее о Лицензионном соглашении EDR Optimum см. в справке Kaspersky Endpoint Detection and Response Optimum.

3. **Включение компонентов Endpoint Detection and Response**

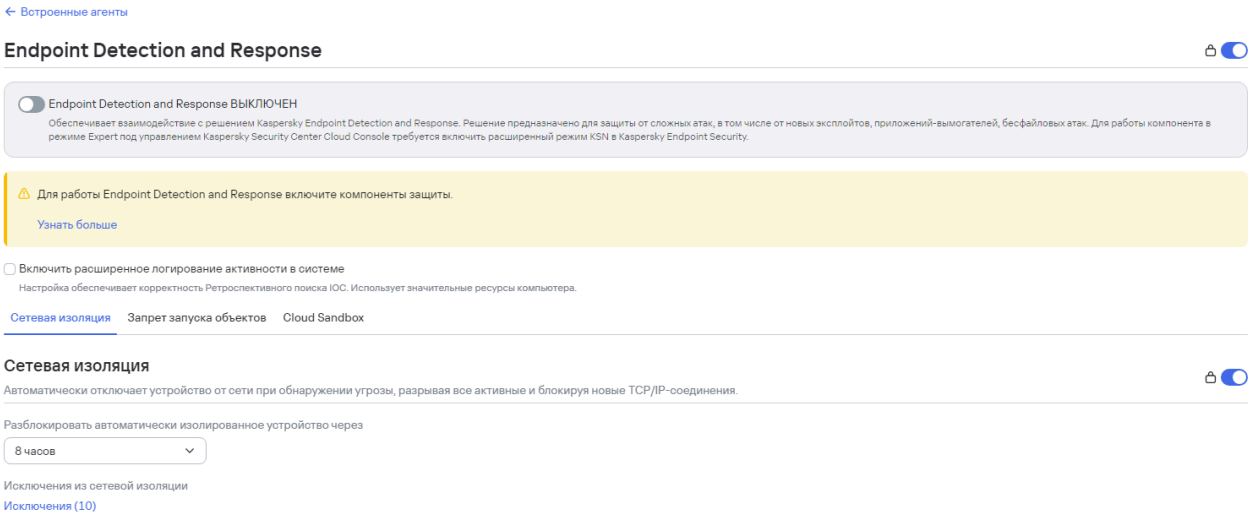
   Вы можете включить или выключить компонент в настройках политики Kaspersky Endpoint Security для Windows.

   Как включить или выключить компонент Endpoint Detection and Response в Web Console

   1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
   2. Нажмите на название политики Kaspersky Endpoint Security.

      Откроется окно свойств политики.
   3. Выберите вкладку **Параметры приложения**.
   4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
   5. Включите переключатель **Endpoint Detection and Response ВКЛЮЧЕН**.

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.



Параметры интеграции с EDR

В результате компонент Endpoint Detection and Response будет включен. Проверьте статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Endpoint Detection and Response Optimum** или **Endpoint Detection and Response Expert (cloud)**.

4 Включение передачи данных на Сервер администрирования

Для работы всех функций Endpoint Detection and Response должна быть включена передача следующих данных:

- Данные о файлах карантина.

  Данные нужны для получения информации о помещенных на компьютере файлах на карантин в Web Console. В Web Console вы можете, например, загрузить файл из карантина на компьютер для анализа.

- Данные о цепочке развития угрозы.

  Данные нужны для получения информации об обнаруженных на компьютере угрозах в Web Console. В Web Console вы можете просматривать детали алерта и выполнять действия по реагированию.

Как включить передачу данных на Сервер администрирования в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Интеграция с KSC**.
5. В блоке **Передача данных на Сервер администрирования** перейдите по ссылке **Дополнительные настройки**.

6. В открывшемся окне установите следующие флажки:

   - **О файлах карантина**.
   - **О цепочке развития угрозы**.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Поиск индикаторов компрометации (стандартная задача)

Индикатор компрометации (Indicator of Compromise, IOC) – набор данных об объекте или активности, который указывает на несанкционированный доступ к компьютеру (компрометация данных). Например, индикатором компрометации может быть большое количество неудачных попыток входа в систему. Задача *Поиск IOC* позволяет обнаруживать индикаторы компрометации на компьютере и выполнять действия по реагированию на угрозы.

Для поиска индикаторов компрометации Kaspersky Endpoint Security использует IOC-файлы. *IOC-файлы* – файлы, содержащие набор индикаторов, при совпадении с которыми приложение считает событие обнаружением. IOC-файлы должны соответствовать стандарту описания OpenIOC.

Режим запуска задачи Поиск IOC

Kaspersky Endpoint Detection and Response позволяет создавать стандартные задачи поиска IOC для обнаружения компрометации данных. *Стандартная задача поиска IOC* – групповая или локальная задача, которые создаются и настраиваются вручную в Web Console. Для запуска задач используются IOC-файлы, подготовленные пользователем. Если вы хотите добавить индикатор компрометации вручную, ознакомьтесь с требованиями к IOC-файлам.

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC.

ЗАГРУЗИТЬ ФАЙЛ IOC_TERMS.XLSX

Kaspersky Endpoint Security также поддерживает автономные задачи поиска IOC при работе приложения в составе решения Kaspersky Sandbox.

Создание IOC-файла

Начиная с версии Kaspersky Endpoint Security для Windows 12.10 добавлена возможность создавать IOC-файлы прямо в свойствах задачи. Для создания IOC-файла вам нужно подготовить TXT-файл со списком индикаторов компрометации. В качестве индикаторов компрометации вы можете добавить списки следующих объектов:

- Хеши файлов (MD5 / SHA256).

  Приложение подготовит IOC-файл с областью поиска FileItem/Md5sum или FileItem/Sha256sum.

- IP-адреса (IPv4, IPv6).

  Приложение подготовит IOC-файл с областью поиска PortItem/RemoteIP.

- DNS-имена.

  Приложение подготовит IOC-файл с областью поиска DnsEntryItem/RecordName.

Как создать IOC-файл в Web Console

1. В главном окне Web Console выберите **Управление активами → Задачи**.

   Откроется список задач.

2. Выберите задачу **Поиск IOC**.

   Откроется окно свойств задачи. Если требуется, создайте задачу **Поиск IOC**.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Поиск угроз**.

5. Нажмите на кнопку **Переопределить IOC-файлы**.

6. Откроется форма для создания IOC-файла:

   a. В блоке **Источник IOC-файлов** выберите **Создать из файла**.

   b. Введите имя для IOC-файла.

   c. Выберите TXT-файл со списком индикаторов компрометации.

   d. Выберите тип IOC-файла: **DNS-имена**, **Хеши файлов**, **IP-адреса**.

   e. Нажмите на кнопку **Загрузить**.

   Kaspersky Endpoint Security добавит IOC-файлы в IOC-коллекцию. Если требуется, вы можете временно выключить IOC-файлы из области действия задачи.

7. Сохраните внесенные изменения.

Создание задачи Поиск IOC

Вы можете создавать задачи *Поиск IOC* вручную следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали алерта – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum и в справке Kaspersky Endpoint Detection and Response Expert.

- С помощью мастера создания задач.

Выполнение групповой задачи *Поиск IOC* недоступно, если на проверяемых компьютерах настроена интеграция с решениями Kaspersky Endpoint Detection and Response Expert (on-premises) или Kaspersky Endpoint Detection and Response Expert (cloud). В таком случае для поиска индикаторов компрометации рекомендуется использовать действие по реагированию *IOC-проверка*. Подробнее см. в справке Kaspersky Endpoint Detection and Response Expert (on-premises).

Вы можете настроить параметры задачи для EDR Optimum в Web Console и Cloud Console. Параметры задачи для EDR Expert доступны только в Cloud Console.

Чтобы создать задачу Поиск IOC, выполните следующие действия:

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Поиск IOC**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Перейдите к следующему шагу.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

У системной учетной записи (SYSTEM) отсутствуют права на выполнение задачи *Поиск IOC* на сетевых дисках. Если вы хотите выполнить задачу на сетевом диске, выберите учетную запись пользователя, у которого есть доступ к этому диску.

Для работы автономных задач поиска IOC на сетевых дисках вам нужно вручную выбрать учетную запись пользователя, у которого есть доступ к этом диску, в свойствах задачи.

6. Завершите работу мастера.

   В списке задач отобразится новая задача.

7. Нажмите на новую задачу.

   Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. Перейдите в раздел **Поиск угроз**.

10. Загрузите IOC-файлы для поиска индикаторов компрометации.

    После загрузки IOC-файлов приложение покажет сводную информацию о файле, включая список индикаторов, которые не прошли проверку. После загрузки IOC-файлов вы можете вручную изменять содержание файлов во встроенном редакторе прямо в свойствах задачи. Kaspersky Endpoint Security поддерживает изменение содержания IOC-файлов, которые соответствуют стандарту OpenIOC версии 1.1. Изменить содержание IOC-файлов, соответствующих стандарту OpenIOC версии 1.0, невозможно.

    Kaspersky Endpoint Security добавит IOC-файлы в IOC-коллекцию. Если требуется, вы можете временно выключить IOC-файлы из области действия задачи.

    Не рекомендуется добавлять или удалять IOC-файлы после запуска задачи. Это может привести к некорректному отображению результатов поиска IOC для предыдущих запусков задачи. Для поиска индикаторов компрометации по новым IOC-файлам рекомендуется добавлять новые задачи.

11. Если требуется, установите флажок **Ретроспективный поиск IOC**. *Ретроспективный поиск IOC* – это режим работы задачи *Поиск IOC*, при котором Kaspersky Endpoint Security выполняет поиск индикаторов компрометации по данным, полученным за определенный интервал времени. Режим предназначен для поиска индикаторов компрометации по телеметрии защищаемого компьютера, такой как сетевая активность, процессы, файлы и другие. Kaspersky Endpoint Security анализирует данные в журналах операционной системы и браузеров на компьютере. Ретроспективный поиск IOC анализирует журналы следующих браузеров: Google Chrome, Mozilla Firefox, Microsoft Edge (версии 79 и выше).

12. Настройте действия при обнаружении индикатора компрометации:

    - **Изолировать устройство от сети**. Если выбран этот вариант действия, то Kaspersky Endpoint Security изолирует компьютер от сети для предотвращения распространения угрозы. Вы можете настроить время изоляции в параметрах компонента Endpoint Detection and Response.

      Если флажок снят, вы можете изолировать компьютер от сети после выполнения задачи вручную. Если в результате выполнения задачи *Поиск IOC* обнаружен IOC, то вы можете изолировать компьютер от сети прямо из результатов поиска IOC (свойства задачи *Поиск IOC* → **Параметры приложения** → **Результаты поиска IOC**). Также Kaspersky Endpoint Security позволяет сразу настроить дополнительные параметры: период выключения Сетевой изоляции и исключения из Сетевой изоляции.

- **Копию поместить на карантин, объект удалить**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удаляет вредоносный объект, обнаруженный на компьютере. Перед удалением объекта Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин.

  Если флажок снят, вы можете поместить файл на карантин после выполнения задачи вручную. Если в результате выполнения задачи *Поиск IOC* обнаружен файл, который может вызывать компрометацию данных, то вы можете поместить этот файл на карантин прямо из результатов поиска IOC (**Параметры приложения → Результаты поиска IOC**). В результате Kaspersky Endpoint Security запустит мастер создания задач с предустановленными данными об обнаруженном файле. Вам нужно только настроить дополнительные параметры задачи, например, задать расписание запуска задачи.

  Если требуется, установите флажок **Применить к критическим объектам системы**. К критически важным системным объектам (англ. System Critical Object, SCO) относятся файлы, необходимые для работы операционной системы.

  Не рекомендуется применять действия к файлам, относящиеся к SCO. Это может привести к нестабильной работе или отказу загрузки операционной системы.

- **Запустить проверку важных областей**. Если выбран этот вариант действия, то Kaspersky Endpoint Security запускает задачу *Проверка важных областей*. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

13. Перейдите в раздел **Дополнительно**.

14. Выберите типы данных (IOC-документы), которые необходимо анализировать во время выполнения задачи.

    Kaspersky Endpoint Security автоматически выбирает типы данных (IOC-документы) для задачи *Поиск IOC* в соответствии с содержанием загруженных IOC-файлов. Не рекомендуется самостоятельно отменять выбор типов данных.

    Дополнительно вы можете настроить области поиска для следующих типов данных:

    - **Файлы - FileItem**. Задайте область поиска IOC на компьютере с помощью предустановленных областей.

      По умолчанию Kaspersky Endpoint Security выполняет поиск IOC только в важных областях компьютера, таких как папки Загрузки, Рабочий стол, папка с временными файлами операционной системы и другие. Также вы можете добавить области поиска вручную.

    - **Журналы событий Windows - EventLogItem**. Задайте период времени, в течение которого зафиксированы события. Также вы можете выбрать журналы событий Windows для поиска IOC. По умолчанию выбраны следующие журналы событий: журнал событий приложений, журнал системных событий и журнал событий безопасности.

      При указании значения IOC-термина EventLogItem\source вам необходимо использовать значение параметра **Provider Name** из XML-схемы события.

    - **Реестр Windows - RegistryItem**. Задайте область поиска IOC в реестре.

      По умолчанию Kaspersky Endpoint Security анализирует определенный набор разделов реестра.

15. В окне свойств задачи выберите вкладку **Расписание**.

16. Настройте расписание запуска задачи.

> Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

17. Сохраните внесенные изменения.

18. Установите флажок напротив задачи.

19. Нажмите на кнопку **Запустить**.

В результате Kaspersky Endpoint Security запустит поиск индикаторов компрометации на компьютере. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты**. Информацию об обнаруженных индикаторах компрометации вы можете посмотреть в свойствах задачи **Параметры приложения → Результаты поиска IOC**. Также в результатах поиска IOC вы можете вручную поместить обнаруженный файл на карантин или изолировать компьютер от сети.

Kaspersky Endpoint Security выполняет поиск дубликатов среди записей, полученных по одному IOC-файлу, и сохраняет в результатах задачи только уникальные записи. Дубликатами считаются записи одного типа, у которых совпадают значения всех сравниваемых полей. Также приложение может не создавать записи при отсутствии у них значений одного или нескольких полей (см. таблицу ниже).

Тип	Сравниваемые поля	Условие, при котором запись не создается
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• У записи отсутствуют значения полей FullPath, Md5sum, Sha256sum. • У записей отсутствует значение поля FullPath и совпадают значения полей Md5sum, Sha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	У записи отсутствует значение какого-либо из следующих полей: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	У записи отсутствуют значения полей startTime или PID.

> В окне **Детали алерта** могут присутствовать записи RegistryItem с одинаковыми значениями полей. Данные записи не являются дубликатами, так как различаются значением поля Text, не отображающегося в интерфейсе.

> Срок хранения результатов поиска IOC составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет старые записи.

Расширенный сбор телеметрии для поиска IOC

Для ретроспективного поиска IOC рекомендуется включить расширенный сбор телеметрии на компьютере. Расширенный сбор телеметрии позволяет более точно определять индикаторы компрометации, но требует больше ресурсов компьютера.

Расширенный сбор телеметрии дополнительно включает в себя поддержку следующих терминов:

- FileItem/Md5sum;
- FileItem/Sha256sum;
- FileItem/SizeInBytes;
- FileItem/Created;
- FileItem/Modified;
- FileItem/Changed;
- FileItem/Accessed;
- FileItem/FileAttributes.

Если расширенный сбор телеметрии выключен, то Kaspersky Endpoint Security может выполнять ротацию данных об обнаруженных индикаторах компрометации.

Чтобы включить расширенный сбор телеметрии, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. Установите флажок **Включить расширенное логирование активности в системе**.
6. Сохраните внесенные изменения.

Помещение файла на карантин

При реагировании на угрозы Kaspersky Endpoint Detection and Response может создавать задачи *Помещение файла на карантин*. Это нужно, чтобы минимизировать последствия угрозы. *Карантин* – это специальное локальное хранилище на компьютере. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства. Kaspersky Endpoint Security использует карантин только при работе с решениями Detection and Response от "Лаборатории Касперского". В остальных случаях Kaspersky Endpoint Security помещает файл в резервное хранилище. Подробнее о работе с карантином в составе решений см. в справке Kaspersky Sandbox, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Endpoint Detection and Response Expert, Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Detection and Response Expert (on-premises).

Вы можете создавать задачи *Помещение файла на карантин* следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали алерта – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum и в справке Kaspersky Endpoint Detection and Response Expert.

- С помощью мастера создания задач.

  Вам нужно ввести путь к файлу или хеш файла (SHA256 или MD5), или путь к файлу и хеш файла.

- В свойствах задачи *Поиск IOC*.

  Если в результате выполнения задачи *Поиск IOC* обнаружен файл, который может вызывать компрометацию данных, то вы можете поместить этот файл на карантин прямо из результатов поиска IOC (**Параметры приложения** → **Результаты поиска IOC**). В результате Kaspersky Endpoint Security запустит мастер создания задач с предустановленными данными об обнаруженном файле. Вам нужно только настроить дополнительные параметры задачи, например, задать расписание запуска задачи.

Задача *Помещение файла на карантин* имеет следующие ограничения:

1. Размер файла не должен превышать 100 МБ.
2. Файлы, необходимые для работы Kaspersky Endpoint Security для Windows, удалить невозможно:
   - файлы, в которые входят в область действия технологии самозащиты Kaspersky Endpoint Security для Windows;
   - файлы, имеющие цифровую подпись "Лаборатории Касперского".
3. Вы можете настроить параметры задачи для EDR Optimum в Web Console и Cloud Console. Параметры задачи для EDR Expert доступны только в Cloud Console.
4. Невозможно выполнить проверку объекта, помещенного на карантине в результате выполнения задачи *Помещение файла на карантин*.

Чтобы создать задачу Помещение файла на карантин, выполните следующие действия:

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Помещение файла на карантин**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.

7. Нажмите на новую задачу.

   Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. Если требуется, установите флажок **Применить к критическим объектам системы**.

   К критически важным системным объектам (англ. System Critical Object, SCO) относятся файлы, необходимые для работы операционной системы.

   Не рекомендуется применять действия к файлам, относящиеся к SCO. Это может привести к нестабильной работе или отказу загрузки операционной системы.

10. В списке файлов нажмите на кнопку **Добавить**.

    Запустится мастер добавления файла.

11. Для добавления файла вам нужно ввести полный путь к файлу или хеш файла и путь к файлу.

    Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.

12. В окне свойств задачи выберите вкладку **Расписание**.

13. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

14. Сохраните внесенные изменения.

15. Установите флажок напротив задачи.

16. Нажмите на кнопку **Запустить**.

В результате Kaspersky Endpoint Security переместит файл в карантин.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом Выполнено, но сам файл будет помещен на карантин только после перезагрузки компьютера. После перезагрузки компьютера убедитесь, что файл удален.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет помещен на карантин только после перезагрузки компьютера. После перезагрузки компьютера убедитесь, что файл удален.

Задача *Помещение файла на карантин* может быть завершена с ошибкой *Доступ запрещен*, если вы пытаетесь поместить на карантин запущенный исполняемый файл. Создайте задачу завершения процесса для этого файла, а затем повторите попытку.

Задача *Помещение файла на карантин* может быть завершена с ошибкой *Недостаточно места в хранилище карантина*, если вы пытаетесь поместить на карантин большой файл. Очистите карантин или увеличьте размер карантина. Затем повторите попытку.

Вы можете восстановить файл из карантина или очистить карантин в Web Console. Восстановление объектов доступно на компьютере локально из командной строки.

Получение файла

Вы можете получать файлы с компьютеров пользователей. Например, вы можете настроить получение файла журнала событий, который создает стороннее приложение. В результате выполнения задачи копия файла будет сохранена в карантине. *Карантин* – это специальное локальное хранилище на компьютере. Вы можете загрузить этот файл на компьютер из карантина в Web Console (**Операции** → **Хранилища** → **Карантин**). При этом на компьютере пользователя файл остается в исходной папке.

Размер файла не должен превышать 2 ГБ.

Вы можете настроить параметры задачи для EDR Optimum в Web Console и Cloud Console. Параметры задачи для EDR Expert доступны только в Cloud Console.

Чтобы создать задачу Получение файла, выполните следующие действия:

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Получение файла**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.

7. Нажмите на новую задачу.

   Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. В списке файлов нажмите на кнопку **Добавить**.

   Запустится мастер добавления файла.

10. Для добавления файла вам нужно ввести полный путь к файлу или хеш файла и путь к файлу.

    Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.

11. В окне свойств задачи выберите вкладку **Расписание**.

12. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

13. Сохраните внесенные изменения.

14. Установите флажок напротив задачи.

15. Нажмите на кнопку **Запустить**.

    В результате Kaspersky Endpoint Security создаст копию файла и поместит копию в карантин. Вы можете загрузить файл из карантина в Web Console.

Удаление файла

Вы можете удаленно удалять файлы с помощью задачи *Удаление файла*. Например, вы можете удаленно удалить файл при реагировании на угрозы. Kaspersky Endpoint Security удаляет файл средствами операционной системы без помещения файла в корзину. В отличие от задачи *Удаление данных*, в задаче *Удаление файла* нет режима удаления файла без возможности восстановления.

Файлы, необходимые для работы Kaspersky Endpoint Security для Windows, удалить невозможно:

- файлы, в которые входят в область действия технологии самозащиты Kaspersky Endpoint Security для Windows;
- файлы, имеющие цифровую подпись "Лаборатории Касперского".

Вы можете настроить параметры задачи для EDR Optimum в Web Console и Cloud Console. Параметры задачи для EDR Expert доступны только в Cloud Console.

Чтобы создать задачу Удаление файла, выполните следующие действия:

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Удаление файла**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.

7. Нажмите на новую задачу.

   Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. Для добавления файла вам нужно ввести полный путь к файлу или хеш файла и путь к файлу.

   Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.

10. Если требуется, установите флажок **Применить к критическим объектам системы**.

    К критически важным системным объектам (англ. System Critical Object, SCO) относятся файлы, необходимые для работы операционной системы.

    Не рекомендуется применять действия к файлам, относящиеся к SCO. Это может привести к нестабильной работе или отказу загрузки операционной системы.

11. В окне свойств задачи выберите вкладку **Расписание**.

12. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

13. Сохраните внесенные изменения.

14. Установите флажок напротив задачи.

15. Нажмите на кнопку **Запустить**.

    В результате Kaspersky Endpoint Security удалит файл с компьютера. Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки компьютера. После перезагрузки компьютера убедитесь, что файл удален.

Задача *Удаление файла* может быть завершена с ошибкой *Доступ запрещен или файл не найден*, если вы пытаетесь удалить запущенный исполняемый файл. Создайте задачу завершения процесса для этого файла, а затем повторите попытку.

Запуск процесса

Вы можете удаленно запускать файлы с помощью задачи *Запуск процесса*. Например, вы можете удаленно запускать утилиту, которая создает файл с конфигурацией компьютера. Далее с помощью задачи *Получение файла*, вы можете получить созданный файл в Kaspersky Security Center Web Console.

Вы можете настроить параметры задачи для EDR Optimum в Web Console и Cloud Console. Параметры задачи для EDR Expert доступны только в Cloud Console.

Чтобы создать задачу Запуск процесса, выполните следующие действия:

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Запуск процесса**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.

7. Нажмите на новую задачу.

8. Откроется окно свойств задачи.

9. Выберите вкладку **Параметры приложения**.

10. Введите команду запуска процесса.

    Например, вы хотите запустить утилиту (`utility.exe`), которая сохраняет информацию о конфигурации компьютера в файл `conf.txt` в текущую папку (по умолчанию). Утилита расположена в папке `C:\Users\admin\Diagnostic\`. Конфигурационный файл необходимо сохранить в папке `C:\Users\admin\Documents\Configuration`. Введите следующие значения:

    - **Исполняемая команда** – `C:\Users\admin\Diagnostic\utility.exe`
    - **Аргументы командной строки (необязательно)** – `/R conf.txt`
    - **Путь к рабочей папке (необязательно)** – `C:\Users\admin\Documents\Configuration`

11. В окне свойств задачи выберите вкладку **Расписание**.

12. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

13. Сохраните внесенные изменения.

14. Установите флажок напротив задачи.

15. Нажмите на кнопку **Запустить**.

В результате Kaspersky Endpoint Security выполнит команду в тихом режиме и запустит процесс. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты выполнения**.

Завершение процесса

Вы можете удаленно завершать процессы с помощью задачи *Завершение процесса*. Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена с помощью задачи *Запуск процесса*.

Если вы хотите запретить запуск файла, вы можете настроить компонент Запрет запуска объектов. Вы можете запретить запуск исполняемых файлов, скриптов, файлов офисного формата.

Задача *Завершение процесса* имеет следующие ограничения:

Завершить процессы файлов, необходимых для работы Kaspersky Endpoint Security для Windows, невозможно:

- файлы, в которые входят в область действия технологии самозащиты Kaspersky Endpoint Security для Windows;
- файлы, имеющие цифровую подпись "Лаборатории Касперского".

Вы можете настроить параметры задачи для EDR Optimum в Web Console и Cloud Console. Параметры задачи для EDR Expert доступны только в Cloud Console.

Чтобы создать задачу Завершение процесса, выполните следующие действия:

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Windows 14.2**.

   b. В раскрывающемся списке **Тип задачи** выберите **Завершение процесса**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.

7. Нажмите на новую задачу.

   Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. Если требуется, установите флажок **Применить к критическим объектам системы**.

   К критически важным системным объектам (англ. System Critical Object, SCO) относятся файлы, необходимые для работы операционной системы.

   Не рекомендуется применять действия к файлам, относящиеся к SCO. Это может привести к нестабильной работе или отказу загрузки операционной системы.

10. Для завершения процесса вам нужно выбрать файл, работу которого вы хотите завершить. Вы можете выбрать файл следующими способами:

    - Введите полный путь к файлу.
    - Введите хеш файла и путь к файлу.
    - Введите идентификатор процесса PID (только для локальных задач).
    - Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.

    Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.

11. В окне свойств задачи выберите вкладку **Расписание**.

12. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

13. Нажмите на кнопку **Сохранить**.

14. Установите флажок напротив задачи.

15. Нажмите на кнопку **Запустить**.

    В результате Kaspersky Endpoint Security завершит процесс на компьютере. Например, если на компьютере запущено приложение GAME и вы завершили процесс game.exe, приложение будет закрыто без сохранения данных. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты**.

Запрет запуска объектов

Запрет запуска объектов позволяет контролировать запуск исполняемых файлов и скриптов, а также открытие файлов офисного формата. Таким образом, вы можете, например, запретить запуск приложений, использование которых считаете небезопасным. В результате распространение угрозы может быть остановлено. Запрет запуска объектов поддерживает определенный набор расширений файлов офисного формата и определенный набор интерпретаторов скриптов.

Запрет запуска объектов управляет доступом пользователей к файлам с помощью правил запрета запуска. *Правило запрета запуска* – это набор критериев, которые приложение учитывает при реагировании на запуск объекта, например, при блокировании запуска объекта. Приложение идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.

Вы можете создавать правила запрета запуска следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали алерта – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum и в справке Kaspersky Endpoint Detection and Response Expert.

- С помощью групповой политики или локальных параметров приложения.

  Вам нужно ввести путь к файлу или хеш файла (SHA256 или MD5), или путь к папке и хеш файла.

Вы также можете управлять Запретом запуска объектов локально из командной строки.

Запрет запуска объектов имеет следующие ограничения:

1. Правила запрета не распространяются на файлы, расположенные на компакт-дисках или в ISO-образах. Приложение не будет блокировать исполнение или открытие этих файлов.

2. Применить правило запрета к файлам, необходимым для работы Kaspersky Endpoint Security для Windows, невозможно:

   - файлы, в которые входят в область действия технологии самозащиты Kaspersky Endpoint Security для Windows;

   - файлы, имеющие цифровую подпись "Лаборатории Касперского".

3. Не рекомендуется создавать более 5000 правил запрета запуска, поскольку это может привести к нестабильности системы.

Управление Запретом запуска объектов

Компонент Запрет запуска объектов может работать в двух режимах:

- **Только статистика**.

  В этом режиме Kaspersky Endpoint Security публикует в журнал событий Windows и Kaspersky Security Center событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.

- **Активный**.

  В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета. Также приложение публикует в журнал событий Windows и Kaspersky Security Center событие о попытках запуска объектов или открытия документов.

Чтобы запретить запуск объектов, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты → Endpoint Detection and Response**.
5. Выберите вкладку **Запрет запуска**.
6. Включите переключатель **Запрет запуска ВКЛЮЧЕН**.
7. В блоке **Действие при запуске или открытии объекта** выберите режим работы компонента:

   - **Заблокировать и записать в журнал событий**. В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета. Также приложение публикует в журнал событий Windows и Kaspersky Security Center событие о попытках запуска объектов или открытия документов.

     Если требуется, установите флажок **Применить к критическим объектам системы**. К критически важным системным объектам (англ. System Critical Object, SCO) относятся файлы, необходимые для работы операционной системы.

     > Не рекомендуется применять действия к файлам, относящиеся к SCO. Это может привести к нестабильной работе или отказу загрузки операционной системы.

   - **Записать в журнал событий**. В этом режиме Kaspersky Endpoint Security публикует в журнал событий Windows и Kaspersky Security Center событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.

8. В блоке **Правила запрета запуска** сформируйте список правил запрета запуска:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне введите имя правила запрета запуска (например, *Приложение A*).

   c. В раскрывающемся списке **Тип** выберите объект, который вы хотите заблокировать: **Исполняемый файл**, **Скрипт**, **Файл Microsoft Office**.

   Если вы выберите неверный тип объекта, Kaspersky Endpoint Security не заблокирует файл или скрипт.

   d. Для добавления файла вам нужно ввести хеш файла (SHA256 или MD5) или полный путь к файлу, или хеш файла и путь к папке.

   > Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, Kaspersky Endpoint Security не заблокирует файл или скрипт.

   Запрет запуска объектов поддерживает определенный набор расширений файлов офисного формата и определенный набор интерпретаторов скриптов.

9. Также вы можете импортировать правила запрета запуска из файла.

   Как импортировать правила запрета запуска объектов из файла

   Если вам нужно добавить большое количество правил запрета, вы можете импортировать правила из CSV-файла. Для этого подготовьте CSV-файл по специальному шаблону и экспортируйте этот файл в Kaspersky Endpoint Security. Пример файла и описание полей файла приведено в таблице ниже.

   Kaspersky Endpoint Security не поддерживает экспорт правил. Вам нужно создавать CSV-файл вручную.

   Файл должен удовлетворять следующим требованиям:

   - Файл не должен содержать более 5000 правил.
   - Не изменяйте кодировку файла (UTF-8).
   - Файл должен иметь следующую структуру:
     - первая строка – названия полей, разделенные `;`.

       > Не удаляйте строку с названиями полей.

     - вторая и последующие строки – значения полей импортируемых правил, разделенные `;`.

   Чтобы создать файл со списком правил запрета запуска, выполните следующие действия:

   1. В главном окне Web Console выберите **Управление активами** → **Политики**.
   2. Нажмите на название политики Kaspersky Endpoint Security.

      Откроется окно свойств политики.

   3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Встроенные агенты → Endpoint Detection and Response**.

5. Выберите вкладку **Запрет запуска**.

6. В блоке **Правила запрета запуска** нажмите на кнопку .

   Запустится мастер импорта правил запрета запуска.

7. Нажмите на кнопку **Скачать шаблон**.

   Kaspersky Endpoint Security сохранит файл `template.csv` в память компьютера.

8. Откройте файл и добавьте правила в соответствии с шаблоном.

9. Сохраните файл с правилами запрета запуска.

Пример

```
Rule name (optional);OS (mandatory, specify 'windows', 'linux' or 'macos');File hash (MD5 or SHA256);Path to object (optional if file hash is specified);File Type (optional, specify 'any', 'executable', 'script', 'office document')
Test rule 1;windows;7c4a8d09a1e3f8b2c5d6e7f8a9b0c1d2;C:\Test\write.exe;executable
;windows;;C:\Test\test.exe;
;windows;7c4a8d09a1e3f8b2c5d6e7f8a9b0c1d2;;
;windows;2d7e9f8a1b3c5e0d7f4a6b2c8e1f3a5b7c9d1e0f2a4b6c8d0e2f4a6b8c0d2e4f;;script
;windows;8f3c2e1d0a9b8c7d6e5f4a3b2c1d0e9f8a7b6c5d4e3f2a1b0c9d8e7f6a5b4c3d;C:\Test\test2.docx;office document
Test rule 2;windows;3d5e2f8a1c9b47e0a6d2b8c5e3f1a490;;any
Test rule 3;windows;64ec88ca00b268e5ba1a35678a1b2c3d4e5f67890abcdef1234567890abcdef1;;office document
```

Подробное описание полей шаблона файла для импорта

Название поля	Описание
`Rule name (optional)`	Имя правила. Максимальная длина – 260 символов. Если поле не заполнено, в качестве имени правила будет использовано значение поля `File hash` или `Path to object`. Необязательное поле.
`OS (mandatory, specify 'windows', 'linux' or 'macos')`	Операционная система, для которой предназначено правило. Допустимые значения: • `windows` • `linux` • `macos` В политику Kaspersky Endpoint Security для Windows могут быть импортированы только те правила, для которых указано значение `windows`. Обязательное поле.
`File hash (MD5 or SHA256)`	Хеш файла. Допустимые значения: • MD5-хеш. 32 символа (в шестнадцатеричном формате) без разделителей и пробелов, регистр не важен. • SHA256-хеш. 64 символа (в шестнадцатеричном формате) без разделителей и пробелов, регистр не важен. Обязательное поле, если не заполнено поле `Path to object`.
`Path to object (optional if file hash is specified)`	Полный путь к файлу, включая его имя и расширение. Максимальная длина пути – 32 767 символов. Путь не должен содержать знаки переноса строки, табуляцию и следующие специальные символы: `*`, `?`, `"`, `<`, `>`, `|`. Обязательное поле, если не заполнено поле `File hash`.

Название поля	Описание
`File Type (optional, specify 'any', 'executable', 'script', 'office document')`	Тип файла, который будет заблокирован: • `any` – приложение не будет учитывать тип файла (значение по умолчанию). • `executable` – исполняемый файл. • `script` – скрипт. • `office document` – файл офисного формата. Запрет запуска объектов поддерживает определенный набор расширений файлов офисного формата и определенный набор интерпретаторов скриптов. Если вы укажете неверный тип файла, приложение не заблокирует запуск данного файла или скрипта. Необязательное поле.

Чтобы импортировать правила запрета запуска, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. Выберите вкладку **Запрет запуска**.
6. В блоке **Правила запрета запуска** нажмите на кнопку .

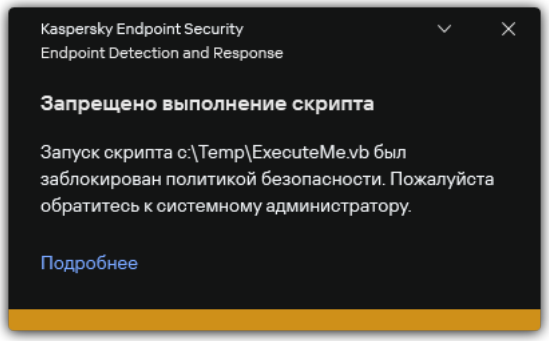
   Запустится мастер импорта правил запрета запуска.
7. Пропустите первый шаг мастер и нажмите на кнопку **Далее**.
8. На следующем шаге загрузите подготовленный файл с правилами.

   Загруженные правила отобразятся в виде таблицы. Если в файле содержалось несколько одинаковых правил, приложение оставит только одно из них. Также в таблицу не будут добавлены правила, уже содержащиеся в списке правил компонента.

   Вы можете отредактировать правила перед импортом, а также удалить правила, которые не требуется импортировать. Также при необходимости вы можете исправить ошибки в заполнении полей правил.
9. Нажмите на кнопку **Готово**.

   Kaspersky Endpoint Security добавит правила из файла к существующим. Правила с ошибками не будут импортированы.
10. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет блокировать запуск объектов: запуск исполняемых файлов, скриптов и открытие файлов офисного формата. При этом вы можете, например, открыть файл скрипта в текстовом редакторе, даже если запуск скрипта запрещен. При блокировании запуска объекта Kaspersky Endpoint Security покажет пользователю стандартное уведомление приложения (см. рис. ниже), если уведомления включены в настройках приложения.



Уведомление Запрета запуска объектов

Создание CSV-файла с правилами запрета

Если вам нужно добавить большое количество правил запрета, вы можете импортировать правила из CSV-файла. Для этого подготовьте CSV-файл по специальному шаблону и экспортируйте этот файл в Kaspersky Endpoint Security. Пример файла и описание полей файла приведено в таблице ниже.

Kaspersky Endpoint Security не поддерживает экспорт правил. Вам нужно создавать CSV-файл вручную.

Файл должен удовлетворять следующим требованиям:

- Файл не должен содержать более 5000 правил.
- Не изменяйте кодировку файла (UTF-8).
- Файл должен иметь следующую структуру:
  - первая строка – названия полей, разделенные `;`.

    > Не удаляйте строку с названиями полей.

  - вторая и последующие строки – значения полей импортируемых правил, разделенные `;`.

Чтобы создать файл со списком правил запрета запуска, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. Выберите вкладку **Запрет запуска**.
6. В блоке **Правила запрета запуска** нажмите на кнопку .
   Запустится мастер импорта правил запрета запуска.

7. Нажмите на кнопку **Скачать шаблон**.

   Kaspersky Endpoint Security сохранит файл `template.csv` в память компьютера.

8. Откройте файл и добавьте правила в соответствии с шаблоном.

9. Сохраните файл с правилами запрета запуска.

Пример

```
Rule name (optional);OS (mandatory, specify 'windows', 'linux' or 'macos');File hash (MD5 or SHA256);Path to
object (optional if file hash is specified);File Type (optional, specify 'any', 'executable', 'script', 'office
document')
Test rule 1;windows;7c4a8d09a1e3f8b2c5d6e7f8a9b0c1d2;C:\Test\write.exe;executable
;windows;;C:\Test\test.exe;
;windows;7c4a8d09a1e3f8b2c5d6e7f8a9b0c1d2;;
;windows;2d7e9f8a1b3c5e0d7f4a6b2c8e1f3a5b7c9d1e0f2a4b6c8d0e2f4a6b8c0d2e4f;;script
;windows;8f3c2e1d0a9b8c7d6e5f4a3b2c1d0e9f8a7b6c5d4e3f2a1b0c9d8e7f6a5b4c3d;C:\Test\test2.docx;office document
Test rule 2;windows;3d5e2f8a1c9b47e0a6d2b8c5e3f1a490;;any
Test rule 3;windows;64ec88ca00b268e5ba1a35678a1b2c3d4e5f67890abcdef1234567890abcdef1;;office document
```

Подробное описание полей шаблона файла для импорта

Название поля	Описание
`Rule name (optional)`	Имя правила. Максимальная длина – 260 символов. Если поле не заполнено, в качестве имени правила будет использовано значение поля `File hash` или `Path to object`. Необязательное поле.
`OS (mandatory, specify 'windows', 'linux' or 'macos')`	Операционная система, для которой предназначено правило. Допустимые значения: • `windows` • `linux` • `macos` В политику Kaspersky Endpoint Security для Windows могут быть импортированы только те правила, для которых указано значение `windows`. Обязательное поле.
`File hash (MD5 or SHA256)`	Хеш файла. Допустимые значения: • MD5-хеш. 32 символа (в шестнадцатеричном формате) без разделителей и пробелов, регистр не важен. • SHA256-хеш. 64 символа (в шестнадцатеричном формате) без разделителей и пробелов, регистр не важен. Обязательное поле, если не заполнено поле `Path to object`.
`Path to object (optional if file hash is specified)`	Полный путь к файлу, включая его имя и расширение. Максимальная длина пути – 32 767 символов. Путь не должен содержать знаки переноса строки, табуляцию и следующие специальные символы: `*`, `?`, `"`, `<`, `>`, `|`. Обязательное поле, если не заполнено поле `File hash`.

Название поля	Описание
`File Type (optional, specify 'any', 'executable', 'script', 'office document')`	Тип файла, который будет заблокирован: • `any` – приложение не будет учитывать тип файла (значение по умолчанию). • `executable` – исполняемый файл. • `script` – скрипт. • `office document` – файл офисного формата. Запрет запуска объектов поддерживает определенный набор расширений файлов офисного формата и определенный набор интерпретаторов скриптов. Если вы укажете неверный тип файла, приложение не заблокирует запуск данного файла или скрипта. Необязательное поле.

Чтобы импортировать правила запрета запуска, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. Выберите вкладку **Запрет запуска**.
6. В блоке **Правила запрета запуска** нажмите на кнопку .

   Запустится мастер импорта правил запрета запуска.
7. Пропустите первый шаг мастер и нажмите на кнопку **Далее**.
8. На следующем шаге загрузите подготовленный файл с правилами.

   Загруженные правила отобразятся в виде таблицы. Если в файле содержалось несколько одинаковых правил, приложение оставит только одно из них. Также в таблицу не будут добавлены правила, уже содержащиеся в списке правил компонента.

   Вы можете отредактировать правила перед импортом, а также удалить правила, которые не требуется импортировать. Также при необходимости вы можете исправить ошибки в заполнении полей правил.
9. Нажмите на кнопку **Готово**.

Kaspersky Endpoint Security добавит правила из файла к существующим. Правила с ошибками не будут импортированы.

Сетевая изоляция компьютера

Сетевая изоляция позволяет автоматически изолировать компьютеры от сети, в результате реагирования на обнаружение индикатора компрометации (IOC) – *автоматический режим*. Также вы можете включить Сетевую изоляцию вручную на время исследования обнаруженной угрозы – *ручной режим*.

После включения Сетевой изоляции приложение разрывает все активные и блокирует все новые сетевые соединения TCP/IP на компьютере, кроме следующих соединений:

- соединения, указанные в исключениях из Сетевой изоляции;
- соединения, инициированные службами Kaspersky Endpoint Security;
- соединения, инициированные Агентом администрирования Kaspersky Security Center;
- соединения с SVM и Сервером интеграции, если приложение используется в режиме Легкого агента;
- соединения с KSN при интеграции приложения с Kaspersky Managed Detection and Response.

Вы можете настроить параметры компонента только в Web Console.

Автоматический режим Сетевой изоляции

Вы можете настроить автоматическое включение Сетевой изоляции, в результате реагирования на обнаружение IOC. Для настройки автоматического режима Сетевой изоляции предназначена групповая политика.

Как настроить автоматическое включение Сетевой изоляции компьютера при обнаружении IOC

1. В главном окне Web Console выберите **Управление активами → Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Поиск IOC**.

   Откроется окно свойств задачи.

   Если требуется, создайте задачу *Поиск IOC*.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Настройки реагирования**.

5. В блоке **Настройка действий по реагированию при обнаружении IOC** выберите **Обнаруживать и реагировать** и установите флажок **Изолировать устройство от сети**.

6. Сохраните внесенные изменения.

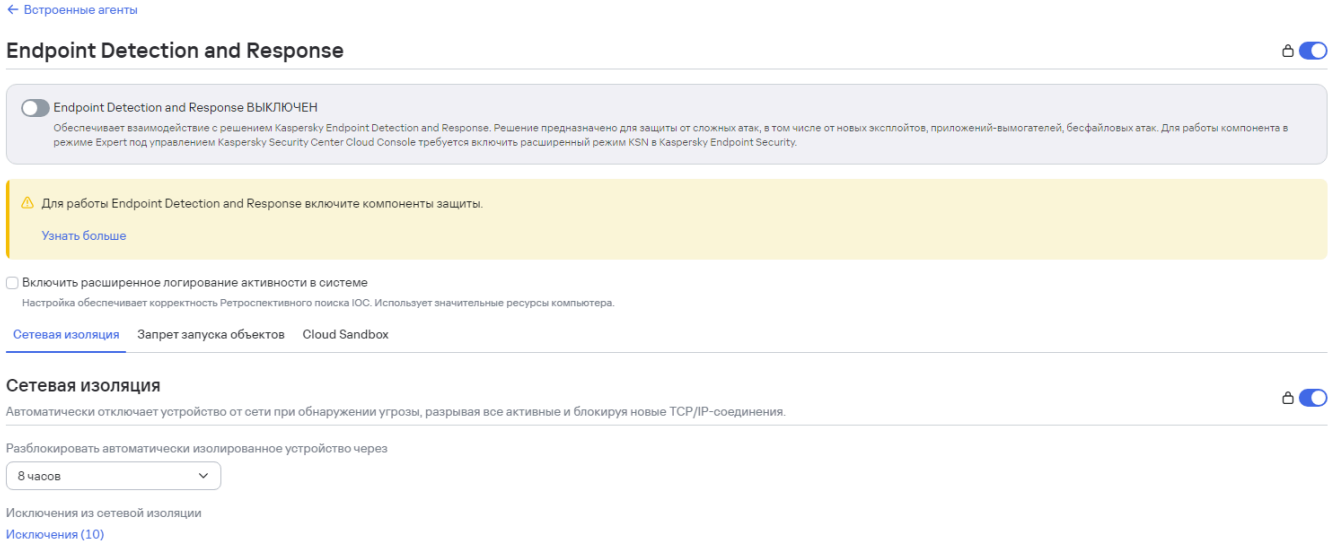
   В результате при обнаружении IOC приложение изолирует компьютер от сети для предотвращения распространения угрозы.

Вы можете настроить автоматическое выключение Сетевой изоляции по истечении заданного периода времени. По умолчанию приложение выключает Сетевую изоляцию через 8 часов с момента включения. Также вы можете выключить Сетевую изоляцию вручную (см. инструкцию ниже). После выключения Сетевой изоляции компьютер может работать в сети без ограничений.

Как задать период выключения Сетевой изоляции компьютера в автоматическом режиме

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. Выберите вкладку **Сетевая изоляция**.
6. Задайте период времени, по истечении которого Сетевая изоляция должна быть выключена.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.



Параметры интеграции с EDR

Ручной режим Сетевой изоляции

Вы можете включать или выключать Сетевую изоляцию вручную. Для настройки ручного режима Сетевой изоляции предназначены свойства компьютера в консоли Kaspersky Security Center.

Вы можете включить Сетевую изоляцию следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали алерта – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum и в справке Kaspersky Endpoint Detection and Response Expert.

- С помощью локальных параметров приложения.

- В свойствах задачи *Поиск IOC*.

  Если в результате выполнения задачи *Поиск IOC* обнаружен IOC, то вы можете изолировать компьютер от сети прямо из результатов поиска IOC (свойства задачи *Поиск IOC* → **Параметры приложения** → **Результаты поиска IOC**). Также Kaspersky Endpoint Security позволяет сразу настроить дополнительные параметры: период выключения Сетевой изоляции и исключения из Сетевой изоляции.

Как вручную включить Сетевую изоляцию компьютера

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите вкладку **Приложения**.
4. Нажмите на **Kaspersky Endpoint Security для Windows 14.2**.

   Откроются локальные параметры приложения.
5. Выберите вкладку **Параметры приложения**.
6. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response**.
7. В блоке параметров **Сетевая изоляция** нажмите на кнопку **Изолировать компьютер от сети**.

Вы можете настроить автоматическое выключение Сетевой изоляции по истечении заданного периода времени. По умолчанию приложение выключает Сетевую изоляцию через 8 часов с момента включения. После выключения Сетевой изоляции компьютер может работать в сети без ограничений.

Как задать период выключения Сетевой изоляции компьютера в ручном режиме

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите вкладку **Задачи**.

   Откроется список задач, доступных на компьютере.
4. Выберите задачу **Сетевая изоляция**.
5. Выберите вкладку **Параметры приложения**.
6. В открывшемся окне задайте период времени, по истечении которого Сетевая изоляция должна быть выключена.
7. Сохраните внесенные изменения.

Как вручную выключить Сетевую изоляцию компьютера

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите вкладку **Приложения**.

4. Нажмите на **Kaspersky Endpoint Security для Windows 14.2**.

   Откроются локальные параметры приложения.

5. Выберите вкладку **Параметры приложения**.

6. Перейдите в раздел **Встроенные агенты → Endpoint Detection and Response**.

7. В блоке параметров **Сетевая изоляция** нажмите на кнопку **Разблокировать изолированный от сети компьютер**.

Вы также можете выключить Сетевую изоляцию локально из командной строки.

Начиная с версии Kaspersky Endpoint Security для Windows 12.10 добавлена возможность управлять Сетевой изоляцией в деталях алерта. Также в деталях алерта вы можете задавать срок Сетевой изоляции компьютера. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum и в справке Kaspersky Endpoint Detection and Response Expert.

Исключения из Сетевой изоляции

Вы можете задать исключения из Сетевой изоляции. Сетевые соединения, подпадающие под заданные правила, не будут заблокированы на компьютере после включения Сетевой изоляции.

Для настройки исключений из Сетевой изоляции в приложении доступен список *стандартных сетевых профилей*. По умолчанию в исключения входят сетевые профили, состоящие из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент. Также вы можете изменить параметры стандартных сетевых профилей или задать исключения вручную (см. инструкцию ниже).

Исключения, заданные в свойствах политики, применяются, только если Сетевая изоляция включена приложением автоматически, в результате реагирования на обнаружение угрозы. Исключения, заданные в свойствах компьютера, применяются, только если Сетевая изоляция включена вручную в свойствах компьютера в консоли Kaspersky Security Center или в деталях алерта.

Активная политика не блокирует применение исключений из Сетевой изоляции, заданных в свойствах компьютера, так как сценарии применения этих параметров разные.

Как добавить исключение из Сетевой изоляции в автоматическом режиме

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Встроенные агенты → Endpoint Detection and Response**.

5. Выберите вкладку **Сетевая изоляция**.

6. В блоке **Исключения из сетевой изоляции** нажмите **Исключения**.

7. В открывшемся окне нажмите на кнопку **Добавить** → **Добавить из профиля** и выберите стандартные сетевые профили для настройки исключений.

   Сетевые соединения из профиля будут добавлены в список исключений из Сетевой изоляции. Вы можете просмотреть свойства сетевых соединений. При необходимости, вы можете изменить параметры сетевого соединения.

8. Если требуется, добавьте исключение из Сетевой изоляции вручную. Для этого в окне со списком исключений нажмите на кнопку **Добавить** → **Добавить** и задайте параметры сетевого соединения вручную.

9. Сохраните внесенные изменения.

Как добавить исключение из Сетевой изоляции в ручном режиме

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.

3. Выберите вкладку **Задачи**.

   Откроется список задач, доступных на компьютере.

4. Выберите задачу **Сетевая изоляция**.

5. Выберите вкладку **Параметры приложения**.

6. В открывшемся окне нажмите **Исключения**.

7. В открывшемся окне нажмите на кнопку **Добавить из профиля** и выберите стандартные сетевые профили для настройки исключений.

   Сетевые соединения из профиля будут добавлены в список исключений из Сетевой изоляции. Вы можете просмотреть свойства сетевых соединений. При необходимости, вы можете изменить параметры сетевого соединения.

8. Если требуется, добавьте исключение из Сетевой изоляции вручную. Для этого в окне со списком исключений нажмите на кнопку **Добавить** и задайте параметры сетевого соединения вручную.

9. Сохраните внесенные изменения.

Вы также можете просмотреть список исключений из Сетевой изоляции локально из командной строки. При этом компьютер должен быть изолирован.

Начиная с версии Kaspersky Endpoint Security для Windows 12.10 добавлена возможность добавлять исключения из Сетевой изоляции в деталях алерта. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum и в справке Kaspersky Endpoint Detection and Response Expert.

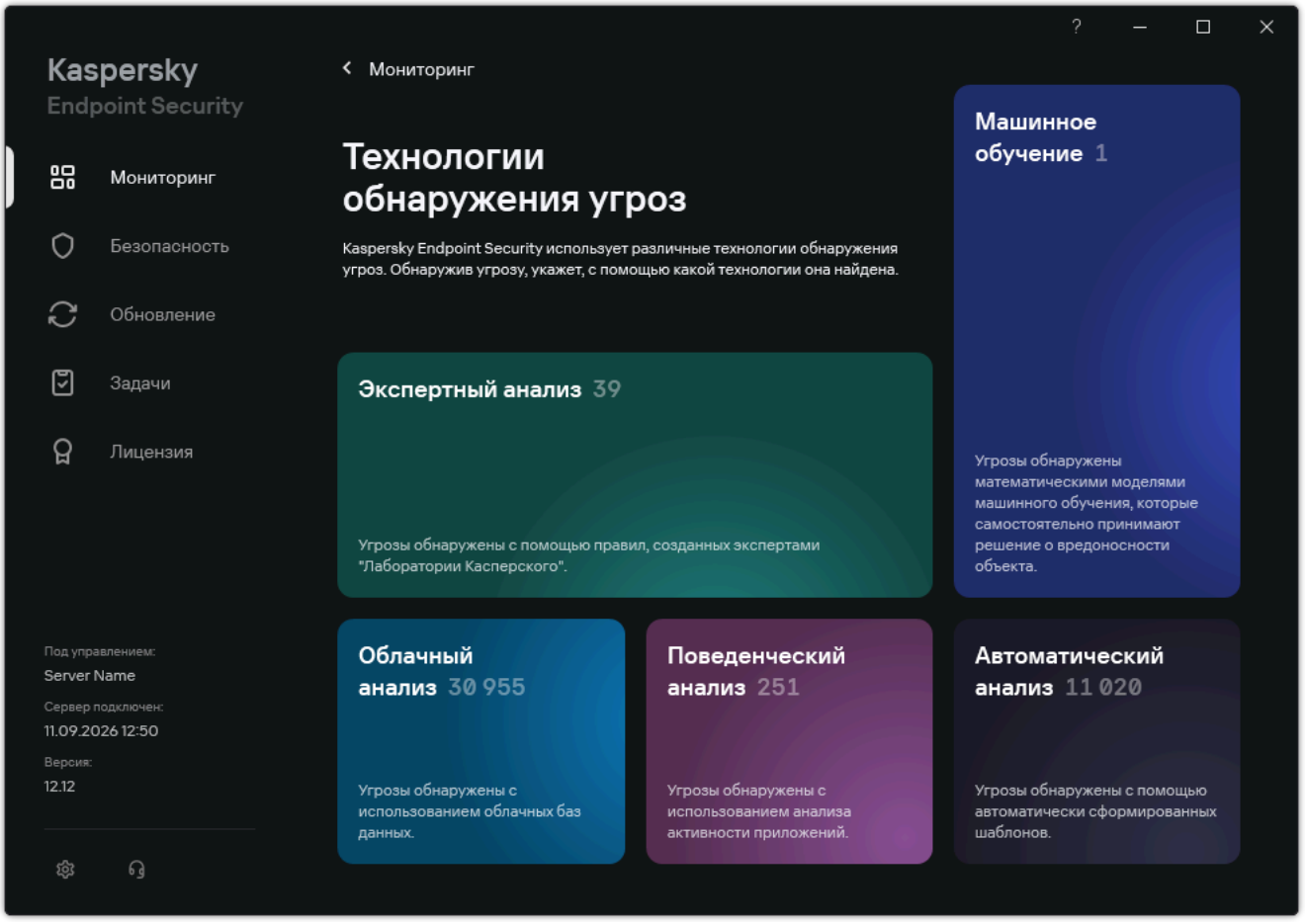
Cloud Sandbox

Cloud Sandbox – технология, которая позволяет обнаруживать сложные угрозы на компьютере. Kaspersky Endpoint Security автоматически отправляет обнаруженные файлы в Cloud Sandbox для анализа. Cloud Sandbox запускает эти файлы в изолированной среде для выявления вредоносной активности и принимает решение о репутации этих файлов. Далее данные об этих файлах попадают в Kaspersky Security Network. Таким образом, если Cloud Sandbox обнаружил вредоносный файл, Kaspersky Endpoint Security выполнит действие для устранения угрозы на всех компьютерах, на которых обнаружит этот файл.

Для работы Cloud Sandbox необходимо включить использование Kaspersky Security Network.

Если вы используете Kaspersky Private Security Network, технология Cloud Sandbox недоступна.

Технология Cloud Sandbox включена постоянно и доступна всем пользователям Kaspersky Security Network независимо от типа лицензии, которую вы используете. Если у вас развернуто решение Endpoint Detection and Response Optimum, вы можете включить отдельный счетчик для угроз, обнаруженных с помощью Cloud Sandbox. Вы можете использовать этот счетчик для составления статистики при анализе обнаруженных угроз. Kaspersky Endpoint Security будет указывать технологию обнаружения угроз Cloud Sandbox в *Отчет об угрозах* в консоли Kaspersky Security Center.



Счетчики угроз

Чтобы включить счетчик Cloud Sandbox, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты → Endpoint Detection and Response**.
5. Выберите вкладку **Cloud Sandbox**.
6. Включите переключатель **Использование Cloud Sandbox ВКЛЮЧЕНО**.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

В результате угрозы Kaspersky Endpoint Security включит счетчик угроз, обнаруженных с помощью Cloud Sandbox, в главном окне приложения в разделе **Технологии обнаружения угроз**. Также Kaspersky Endpoint Security будет указывать технологию обнаружения угроз Cloud Sandbox в *Отчет об угрозах* в консоли Kaspersky Security Center.

Раздел политики Endpoint Detection and Response

Руководство по миграции с KEA на KES для EDR Optimum

В Kaspersky Endpoint Security для Windows включен встроенный агент для работы решения Kaspersky Endpoint Detection and Response Optimum. Теперь вам не нужно отдельное приложение Kaspersky Endpoint Agent для работы EDR Optimum. Все функции Kaspersky Endpoint Agent будет выполнять Kaspersky Endpoint Security.

При развертывании Kaspersky Endpoint Security на компьютеры с установленным приложением Kaspersky Endpoint Agent решение Kaspersky Endpoint Detection and Response Optimum продолжит работу с Kaspersky Endpoint Security. Также приложение Kaspersky Endpoint Agent будет удалено с компьютера. Такое же поведение в системе будет при обновлении Kaspersky Endpoint Security до версии 11.7.0 или выше.

Kaspersky Endpoint Security несовместим с Kaspersky Endpoint Agent. Установить оба этих приложения на одном компьютере невозможно.

Для работы Kaspersky Endpoint Security в составе Kaspersky Endpoint Detection and Response Optimum должны быть выполнены следующие условия:

- Kaspersky Endpoint Detection and Response Optimum версии 2.0 или выше.
- Kaspersky Security Center версии 13.2 или выше (включая Агент администрирования). В более ранних версиях Kaspersky Security Center невозможно активировать функциональность EDR Optimum.
- Управление EDR Optimum доступно только в Kaspersky Security Center Web Console.

- Передача данных на Сервер администрирования включена. Данные нужны для получения информации о помещенных на компьютере файлах на карантин в Web Console.
- Установлено фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования. Для работы EDR Optimum с Сервером администрирования через Kaspersky Security Center Web Console вам нужно установить новое безопасное соединение – *фоновое соединение*.

Этапы миграции конфигурации [KES+KEA] на [KES+встроенный агент] для EDR Optimum

1. **Обновление веб-плагина Kaspersky Endpoint Security**

   Управление компонентом EDR Optimum доступно с помощью веб-плагина Kaspersky Endpoint Security версии 11.7.0 или выше.

2. **Миграция политик и задач**

   Перенесите параметры работы Kaspersky Endpoint Agent в приложение Kaspersky Endpoint Security для Windows. Для этого в Web Console предназначен Мастер миграции с Kaspersky Endpoint Agent.

   Как перенести параметры политик и задач с помощью Мастера миграции с Kaspersky Endpoint Agent в Web Console

   В главном окне Web Console выберите **Операции** → **Миграция с Kaspersky Endpoint Agent**.

   В результате запустится мастер миграции политик и задач. Следуйте его указаниям.

   Шаг 1. Миграция политик

   Мастер миграции создает новую политику, в которой будут объединены параметры политик Kaspersky Endpoint Security и Kaspersky Endpoint Agent. В списке политик выберите политики Kaspersky Endpoint Agent, параметры которых вы хотите объединить с политикой Kaspersky Endpoint Security. Нажмите на политику Kaspersky Endpoint Agent, чтобы выбрать политику Kaspersky Endpoint Security, с которой вы хотите объединить параметры. Убедитесь, что политики выбраны верно и перейдите к следующем шагу.

   Шаг 2. Миграция задач

   Мастер миграции создает новые задачи для Kaspersky Endpoint Security. В списке задач выберите задачи Kaspersky Endpoint Agent, которые вы хотите создать для Kaspersky Endpoint Security. Перейдите к следующему шагу.

   Шаг 3. Завершение работы мастера

   Завершите работу мастера. В результате работы мастера будут выполнены следующие действия:

   - Создана новая политика Kaspersky Endpoint Security.

В политике объединены параметры Kaspersky Endpoint Security и Kaspersky Endpoint Agent. Политика называется *<Название политики Kaspersky Endpoint Security> & <Название политики Kaspersky Endpoint Agent>*. Новая политика имеет статус *Неактивна*. Для продолжения работы измените статусы политик Kaspersky Endpoint Agent и Kaspersky Endpoint Security на *Неактивна* и активируйте новую объединенную политику.

После миграции из Kaspersky Endpoint Agent на Kaspersky Endpoint Security для Windows убедитесь, что в новой политике настроены функции передачи данных на Сервер администрирования: данные о файлах карантина и данные о цепочке развития угрозы. Значения параметров передачи данных не мигрируют из политики Kaspersky Endpoint Agent.

- Созданы новые задачи Kaspersky Endpoint Security.

  Новые задачи представляют собой копии задач Kaspersky Endpoint Agent. При этом мастер оставляет задачи Kaspersky Endpoint Agent без изменений.

3. **Лицензирование функции EDR Optimum**

   Если для активации Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Agent у вас общая лицензия Kaspersky Endpoint Detection and Response Optimum или Kaspersky Optimum Security, после обновления приложения до версии 11.7.0 или выше активация функции EDR Optimum будет выполнена автоматически. Дополнительных действий не требуется.

   Если для активации функциональности EDR Optimum у вас отдельная лицензия Kaspersky Endpoint Detection and Response Optimum Add-on, вам нужно убедиться, что ключ EDR Optimum добавлен в хранилище Kaspersky Security Center и функция автоматического распространения лицензионного ключа включена. После обновления приложения до версии 11.7.0 или выше активация функции EDR Optimum будет выполнена автоматически.

   Если для активации Kaspersky Endpoint Agent у вас лицензия Kaspersky Endpoint Detection and Response Optimum или Kaspersky Optimum Security, а для активации Kaspersky Endpoint Security для Windows у вас другая лицензия, вам нужно заменить ключ для Kaspersky Endpoint Security для Windows на общий ключ Kaspersky Endpoint Detection and Response Optimum или Kaspersky Optimum Security. Вы можете заменить ключ с помощью задачи *Добавление ключа*.

4. **Установка / Обновление версии приложения Kaspersky Endpoint Security**

   Для миграции функций EDR Optimum во время установки или обновления приложения рекомендуется использовать задачу удаленной установки. При создании задачи удаленной установки вам нужно выбрать компонент EDR Optimum в параметрах инсталляционного пакета.

   Также вы можете обновить приложение следующими способами:

   - Через службу обновлений "Лаборатории Касперского".
   - Локально с помощью мастера установки.

   Kaspersky Endpoint Security поддерживает автоматический выбор компонентов при обновлении приложения на компьютере с установленным приложением Kaspersky Endpoint Agent. Автоматический выбор компонентов зависит от прав учетной записи пользователя, который обновляет приложение.

   Если вы обновляете Kaspersky Endpoint Security с помощью EXE-файла или с помощью MSI-файла под системной учетной записью (SYSTEM), Kaspersky Endpoint Security получает доступ к действующим лицензиям решений "Лаборатории Касперского". Таким образом, если на компьютере, например, установлено приложение Kaspersky Endpoint Agent и активировано решение EDR Optimum, установщик Kaspersky Endpoint Security автоматически сконфигурирует набор компонентов и выберет компонент EDR Optimum. При этом Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent. Запуск установщика MSI под системной учетной записью (SYSTEM) обычно выполняется при обновлении через службу обновлений "Лаборатории Касперского" или при развертывании инсталляционного пакета через Kaspersky Security Center.

Если вы обновляете Kaspersky Endpoint Security с помощью MSI-файла под учетной записью непривилегированного пользователя, у Kaspersky Endpoint Security отсутствует доступ к действующим лицензиям решений "Лаборатории Касперского". При этом Kaspersky Endpoint Security автоматически выбирает компоненты на основании конфигурации Kaspersky Endpoint Agent. Далее Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent.

Kaspersky Endpoint Security поддерживает обновление без перезагрузки компьютера. Вы можете выбрать режим обновления приложения в параметрах политики.

5. **Проверка работы приложения**

Если после установки или обновления приложения компьютер имеет статус *Критический* в консоли Kaspersky Security Center, выполните следующие действия:

- Убедитесь, что на компьютере установлен Агент администрирования версии 13.2 или выше.
- Проверьте статус работы встроенного агента с помощью отчета *Отчет о статусе компонентов приложения*. Если компонент имеет статус *Не установлен*, установите компонент с помощью задачи *Изменение состава компонентов приложения*. Если компонент имеет статус *Не поддерживается лицензией*, убедитесь, что вы активировали функцию встроенного агента.
- Убедитесь, что вы приняли условия Положения о Kaspersky Security Network в новой политике Kaspersky Endpoint Security для Windows.

Kaspersky Anti Targeted Attack Platform



Kaspersky Endpoint Security для Windows поддерживает работу с решением Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* – решение, предназначенное для своевременного обнаружения сложных угроз, таких как целевые атаки, сложные постоянные угрозы (англ. Advanced Persistent Threat, APT), атаки "нулевого дня" и другие. Kaspersky Anti Targeted Attack Platform включает в себя три функциональных блока:

- Kaspersky Anti Targeted Attack (далее также "*KATA*");
- Kaspersky Endpoint Detection and Response (далее также "*EDR (KATA)*");
- Network Detection and Response (далее также "*NDR (KATA)*").

Вы можете приобрести все функциональные блоки или приобрести функциональные блоки по отдельности. Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform. В приложение добавлены встроенные агенты для работы компонентов EDR, NDR. Также приложение поддерживает работу с компонентом Sandbox, который входит в состав KATA.

Средства анализа угроз

Kaspersky Endpoint Detection and Response использует следующие средства анализа угроз (Threat Intelligence):

- Интеграция с Kaspersky Threat Intelligence Portal, который содержит и отображает информацию о репутации файлов и веб-адресов.
- База угроз "Лаборатории Касперского" Kaspersky Threats.
- Инфраструктура облачных служб Kaspersky Security Network (далее также "KSN"), предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Принцип работы решения

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

Настройка интеграции с EDR (KATA) и NDR (KATA) выполняется в консоли Kaspersky Security Center. Дальнейшее управление встроенным агентом осуществляется в консоли Kaspersky Anti Targeted Attack Platform, включая запуск задач, управление объектами на карантине, просмотр отчетов и другие действия.

Конфигурации Kaspersky Endpoint Security для работы с EDR / NDR (KATA)

Для работы с EDR / NDR (KATA) предусмотрены следующие конфигурации:

- **[KES+встроенный агент]**. В этой конфигурации Kaspersky Endpoint Security является и приложением, которое обеспечивает безопасность компьютера, и приложением для работы с EDR / NDR (KATA). Встроенный агент для EDR (KATA) доступен в Kaspersky Endpoint Security для Windows версии 12.1 и выше. Встроенный агент для NDR (KATA) доступен в Kaspersky Endpoint Security для Windows версии 12.7 и выше.
- **[стороннее EPP+EDR-агент]**. В этой конфигурации безопасность IT-инфраструктуры обеспечивает система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков. Работу с EDR / NDR (KATA) обеспечивает Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента (EDR-агент). В этой конфигурации EDR-агент совместим со сторонними EPP-приложениями. EDR-агент для EDR (KATA) доступен в Kaspersky Endpoint Security для Windows версии 12.3 и выше. EDR-агент для NDR (KATA) доступен в Kaspersky Endpoint Security для Windows версии 12.7 и выше.

Поддержка предыдущих версий Kaspersky Endpoint Security

Если вы используете Kaspersky Endpoint Security 11.2.0 – 11.8.0 для взаимодействия с Kaspersky Anti Targeted Attack Platform (EDR), в состав приложения включено приложение Kaspersky Endpoint Agent. Вы можете установить Kaspersky Endpoint Agent совместно с Kaspersky Endpoint Security.

Если вы используете Kaspersky Endpoint Security 11.9.0 – 12.0, вам нужно установить Kaspersky Endpoint Agent отдельно, потому что в Kaspersky Endpoint Security 11.9.0 дистрибутив приложения Kaspersky Endpoint Agent исключен из комплекта поставки Kaspersky Endpoint Security.

Интеграция встроенного агента с EDR (KATA)

Для интеграции с EDR (KATA) вам нужно установить встроенный агент Endpoint Detection and Response (KATA). Вы можете выбрать компонент для интеграции с EDR (KATA) во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

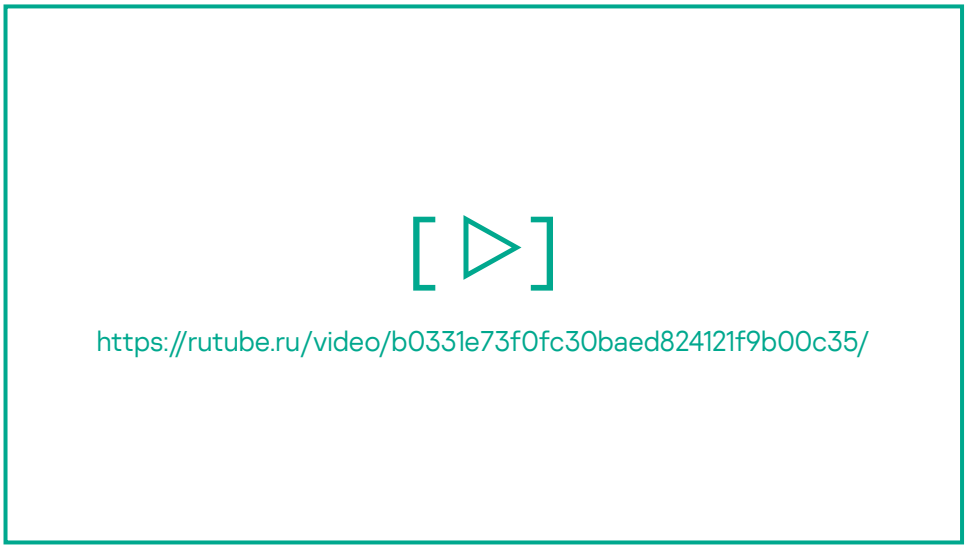
Начиная с версии Kaspersky Endpoint Security для Windows 12.11 компонент EDR (KATA) переименован в **Endpoint Detection and Response Expert (версия 8.0 и выше)**. В этой версии приложения компонент совместим с Kaspersky Anti Targeted Attack Platform версии 7.1 и ниже и Kaspersky Endpoint Detection and Response Expert (on-premises).

Компоненты Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), Endpoint Detection and Response Expert (on-premises) несовместимы между собой.

Для работы EDR (KATA) должны быть выполнены следующие условия:

- Kaspersky Anti Targeted Attack Platform версии 5.0 – 7.1.
- Kaspersky Endpoint Security для Windows 12.1 или выше. Подробнее о совместимости KATA с Kaspersky Endpoint Security разных версий см. в справке Kaspersky Anti Targeted Attack Platform.
- Kaspersky Security Center версии 14.2 или выше. В более ранних версиях Kaspersky Security Center невозможно активировать функциональность EDR (KATA).
- Приложение активировано и функциональность входит в лицензию.
- Компонент Endpoint Detection and Response (KATA) включен (см. инструкцию ниже).
- Компоненты приложения, которые обеспечивают работу EDR (KATA), включены и работают. Работу EDR (KATA) обеспечивают следующие компоненты:
  - Защита от файловых угроз.
  - Защита от веб-угроз.
  - Защита от почтовых угроз.
  - Защита от эксплойтов.

- Анализ поведения.
- Предотвращение вторжений.
- AMSI-защита.
- Фоновая проверка.
- Kaspersky Security Network.



Интеграция с Endpoint Detection and Response (KATA) состоит из следующих этапов:

1. **Установка встроенного агента Endpoint Detection and Response (KATA)**

   Вы можете выбрать компонент EDR (KATA) во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

   > Для завершения обновления приложения с новыми компонентами нужно перезагрузить компьютер.

2. **Активация Endpoint Detection and Response (KATA)**

   Вам нужно приобрести отдельную лицензию на использование EDR (KATA) (например, Kaspersky Endpoint Detection and Response (KATA) Add-on).

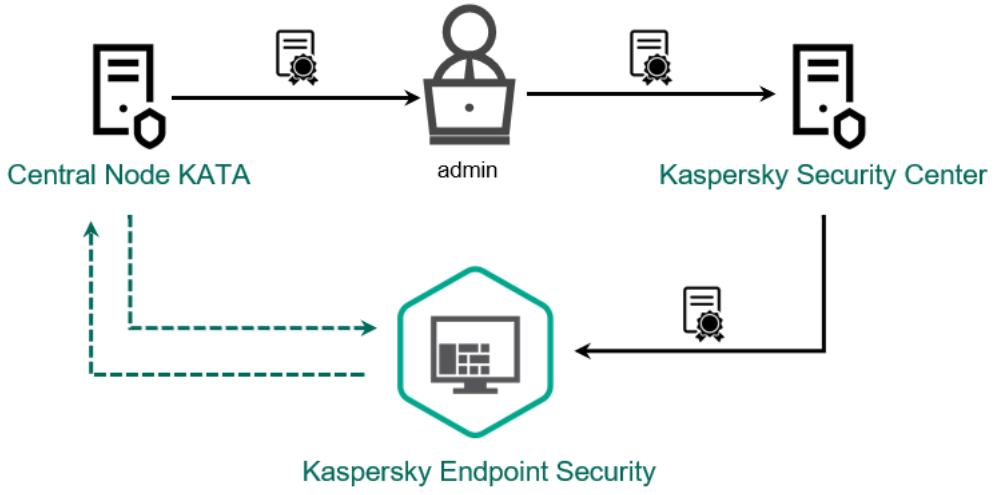
   Функциональность будет доступна после добавления отдельного ключа, который включает в себя функциональность EDR (KATA). В результате на компьютере будет добавлено несколько ключей: ключ для Kaspersky Endpoint Security и ключ для Kaspersky Endpoint Detection and Response (KATA).

   Лицензирование отдельной функциональности EDR (KATA) не отличается от лицензирования Kaspersky Endpoint Security.

   Убедитесь, что функциональность EDR (KATA) включены в лицензию и работают в локальном интерфейсе приложения.

3. **Подключение к Central Node**

Для работы Kaspersky Anti Targeted Attack Platform необходимо установить доверенное соединение между Kaspersky Endpoint Security и компонентом Central Node. Для настройки доверенного соединения вам нужен TLS-сертификат. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). Далее вам нужно добавить TLS-сертификат в Kaspersky Endpoint Security (см. инструкцию ниже).



Добавление TLS-сертификата в Kaspersky Endpoint Security

По умолчанию Kaspersky Endpoint Security проверяет только TLS-сертификат Central Node. Чтобы сделать соединение более безопасным, вы можете включить дополнительную проверку компьютера в Central Node (двусторонняя аутентификация). Для включения такой проверки вам нужно включить двустороннюю аутентификацию в параметрах Central Node и Kaspersky Endpoint Security. Также для двусторонней аутентификации вам нужен криптоконтейнер. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

Как подключить компьютер с Kaspersky Endpoint Security к Central Node в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Detection and Response → Endpoint Detection and Response Expert (on-premises)**.
5. Установите флажок **Endpoint Detection and Response Expert (версия 7.1 и ниже)**.
6. Нажмите на кнопку **Настройки подключения к серверам**.
7. Настройте параметры подключения к серверам:
   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу Central Node.
   - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

- **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

  Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

8. Нажмите на кнопку **OK**.
9. Добавьте серверы Central Node. Для этого укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.

   Вы можете добавить несколько адресов сервера Central Node. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.
10. Если требуется, настройте параметры отправки телеметрии.
11. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как подключить компьютер с Kaspersky Endpoint Security к Central Node в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response Expert (on-premises)**.
5. Включите переключатель **Endpoint Detection and Response Expert (on-premises) ВКЛЮЧЕН**.
6. Для настройки EDR (KATA) в списке решений выберите **Endpoint Detection and Response Expert (версия 7.1 и ниже)**.
7. Нажмите на кнопку **Настройки подключения**.
8. Настройте параметры подключения к серверам:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу Central Node.
   - **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

- **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

  Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

9. Нажмите на кнопку **OK**.
10. Добавьте серверы Central Node. Для этого укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.

    Вы можете добавить несколько адресов сервера Central Node. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.
11. Если требуется, настройте параметры отправки телеметрии.
12. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Вы также можете добавить TLS-сертификат локально из командной строки.

В результате компьютер будет добавлен в консоли Kaspersky Anti Targeted Attack Platform. Проверьте статус работы компонентов с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонентов в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Endpoint Detection and Response Expert (версия 8.0 и выше)**.

Вы можете проверить статус работы компонентов в консоли Kaspersky Security Center в свойствах компьютера в разделе **Компоненты**. Отображение статуса компонента в консоли имеет особенность. Если компонент не установлен и функциональность не включена в лицензию, то консоль покажет статус **Не поддерживается лицензией** вместо **Не установлен**.

Начиная с версии Kaspersky Endpoint Security для Windows 12.6 вы можете контролировать статус компонента EDR (KATA) в Консоли администрирования (MMC) Kaspersky Security Center. Текущий статус компонента отображается в свойствах компьютера в графе **Статус Endpoint Sensor** (значения *Выполняется*, *Запускается*, *Остановлена*, *Приостановлена*, *Сбой*, *Нет данных*). В Web Console статус Endpoint Sensor отсутствует.

Интеграция встроенного агента с NDR (KATA)

Для интеграции с NDR (KATA) вам нужно установить встроенный агент Network Detection and Response (KATA). Вы можете выбрать компонент для интеграции с NDR (KATA) во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

Для работы NDR (KATA) должны быть выполнены следующие условия:

- Kaspersky Anti Targeted Attack Platform версии 7.0 или выше.
- Kaspersky Endpoint Security для Windows 12.7 или выше.
- Установлена единая платформа управления OSMP (Open Single Management Platform) или Kaspersky Security Center версии 14.2 или выше. В более ранних версиях Kaspersky Security Center невозможно активировать функциональность EDR / NDR (KATA).
- Приложение активировано и функциональность входит в лицензию.
- Компонент Network Detection and Response (KATA) включен (см. инструкцию ниже).
- Компоненты приложения, которые обеспечивают работу NDR (KATA), включены и работают. Работу NDR (KATA) обеспечивают следующие компоненты:
  - Защита от файловых угроз.
  - Защита от веб-угроз.
  - Защита от почтовых угроз.
  - Защита от эксплойтов.
  - Анализ поведения.
  - Предотвращение вторжений.
  - AMSI-защита.
  - Фоновая проверка.
  - Kaspersky Security Network.

Интеграция с Network Detection and Response (KATA) состоит из следующих этапов:

1. **Установка встроенного агента Network Detection and Response (KATA)**

   Вы можете выбрать компонент NDR (KATA) во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

   > Для завершения обновления приложения с новыми компонентами нужно перезагрузить компьютер.

2. **Активация Network Detection and Response (KATA)**

   Вам нужно приобрести отдельную лицензию на использование NDR (KATA) (например, Kaspersky Network Detection and Response (KATA) Add-on).

   Функциональность будет доступна после добавления отдельного ключа, который включает в себя функциональность NDR (KATA). В результате на компьютере будет добавлено несколько ключей: ключ для Kaspersky Endpoint Security и ключ для Network Detection and Response (KATA).

   Лицензирование отдельной функциональности NDR (KATA) не отличается от лицензирования Kaspersky Endpoint Security.

Убедитесь, что функциональность NDR (KATA) включена в лицензию и работает в локальном интерфейсе приложения.

3 Подключение к Серверу интеграции

Для работы NDR (KATA) необходимо установить доверенное соединение между Kaspersky Endpoint Security и компонентом Сервер интеграции. Для настройки доверенного соединения вам нужен TLS-сертификат. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). Далее вам нужно добавить TLS-сертификат в Kaspersky Endpoint Security (см. инструкцию ниже).

По умолчанию Kaspersky Endpoint Security проверяет только TLS-сертификат Сервера интеграции. Чтобы сделать соединение более безопасным, вы можете включить дополнительную проверку компьютера в Сервере интеграции (двусторонняя аутентификация). Для включения такой проверки вам нужно включить двустороннюю аутентификацию в параметрах Сервера интеграции и Kaspersky Endpoint Security. Также для двусторонней аутентификации вам нужен криптоконтейнер. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

Как подключить компьютер с Kaspersky Endpoint Security к Серверу интеграции в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Detection and Response** → **Network Detection and Response (KATA)**.
5. Установите флажок **Network Detection and Response (KATA)**.
6. Нажмите на кнопку **Настройки подключения к серверам**.
7. Настройте параметры подключения к серверам:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от Сервера интеграции. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому Серверу интеграции.
   - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с Сервером интеграции. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).
   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и Сервером интеграции. Для использования двусторонней аутентификации вам нужно в параметрах Сервера интеграции включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Сервера интеграции вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

     Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

8. Нажмите на кнопку **OK**.

9. Добавьте Серверы интеграции. Для этого укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.

   Вы можете добавить несколько адресов Сервера интеграции. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.

10. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как подключить компьютер с Kaspersky Endpoint Security к Серверу интеграции в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Встроенные агенты** → **Network Detection and Response (KATA)**.

5. Включите переключатель **Network Detection and Response (KATA) ВКЛЮЧЕН**.

6. Нажмите на кнопку **Настройки подключения**.

7. Настройте параметры подключения к серверам:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от Сервера интеграции. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому Серверу интеграции.

   - **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с Сервером интеграции. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и Сервером интеграции. Для использования двусторонней аутентификации вам нужно в параметрах Сервера интеграции включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Сервера интеграции вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

     Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

8. Выберите Сервер интеграции из списка доступных серверов или добавьте сервер вручную. Выбор сервера доступен, если компьютер находится под управлением OSMP. Для выбора сервера нажмите на кнопку **Добавить** и в выпадающем списке выберите **Выбрать сервер**.

   Если выбор серверов недоступен, выпадающий список отображаться не будет. Для добавления сервера вручную нажмите на кнопку **Добавить**.

9. В открывшемся окне выберите нужный сервер.

   Если вы ранее уже добавили TLS-сертификат, вам будет предложено заменить его TLS-сертификатом выбранного сервера.

10. Для добавления сервера вручную нажмите на кнопку **Добавить** и в выпадающем списке выберите **Новый сервер**.

    Откроется форма добавления сервера.

11. Укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.

    Вы можете добавить несколько Серверов интеграции. Kaspersky Endpoint Security пытается установить соединение с первым сервером из списка. Если установить соединение не удалось, выполняется попытка подключения ко второму серверу и так далее по списку.

12. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Вы также можете добавить TLS-сертификат локально из командной строки.

В результате компьютер будет добавлен в консоли Kaspersky Anti Targeted Attack Platform. Проверьте статус работы компонентов с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонентов в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Network Detection and Response (KATA)**.

Вы можете проверить статус работы компонентов в консоли Kaspersky Security Center в свойствах компьютера в разделе **Компоненты**. Отображение статуса компонента в консоли имеет особенность. Если компонент не установлен и функциональность не включена в лицензию, то консоль покажет статус **Не поддерживается лицензией** вместо **Не установлен**.

Настройка отправки телеметрии EDR (KATA)

Телеметрия – список событий, которые произошли на защищаемом компьютере. Kaspersky Endpoint Security анализирует данные телеметрии и отправляет их на серверы Kaspersky Anti Targeted Attack Platform во время синхронизации. События телеметрии поступают на сервер почти непрерывно. Kaspersky Endpoint Security выполняет синхронизацию с сервером при выполнении любого из следующих условий:

- Истек период синхронизации.
- Количество событий в буфере превысило максимальное значение.

Таким образом, по умолчанию приложение выполняет синхронизацию каждые 30 секунд или при накоплении в буфере 1024 события. Вы можете настроить параметры синхронизации в политике Kaspersky Endpoint Security и выбрать оптимальные значения исходя из нагрузки на сеть (см. инструкцию ниже).

Если соединение между Kaspersky Endpoint Security и сервером отсутствует, то приложение ставит новые события в очередь. При восстановлении соединения Kaspersky Endpoint Security отправляет события из очереди на сервер по порядку. При этом, чтобы не перегрузить сервер, Kaspersky Endpoint Security может отправлять не все события. Для этого вы можете оптимизировать параметры отправки событий и, например, задать максимальное количество событий в час (см. инструкцию ниже).

Если вы используете Kaspersky Anti Targeted Attack Platform совместно с другим решением, которое также использует телеметрию, вы можете выключить отправку телеметрии для KATA (EDR) (см. инструкцию ниже). Это позволит оптимизировать нагрузку на серверы для этих решений. Например, если у вас развернуто решение Managed Detection and Response и KATA (EDR), вы можете использовать телеметрию MDR, а создавать задачи реагирования на угрозы в KATA (EDR).

Как настроить параметры отправки телеметрии в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Detection and Response** и выберите компонент, который вы хотите настроить: **Endpoint Detection and Response Expert (on-premises)** или **Network Detection and Response (KATA)**.
5. Настройте параметр **Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)**. Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Endpoint Security передает данные об изменениях в параметрах приложения и задачах.
6. Убедитесь, что флажок **Отправлять телеметрию в KATA** установлен.
7. Если требуется, в блоке **Настройка передачи данных** настройте параметры синхронизации с сервером:
   - **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд.
   - **Максимальное количество пакетов событий**. Приложение выполняет синхронизацию с сервером при заполнении буфера событиями. По умолчанию установлено значение 1024 события.
8. Если требуется, в блоке **Регулирование количества запросов** установите флажок **Включить регулирование количества запросов**.

   Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события.

9. Настройте параметры оптимизации отправки событий на сервер:

   - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

   - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Endpoint Security восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.

10. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить параметры отправки телеметрии в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Встроенные агенты → Endpoint Detection and Response Expert (on-premises)**.

5. Для настройки EDR (KATA) в списке решений выберите **Endpoint Detection and Response Expert (версия 7.1 и ниже)**.

6. В блоке **Настройка передачи данных** убедитесь, что установлен флажок **Отправлять телеметрию на серверы KATA**.

7. Настройте параметр **Отправлять запрос на синхронизацию на сервер каждые (мин.)**. Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Endpoint Security передает данные об изменениях в параметрах приложения и задачах.

8. Убедитесь, что флажок **Отправлять телеметрию на серверы KATA** установлен.

9. Если требуется, в блоке **Настройка передачи данных** настройте параметры синхронизации с сервером:

   - **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд.

   - **Максимальное количество пакетов событий**. Приложение выполняет синхронизацию с сервером при заполнении буфера событиями. По умолчанию установлено значение 1024 события.

10. Если требуется, в блоке **Регулирование количества запросов** установите флажок **Включить регулирование количества запросов**.

    Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события.

11. Настройте параметры оптимизации отправки событий на сервер:

    - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

    - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Endpoint Security восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.

12. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Интеграция с KATA** → **Исключения из телеметрии**.
5. В блоке **Настройка передачи данных** установите флажок **Использовать исключения**.
6. Нажмите на кнопку **Добавить** и настройте параметры исключения:

   > Критерии применяются при помощи логического *И*.

   - **Путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. Для работы исключения необходимо обязательно задать путь к файлу.
   - **Командная строка**. Команда для запуска объекта.
   - **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo).

     Подробнее о ресурсе VersionInfo см. на сайте Microsoft.
   - **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo).
   - **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo).
   - **MD5**. MD5-хеш файла.

- **SHA256**. SHA256-хеш файла.
- **Типы событий**. Для работы исключения необходимо выбрать хотя бы один тип событий.

7. Сохраните внесенные изменения.

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

1. Выберите **Kaspersky Endpoint Security для Windows (14.3)** → **Откат обновления**.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 3. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную.

Шаг 4. Определение названия задачи

Введите название задачи.

Шаг 7. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Исключения из телеметрии EDR (KATA)

Для повышения производительности и оптимизации отправки данных на Сервер сбора телеметрии вы можете настроить исключения из телеметрии. Например, вы можете отменить обработку данных о сетевых коммуникациях для отдельных приложений.

Как создать исключение из телеметрии в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки** → **Исключения и типы объектов**.
4. В блоке **Настройки телеметрии** → **Телеметрия EDR (KATA) / NDR (KATA)** нажмите на кнопку **Настройка**.
5. В открывшемся окне настройте исключения из телеметрии (см. таблицу ниже).

   Приложение применяет условия для исключений при помощи логического И. Для создания правила необходимо обязательно задать значение в поле **Полный путь** и выбрать хотя бы один из типов событий в списке **Использовать для следующих типов событий**.
6. Сохраните внесенные изменения.

Как создать исключение из телеметрии в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки телеметрии**.
5. Выберите вкладку **Телеметрия EDR (KATA) / NDR (KATA)**.
6. В открывшемся окне настройте исключения из телеметрии (см. таблицу ниже).

   Приложение применяет условия для исключений при помощи логического И. Для создания правила необходимо обязательно задать значение в поле **Полный путь** и выбрать хотя бы один из типов событий.
7. Сохраните внесенные изменения.

Параметры исключений из телеметрии

Параметр	Описание
Исключенные процессы	**Оптимизировать объем отправляемой телеметрии**. Kaspersky Endpoint Security позволяет оптимизировать объем отправляемых данных и исключить из телеметрии события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB, службы WinRM и процесса Агента администрирования klnagent.exe, а также расширенную информацию о типе сетевых пакетов для всех типов сетевых протоколов. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **Использовать для следующих типов событий**: • **Изменение файла**. • **Сетевые события**. • **Интерактивный ввод команд в консоли**. • **Модуль загружен**. • **Изменение в реестре**. • **Логи DNS**. • **Доступ к процессу**. • **Внедрение в код**. • **Запрос WMI**. • **Канал**. • **LDAP**. • **AMSI**.
Исключенные сетевые коммуникации	**Название правила**. **Направление**. **Протокол**. **Сырой сокет**. **Номер протокола**. **TLS-сертификат**. **Локальный порт или диапазон**. **Удаленный порт или диапазон**. **Локальный адрес**. Сетевой адрес компьютера, для которого Kaspersky Endpoint Security исключает телеметрию из сетевого трафика. **Удаленный адрес**. Сетевой адрес компьютера, для которого Kaspersky Endpoint Security исключает телеметрию из сетевого трафика. Для IP-адресов поддерживается только формат IPv4. **Приложения**. Список исполняемых файлов приложений, для которых Kaspersky Endpoint Security исключает EDR-телеметрию из сетевого трафика.

Параметр	Описание
Исключенные операции с файлами	**Название правила**. **Имя или маска файла**. Имя или маска имени файла или папки, при доступе к которым Kaspersky Endpoint Security применяет правило исключения. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски. **Тип операции**. **Предыдущий путь**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные операции с DNS	**Название правила**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **DNS**: • **IP-адрес DNS-сервера**. • **Настройки запроса**. • **Статус**. • **Имя домена**. • **ID типа настроек**. • **Ответная информация**.

Параметр	Описание
Исключенные операции с LDAP	**Название правила**. **Область поиска LDAP**. **Фильтр**. **Отличительное имя для поиска объектов в LDAP**. **Атрибуты объекта**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные запросы доступа к процессу	**Название правила**. **Тип операции**. **Запрошенный доступ к процессу**. **Трассировка стека вызовов**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс**, **Родительский процесс**, **Файл целевого процесса**, **Дескриптор исходного процесса** и **Дескриптор целевого процесса**. • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Укажите критерии срабатывания правила, а также для каких типов событий его использовать**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.

Параметр	Описание
Исключенные внедрения в код	**Название правила**. **Метод доступа**. **Стек вызовов**. **Измененная командная строка**. **Адрес внедрения**. **Имя внедряемой библиотеки DLL**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные запросы WMI	**Название правила**. **Тип операции WMI**. **Удаленный запрос**. **Имя компьютера, с которого выполнена команда WMI**. **Учетная запись пользователя WMI**. **Выполненная команда WMI**. **Пространство имен WMI**. **Фильтр потребителя событий WMI**. **Имя созданного потребителя событий WMI**. **Исходный код потребителя событий WMI**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.

Параметр	Описание
Исключенные операции с каналами	**Название правила**. **Имя канала**. **Тип операции**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные изменения реестра	**Название правила**. **Тип операции**. **Путь**. **Имя значения**. **Значение**. **Полное имя файла реестра**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные операции с устройствами	**Название правила**. **Тип устройства**. **Идентификатор устройства**. **Название устройства**.

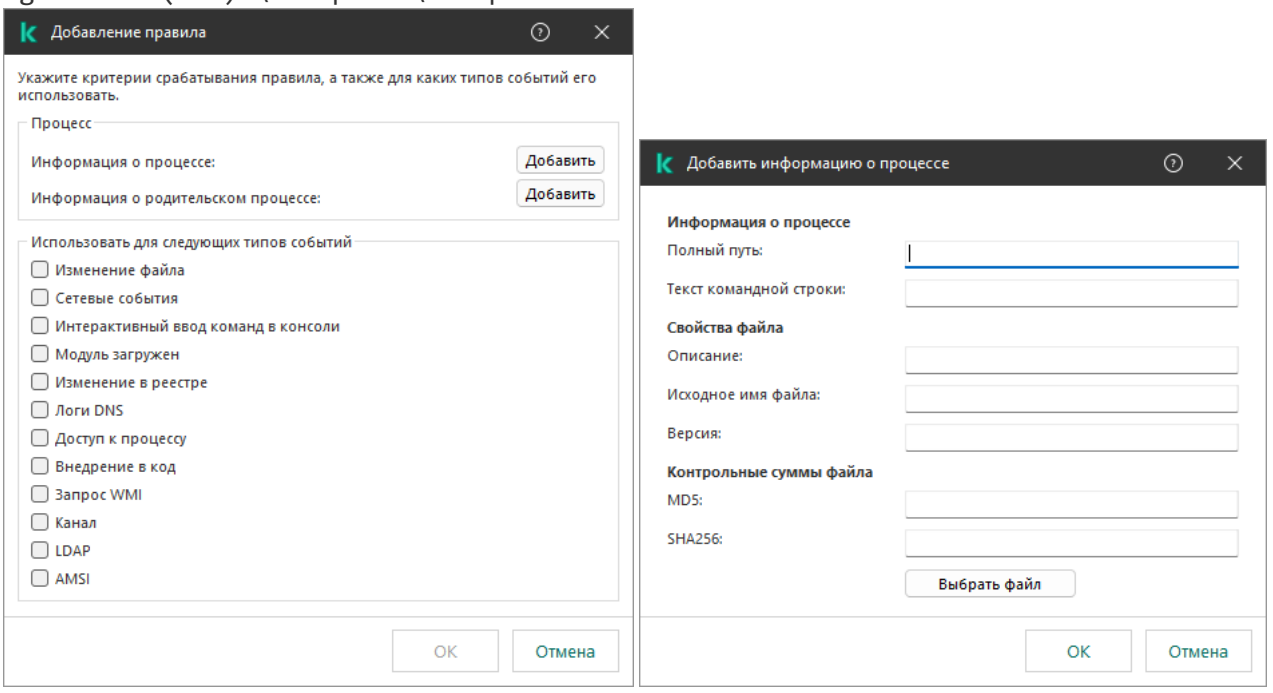
Пример 1. Исключенные процессы

Чтобы исключить из телеметрии события от сторонних приложений (процессов), вам нужно открыть окно исключений для EDR-телеметрии на вкладке **Исключенные процессы** и добавить исполняемый файл приложения.

Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И.

Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. Например:

- `C:\Program Files\*\notepad++.exe`;
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`.



Исключение процесса

Пример 1. Изменение файла

Если вы постоянно работаете над скриптами в приложении Notepad++ и вы хотите исключить из телеметрии события изменения этих файлов, вам нужно добавить в исключения из телеметрии исполняемый файл Notepad++.

Задайте следующие параметры:

- **Полный путь**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Использовать для следующих типов событий**: Изменение файла.

Пример 2. Сетевые события

Если вы используете приложение WinSCP для работы с файлами на удаленном сервере и вы хотите исключить сетевые события, вам нужно добавить в исключения из телеметрии исполняемый файл WinSCP.

Задайте следующие параметры:

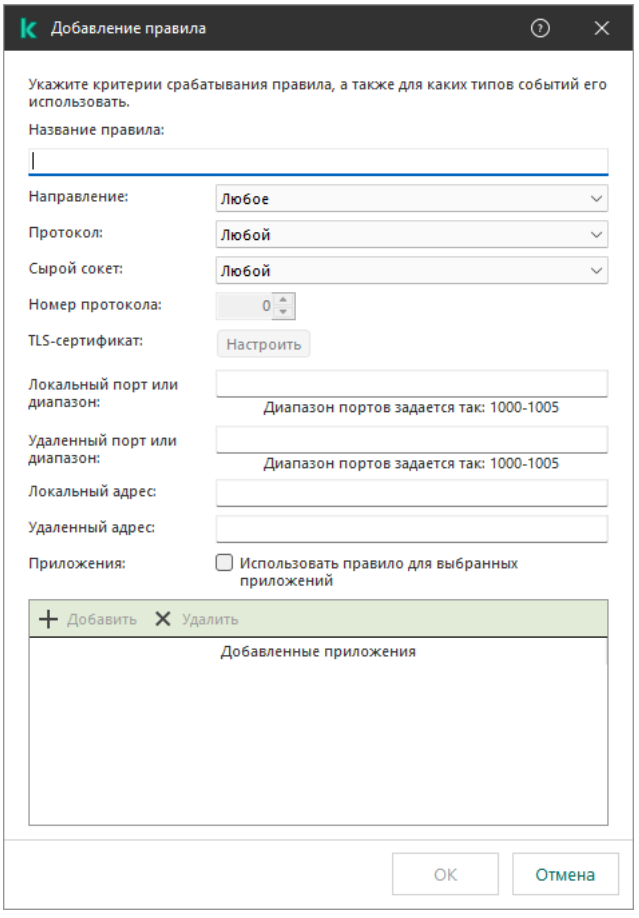
- **Полный путь**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (не обязательно).
- **Использовать для следующих типов событий**: Сетевые события.

Пример 2. Исключенные сетевые коммуникации

Чтобы исключить из телеметрии события о подключениях к удаленным сервисам, вам нужно открыть окно исключений для EDR-телеметрии на вкладке **Исключенные сетевые коммуникации** и добавить параметры подключения: протокол, порт, направление, IP-адрес, сертификат TLS и другие.

Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И.

Невозможно указать адрес подсети (например, 10.28.0.0/24). Приложение позволяет указать только один IP-адрес (например, 10.28.0.105).



Исключение сетевой коммуникации

Если вы используете корпоративный веб-сервер и вы хотите исключить события от браузера при обращении к этому веб-серверу, вам нужно добавить в исключения из телеметрии IP-адрес сервера и исполняемый файл браузера.

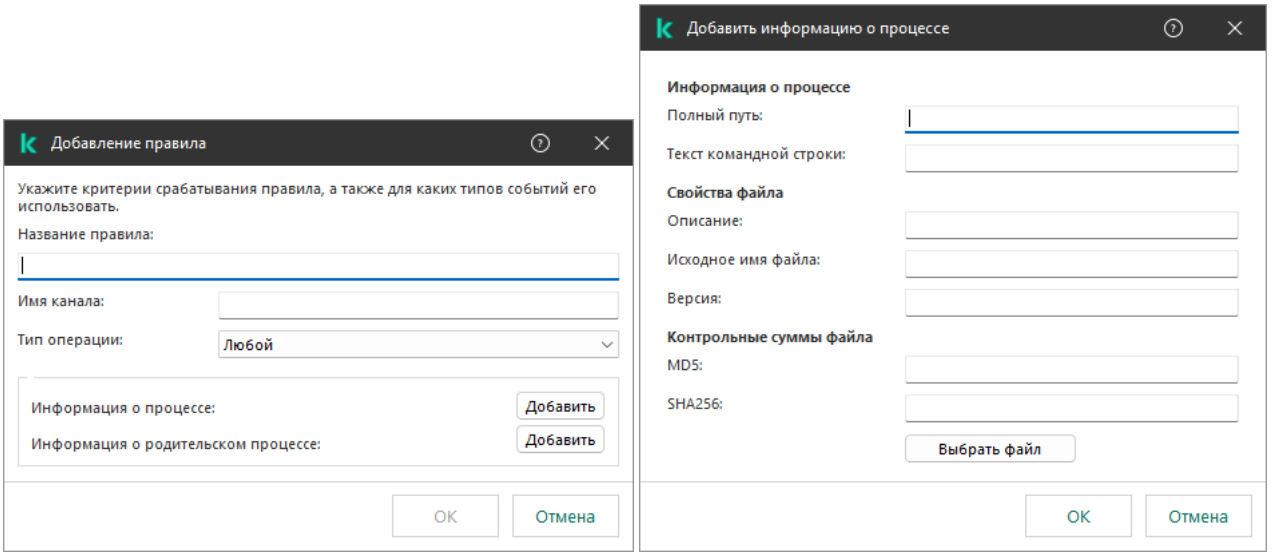
Задайте следующие параметры:

- **Протокол**: TCP.
- **Удаленный порт или диапазон**: 443.
- **Удаленный адрес**: 10.28.0.105.
- **Приложения**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Пример 3. Исключенные операции с файлами

Чтобы исключить из телеметрии события об операциях с доверенными файлами, вам нужно открыть окно исключений для EDR-телеметрии на вкладке **Исключенные операции с файлами** и добавить доверенный файл.

Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И.



Исключение операций с файлами

Если приложение ведет журнал и вы хотите исключить события изменения файла журнала, вам нужно добавить в исключения из телеметрии файл журнала и исполняемый файл приложения.

Задайте следующие параметры:

- **Имя или маска файла**: `C:\Apache24\logs\error.log`.
- **Тип операции**: Изменение файла.
- **Полный путь**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Пример 4. Исключенные изменения реестра

Чтобы исключить из телеметрии события об изменениях реестра, вам нужно открыть окно исключений для EDR-телеметрии на вкладке **Исключенные изменения реестра** и добавить путь реестра.

Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И.

Если приложение постоянно изменяет свои значения в реестре и вы хотите исключить из телеметрии события изменения реестра, вам нужно добавить в исключения из телеметрии путь в реестре и исполняемый файл приложения.

Задайте следующие параметры:

- **Тип операции**: Изменение.
- **Путь**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Полный путь**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

Kaspersky Anti Targeted Attack Platform включает в себя компонент Sandbox (KATA Sandbox). *Sandbox* – технология, которая позволяет обнаруживать сложные угрозы на компьютере. Sandbox анализирует поведение объектов для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации. Sandbox выполняет анализ и проверку объектов на специальных серверах с развернутыми виртуальными образами операционных систем Microsoft Windows (серверы Sandbox). Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform.

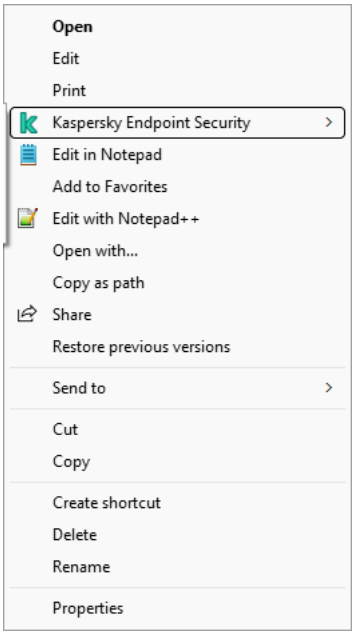
Для активации KATA Sandbox вам потребуется лицензионный ключ, который включает в себе функциональность KATA или KEDR. Подробнее о доступных функциональностях см. в справке Kaspersky Anti Targeted Attack Platform.

KATA Sandbox позволяет проверять файлы в следующих режимах:

- *Вручную*. Пользователь вручную отправляет файл на проверку из контекстного меню (**Отправить в Sandbox**). При отправке файла в Sandbox приложение также проверяет файл с помощью антивирусных баз.
- *Автоматически*. Приложение автоматически обнаруживает объекты и отправляет их на проверку в Sandbox.

После отправки файла в Sandbox файл остается доступным для пользователя. Kaspersky Endpoint Security регистрирует соответствующее событие, а также отправляет событие в Kaspersky Security Center и консоль Kaspersky Anti Targeted Attack Platform. Если Sandbox выявляет вредоносную активность, Kaspersky Endpoint Security выполняет действие по реагированию на угрозы автоматически (например, удаляет объект и запускает проверку важных областей).

Для работы KATA Sandbox в ручном режиме должно быть развернуто решение Kaspersky Anti Targeted Attack Platform версии 7.0 или выше. Для работы KATA Sandbox в автоматическом режим должно быть развернуто решение Kaspersky Anti Targeted Attack Platform версии 8.0 или выше.



Проверка в KATA Sandbox из контекстного меню

Интеграция встроенного агента с KATA Sandbox

Для интеграции с KATA Sandbox вам нужно добавить компонент Sandbox. Вы можете выбрать компонент Sandbox во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

Для отправки файлов на проверку вам нужно включить интеграцию с KATA Sandbox и добавить сервер Central Node, которые развернуты внутри решения. Управление компонентом доступно только в Kaspersky Security Center Web Console. Управлять компонентом в Консоли администрирования (MMC) невозможно.

Чтобы включить или выключить интеграцию с KATA Sandbox, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Sandbox**.
5. Используйте переключатель **Интеграция с Sandbox ВКЛЮЧЕНА**, чтобы включить или выключить компонент.

6. Выберите режим работы KATA Sandbox:

   - **Вручную**. Пользователь вручную отправляет файл на проверку из контекстного меню (**Отправить в Sandbox**).
   - **Автоматически**. Приложение автоматически обнаруживает объекты и отправляет их на проверку в Sandbox.
   - **Комбинированный**.

7. Перейдите по ссылке **Настройки подключения**.

8. Настройте параметры подключения к серверу Central Node:

   - **Время ожидания (мсек.)**. Время ожидания соединения с сервером Central Node. По истечению заданного времени ожидания Kaspersky Endpoint Security отправит запрос на следующий сервер. Вы можете увеличить время ожидания соединения с сервером, если у вас низкая скорость соединения или соединение нестабильно. Рекомендованное значение времени ожидания запроса не более 0,5 сек.
   - **Очередь запросов**. Размер папки хранения очереди запросов. При отправке нескольких объектов на проверку в Sandbox приложение Kaspersky Endpoint Security создает очередь запросов. По умолчанию размер папки хранения очереди запросов ограничен 100 МБ. После достижения максимального размера Sandbox перестает добавлять новые запросы в очередь и отправляет соответствующее событие в Kaspersky Security Center. Вы можете настроить размер папки хранения очереди запросов в зависимости от конфигурации сервера.
   - **TLS-сертификат сервера**. Для настройки доверенного соединения с сервером Central Node вам нужно подготовить TLS-сертификат. Далее вам нужно добавить сертификат на компьютер с помощью политики. Также вам нужно добавить сертификат на сервер Central Node.
   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

9. В блоке **Подключение к серверам Sandbox** нажмите на кнопку **Добавить**.

10. В открывшемся окне введите адрес сервера Central Node (IPv4, IPv6, DNS), а также порт подключения к серверу.

    Подробнее о развертывании виртуальных образов и конфигурации серверов Central Node см. в справке Kaspersky Anti Targeted Attack Platform.

11. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

В результате компонент Sandbox будет включен. Проверьте статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Sandbox**.

Настройка действий по реагированию на угрозы

Если Sandbox выявляет вредоносную активность, Kaspersky Endpoint Security выполняет действие по реагированию на угрозы автоматически (например, удаляет объект и запускает проверку важных областей).

Чтобы настроить действия по реагированию на угрозы, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Sandbox**.
5. В блоке **Действие при обнаружении угрозы** выберите нужное действие:

   - **Копию поместить на карантин, объект удалить**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удаляет вредоносный объект, обнаруженный на компьютере. Перед удалением объекта Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин.

   - **Запустить проверку важных областей**. Если выбран этот вариант действия, то Kaspersky Endpoint Security запускает задачу *Проверка важных областей*. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

   - **Создать задачу поиска IOC**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически создает задачу *Поиск IOC (автономная задача поиска IOC)*. Вы можете настроить режим запуска задачи, область поиска и действие при обнаружении IOC (*Копию поместить на карантин, объект удалить* или *Запустить проверку важных областей*). Для настройки других параметров задачи *Поиск IOC* перейдите в свойства задачи.
6. Если требуется, в блоке **Область поиска IOC** настройте параметры для задачи *Поиск IOC*:

   - **Важные файловые области**. Если выбран этот вариант, Kaspersky Endpoint Security выполняет поиск IOC только в важных файловых областях компьютера: память ядра и загрузочные секторы.

   - **Файловые области на системном диске компьютера**. Если выбран этот вариант, Kaspersky Endpoint Security выполняет поиск IOC на системном диске компьютера.

7. Если требуется, в блоке **Запуск задачи поиска IOC** настройте параметры для задачи *Поиск IOC*:

   - **Вручную**. Режим запуска, при котором вы запускаете задачу *Поиск IOC* вручную в удобное для вас время.
   - **Автоматически**. Режим запуска, при котором Kaspersky Endpoint Security запускает задачу *Поиск IOC* автоматически после обнаружения угрозы.
   - **Выполнять только во время простоя компьютера**. Режим запуска, при котором Kaspersky Endpoint Security запускает задачу *Поиск IOC*, если включена экранная заставка или компьютер заблокирован. Если пользователь разблокировал компьютер, Kaspersky Endpoint Security приостанавливает выполнение задачи. Таким образом, приложение может выполнять задачу несколько дней.

8. Настройте дополнительные параметры задачи *Поиск IOC*.

9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Руководство по миграции с KEA на KES для EDR (KATA)

Начиная с версии Kaspersky Endpoint Security для Windows 12.1 в приложение добавлен встроенный агент для работы с компонентом Kaspersky Endpoint Detection and Response в составе решения Kaspersky Anti Targeted Attack Platform. Теперь вам не нужно отдельное приложение Kaspersky Endpoint Agent для работы EDR (KATA). Все функции Kaspersky Endpoint Agent будет выполнять Kaspersky Endpoint Security. При этом нагрузка на серверы Kaspersky Anti Targeted Attack Platform останется прежней.

При развертывании Kaspersky Endpoint Security на компьютеры с установленным приложением Kaspersky Endpoint Agent решение Kaspersky Anti Targeted Attack Platform (EDR) продолжит работу с Kaspersky Endpoint Security. Также приложение Kaspersky Endpoint Agent будет удалено с компьютера. Такое же поведение в системе будет при обновлении Kaspersky Endpoint Security до версии 12.1 или выше.

> Kaspersky Endpoint Security несовместим с Kaspersky Endpoint Agent. Установить оба этих приложения на одном компьютере невозможно.

Для работы Kaspersky Endpoint Security в составе Endpoint Detection and Response (KATA) должны быть выполнены следующие условия:

- Kaspersky Anti Targeted Attack Platform версии 5.0 или выше.
- Kaspersky Security Center версии 14.2 или выше (включая Агент администрирования). В более ранних версиях Kaspersky Security Center невозможно активировать функциональность Endpoint Detection and Response (KATA).

Этапы миграции конфигурации [KES+KEA] на [KES+встроенный агент] для EDR (KATA)

1. **Обновление плагина управления Kaspersky Endpoint Security**

   Управление компонентом EDR (KATA) доступно с помощью плагина управления Kaspersky Endpoint Security версии 12.1 или выше. В зависимости от консоли Kaspersky Security Center, которую вы используете, обновите плагин управления в Консоли администрирования (MMC) или веб-плагин в Web Console.

2. **Миграция политик и задач**

Перенесите параметры работы Kaspersky Endpoint Agent в приложение Kaspersky Endpoint Security для Windows. Вам доступны следующие способы:

- Мастер миграции с Kaspersky Endpoint Agent. Мастер миграции с Kaspersky Endpoint Agent работает только в Web Console.

  Как перенести параметры политик и задач с помощью Мастера миграции с Kaspersky Endpoint Agent в Web Console

  В главном окне Web Console выберите **Операции** → **Миграция с Kaspersky Endpoint Agent**.

  В результате запустится мастер миграции политик и задач. Следуйте его указаниям.

  Шаг 1. Миграция политик

  Мастер миграции создает новую политику, в которой будут объединены параметры политик Kaspersky Endpoint Security и Kaspersky Endpoint Agent. В списке политик выберите политики Kaspersky Endpoint Agent, параметры которых вы хотите объединить с политикой Kaspersky Endpoint Security. Нажмите на политику Kaspersky Endpoint Agent, чтобы выбрать политику Kaspersky Endpoint Security, с которой вы хотите объединить параметры. Убедитесь, что политики выбраны верно и перейдите к следующем шагу.

  Шаг 2. Миграция задач

  Мастер миграции не поддерживает задачи EDR (KATA). Пропустите этот шаг.

  Шаг 3. Завершение работы мастера

  Завершите работу мастера. В результате работы мастера будет создана новая политика Kaspersky Endpoint Security. В политике объединены параметры Kaspersky Endpoint Security и Kaspersky Endpoint Agent. Политика называется *<Название политики Kaspersky Endpoint Security> & <Название политики Kaspersky Endpoint Agent>*. Новая политика имеет статус *Неактивна*. Для продолжения работы измените статусы политик Kaspersky Endpoint Agent и Kaspersky Endpoint Security на *Неактивна* и активируйте новую объединенную политику.

  Мастер миграции в Web Console пропускает и не переносит следующие параметры политики:

  - Запрет на изменение параметров **Настройки подключения** ("замок").

    По умолчанию изменение параметров разрешено ("замок" открыт). Поэтому параметры не будут применены на компьютере. Вам нужно запретить изменение параметров и закрыть "замок".

  - Криптоконтейнер.

    Если вы используете двустороннюю аутентификацию для подключения к серверам Central Node, нужно добавить криптоконтейнер повторно.

Так как Мастер миграции не переносит эти параметры, могут возникнуть ошибки подключения компьютера к серверам Central Node. Для устранения ошибок вам нужно перейти в свойства политики и настроить параметры подключения.

- Стандартный Мастер массовой конвертации политик и задач. Мастер массовой конвертации политик и задач доступен в Консоли администрирования (MMC). Подробнее о Мастере массовой конвертации политик и задач см. в справке Kaspersky Security Center.

Для корректной работы Kaspersky Endpoint Security на серверах рекомендуется добавить в доверенную зону файлы, важные для выполнения сервером своих функций. Для SQL-серверов вам нужно добавить файлы баз данных MDF и LDF. Для Microsoft Exchange-серверов вам нужно добавить файлы CHK, EDB, JRS, LOG и JSL. Вы можете использовать маски, например, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах.

Исключения EDR-телеметрии не мигрируют из политики Kaspersky Endpoint Agent в политику Kaspersky Endpoint Security. Kaspersky Endpoint Security имеет собственные инструменты исключений – доверенные приложения. Работа Kaspersky Endpoint Security оптимизирована таким образом, что отсутствие отдельных исключений EDR-телеметрии не приводит к дополнительной нагрузке на компьютер в сравнении с Kaspersky Endpoint Agent. Kaspersky Endpoint Security использует телеметрию не только для EDR (KATA), но и для работы компонентов защиты приложения. Поэтому переносить отдельные исключения EDR-телеметрии не требуется. Если вы наблюдаете снижение производительности компьютера, проверьте работу приложения (см. п. 7. Проверка производительности).

3. **Лицензирование функции EDR (KATA)**

Для активации Kaspersky Endpoint Security в составе решения Kaspersky Anti Targeted Attack Platform вам потребуется отдельная лицензия Kaspersky Endpoint Detection and Response (KATA) Add-on. Вы можете добавить ключ с помощью задачи *Добавление ключа*. Таким образом, в приложение будет добавлено два ключа: *Kaspersky Endpoint Security* и *Kaspersky Endpoint Detection and Response (KATA)*.

Лицензирование Kaspersky Endpoint Detection and Response (KATA) Add-on на компьютерах с уже активированными функциями EDR Optimum или EDR Expert имеет следующие особенности:

- Если для лицензирования Kaspersky Endpoint Security с функциями EDR Optimum или EDR Expert вы используете *файл ключа*, добавить отдельный ключ Kaspersky Endpoint Detection and Response (KATA) Add-on невозможно. Вы можете или перейти на использование кода активации для лицензирования, или обратиться к поставщику услуг за новым файлом ключа для активации Kaspersky Endpoint Security и функций EDR. Поставщик услуг предоставит вам один или несколько файлов ключей для лицензирования.

- Если для лицензирования Kaspersky Endpoint Security без функций EDR Optimum или EDR Expert вы используете *файл ключа*, вы можете добавить отдельный ключ Kaspersky Endpoint Detection and Response (KATA) Add-on без перевыпуска файлов ключей.

- Если для лицензирования вы используете *код активации*, сервер активации "Лаборатории Касперского" автоматически перевыпустит ключи, и функции EDR (KATA) будут доступны автоматически. При этом функции EDR Optimum и EDR Expert будут выключены.

- Kaspersky Endpoint Security позволяет добавлять до двух активных ключей: ключ Kaspersky Endpoint Security и ключ типа Add-on. Также вы можете добавлять до двух резервных ключей. Один резервный ключ Kaspersky Endpoint Security и один резервный ключ типа Add-on.

4. **Установка / Обновление версии приложения Kaspersky Endpoint Security**

Для миграции функций EDR (KATA) во время установки или обновления приложения рекомендуется использовать задачу удаленной установки. При создании задачи удаленной установки вам нужно выбрать компонент EDR (KATA) в параметрах инсталляционного пакета.

Также вы можете обновить приложение следующими способами:

- Через службу обновлений "Лаборатории Касперского".

- Локально с помощью мастера установки.

Kaspersky Endpoint Security поддерживает автоматический выбор компонентов при обновлении приложения на компьютере с установленным приложением Kaspersky Endpoint Agent. Автоматический выбор компонентов зависит от прав учетной записи пользователя, который обновляет приложение.

Если вы обновляете Kaspersky Endpoint Security с помощью EXE-файла или с помощью MSI-файла под системной учетной записью (SYSTEM), Kaspersky Endpoint Security получает доступ к действующим лицензиям решений "Лаборатории Касперского". Таким образом, если на компьютере установлено приложение Kaspersky Endpoint Agent и активировано решение EDR (KATA), установщик Kaspersky Endpoint Security автоматически сконфигурирует набор компонентов и выберет компонент EDR (KATA). При этом Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent. Запуск установщика MSI под системной учетной записью (SYSTEM) обычно выполняется при обновлении через службу обновлений "Лаборатории Касперского" или при развертывании инсталляционного пакета через Kaspersky Security Center.

Если вы обновляете Kaspersky Endpoint Security с помощью MSI-файла под учетной записью непривилегированного пользователя, у Kaspersky Endpoint Security отсутствует доступ к действующим лицензиям решений "Лаборатории Касперского". При этом Kaspersky Endpoint Security автоматически выбирает компоненты на основании состава компонентов Kaspersky Endpoint Agent. Далее Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent.

Kaspersky Endpoint Security поддерживает обновление без перезагрузки компьютера. Вы можете выбрать режим обновления приложения в параметрах политики.

5. **Проверка работы приложения**

Если после установки или обновления приложения компьютер имеет статус *Критический* в консоли Kaspersky Security Center, выполните следующие действия:

- Убедитесь, что на компьютере установлен Агент администрирования версии 13.2 или выше.

- Проверьте статус работы встроенного агента с помощью отчета *Отчет о статусе компонентов приложения*. Если компонент имеет статус *Не установлен*, установите компонент с помощью задачи *Изменение состава компонентов приложения*. Если компонент имеет статус *Не поддерживается лицензией*, убедитесь, что вы активировали функцию встроенного агента.

- Убедитесь, что вы приняли условия Положения о Kaspersky Security Network в новой политике Kaspersky Endpoint Security для Windows.

6. **Проверка подключения к серверу Kaspersky Anti Targeted Attack Platform**

Проверьте подключение к серверу Kaspersky Anti Targeted Attack Platform. Для этого выполните следующие действия:

1. Проверьте наличие действительного сертификата.
2. Проверьте параметры подключения к серверу.
3. Проверьте журнал событий.

   Если подключение к серверу установлено, приложение отправляет событие *Успешное подключение к серверу EDR Expert*. Если события об успешном подключении нет, а также отсутствуют события с ошибками подключения, проверьте параметры журналов событий и включите отправку событий для Endpoint Detection and Response (KATA).

Статус подключения к серверу не влияет на статус компьютера в консоли Kaspersky Security Center. То есть, если подключение к серверу отсутствует, компьютер может иметь статус *OK*. Для проверки подключения к серверу проверьте журнал событий.

7 Проверка производительности

Если после установки или обновления приложения производительность компьютера снизилась, вы можете оптимизировать передачу данных. Для этого выполните следующие действия:

1. Выключите компонент EDR (KATA) и убедитесь, что снижение производительности происходит именно из-за EDR (KATA).
2. Для доверенных приложений выключите сбор телеметрии по операциям консольного ввода (по умолчанию включен).
3. Добавьте приложения, которые снижают производительность компьютера, в список доверенных приложений.
4. Обратитесь в Службу технической поддержки "Лаборатории Касперского". Специалисты помогут настроить фильтрацию телеметрии в Kaspersky Anti Targeted Attack Platform. Это уменьшит расход трафика. Если на производительность компьютера влияет определенное приложение, прикрепите дистрибутив этого приложения к обращению.

Kaspersky Sandbox



В Kaspersky Endpoint Security для Windows включен встроенный агент для интеграции с решением Kaspersky Sandbox. *Sandbox* обнаруживает и автоматически блокирует сложные угрозы на компьютерах. Sandbox анализирует поведение объектов для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации. Sandbox выполняет анализ и проверку объектов на специальных серверах с развернутыми виртуальными образами операционных систем Microsoft Windows (серверы Sandbox). Подробнее о решении см. в справке Kaspersky Sandbox и справке Kaspersky Anti Targeted Attack Platform.

Интеграция встроенного агента с Kaspersky Sandbox

Для интеграции с Kaspersky Sandbox вам нужно добавить компонент Sandbox. Вы можете выбрать компонент Sandbox во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

Для работы компонента должны быть выполнены следующие условия:

- Kaspersky Security Center версии 13.2. В более ранних версиях Kaspersky Security Center недоступно создание автономных задач поиска IOC при реагировании на угрозы.
- Управление компонентом доступно только в Web Console. Управлять компонентом в Консоли администрирования (MMC) невозможно.
- Приложение активировано и функциональность входит в лицензию.
- Передача данных на Сервер администрирования включена.

  Для работы всех функций Kaspersky Sandbox должна быть включена передача данных о файлах карантина. Данные нужны для получения информации о помещенных на компьютере файлах на карантин в Web Console. В Web Console вы можете, например, загрузить файл из карантина на компьютер для анализа.

  Как включить передачу данных на Сервер администрирования в Web Console

  1. В главном окне Web Console выберите **Управление активами** → **Политики**.
  2. Нажмите на название политики Kaspersky Endpoint Security.

     Откроется окно свойств политики.
  3. Выберите вкладку **Параметры приложения**.
  4. Перейдите в раздел **Общие настройки** → **Интеграция с KSC**.
  5. В блоке **Передача данных на Сервер администрирования** установите флажок **О файлах карантина**.
  6. Сохраните внесенные изменения.
- Установлено фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования

  Для работы Kaspersky Sandbox с Сервером администрирования через Kaspersky Security Center Web Console вам нужно установить новое безопасное соединение – *фоновое соединение*. Подробнее об интеграции Kaspersky Security Center с другими решениями "Лаборатории Касперского" см. в справке Kaspersky Security Center.

  Как установить фоновое соединение в Web Console

  1. В главном окне Web Console выберите **Параметры** → **Интеграция**.
  2. Перейдите в раздел **Интеграция**.
  3. Включите переключатель **Фоновое соединение для интеграции Включено**.
  4. Сохраните внесенные изменения.

  Если фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования отсутствует, создание автономных задач поиска IOC при реагировании на угрозы недоступно.
- Для настройки доверенного соединения с сервером Sandbox вам нужно подготовить TLS-сертификат. Далее вам нужно добавить сертификат на компьютер с помощью политики. Также вам нужно добавить сертификат на сервер Sandbox.

Двусторонняя аутентификация с помощью криптоконтейнера для Kaspersky Sandbox недоступна.

Вы можете добавить TLS-сертификат в Web Console или локально из командной строки.

- Компонент Kaspersky Sandbox включен.
- Компоненты приложения, которые обеспечивают работу Sandbox, включены и работают. Работу Sandbox обеспечивают следующие компоненты:
  - Защита от файловых угроз.
  - Предотвращение вторжений.
  - Сетевой экран.
  - AMSI-защита.
  - Фоновая проверка.

Чтобы включить или выключить интеграцию с Kaspersky Sandbox, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Sandbox**.
5. Используйте переключатель **Интеграция с Sandbox ВКЛЮЧЕНА**, чтобы включить или выключить компонент.
6. В блоке **Режим интеграции** выберите режим работы компонента **Kaspersky Sandbox**.
7. Перейдите по ссылке **Настройки подключения**.

   Откроется окно с параметрами подключения к серверам Sandbox.
8. В блоке **TLS-сертификат сервера** нажмите на кнопку **Загрузить** и выберите файл TLS-сертификата.

   В Kaspersky Endpoint Security может быть только один TLS-сертификат сервера Sandbox. Если вы ранее уже добавили TLS-сертификат, то этот сертификат прекращает действовать. Только последний добавленный сертификат будет актуальным.

9. Настройте дополнительные параметры подключения к серверам Sandbox:

   - **Время ожидания (мсек.)**. Время ожидания соединения с сервером Sandbox. По истечению заданного времени ожидания Kaspersky Endpoint Security отправит запрос на следующий сервер. Вы можете увеличить время ожидания соединения с сервером, если у вас низкая скорость соединения или соединение нестабильно. Рекомендованное значение времени ожидания запроса не более 0,5 сек.

   - **Очередь запросов**. Размер папки хранения очереди запросов. При отправке нескольких объектов на проверку в Sandbox приложение Kaspersky Endpoint Security создает очередь запросов. По умолчанию размер папки хранения очереди запросов ограничен 100 МБ. После достижения максимального размера Sandbox перестает добавлять новые запросы в очередь и отправляет соответствующее событие в Kaspersky Security Center. Вы можете настроить размер папки хранения очереди запросов в зависимости от конфигурации сервера.

10. В блоке **Подключение к серверам Sandbox** нажмите на кнопку **Добавить**.

11. В открывшемся окне введите адрес сервера Sandbox (IPv4, IPv6, DNS), а также порт подключения к серверу.

    Подробнее о развертывании виртуальных образов и конфигурации серверов Sandbox см. в справке Kaspersky Sandbox.

12. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security проверит TLS-сертификат. Если сертификат прошел проверку, Kaspersky Endpoint Security отправит файл сертификата на компьютер при следующей синхронизации с Kaspersky Security Center. Если вы добавили два TLS-сертификата, Kaspersky Sandbox использует последний сертификат для установки доверенного соединения. Проверьте статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Sandbox**.

Вы можете включать и выключать интеграцию с Kaspersky Sandbox в Web Console или локально из командной строки.

Kaspersky Endpoint Security сохраняет информацию о работе компонента Kaspersky Sandbox в отчет. Отчет также содержит информацию об ошибках. Если вы получили ошибку с описанием в формате `Error code: XXX` (например, `0xa67b01f4`), вам нужно обратиться в Службу технической поддержки.

Поиск индикаторов компрометации (автономная задача)

Индикатор компрометации (Indicator of Compromise, IOC) – набор данных об объекте или активности, который указывает на несанкционированный доступ к компьютеру (компрометация данных). Например, индикатором компрометации может быть большое количество неудачных попыток входа в систему. Задача *Поиск IOC* позволяет обнаруживать индикаторы компрометации на компьютере и выполнять действия по реагированию на угрозы.

Для поиска индикаторов компрометации Kaspersky Endpoint Security использует IOC-файлы. *IOC-файлы* – файлы, содержащие набор индикаторов, при совпадении с которыми приложение считает событие обнаружением. IOC-файлы должны соответствовать стандарту описания OpenIOC. Kaspersky Endpoint Security автоматические формирует IOC-файлы для работы Kaspersky Sandbox.

Режим запуска задачи Поиск IOC

Для работы Kaspersky Sandbox приложение создает автономные задачи поиска IOC. *Автономная задача поиска IOC* – групповая задача, которая создается автоматически при реагировании на угрозу, обнаруженную Kaspersky Sandbox. Kaspersky Endpoint Security автоматически формирует IOC-файл. Работа пользователя с IOC-файлами не предусмотрена. Задачи автоматически удаляются через 30 дней с момента создания. Подробнее об автономных задачах поиска IOC см. в справке Kaspersky Sandbox.

Настройка задачи Поиск IOC

При реагировании на угрозы Kaspersky Sandbox автоматически создает и запускает задачи *Поиск IOC*.

Вы можете настроить параметры задачи только в Web Console.

Для работы с автономными задачами поиска IOC требуется Kaspersky Security Center версии 13.2.

Чтобы изменить параметры задачи Поиск IOC, выполните следующие действия:

1. В главном окне Web Console выберите **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Поиск IOC**.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Настройки поиска IOC**.

5. Настройте действия при обнаружении индикатора компрометации:

- **Копию поместить на карантин, объект удалить**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удаляет вредоносный объект, обнаруженный на компьютере. Перед удалением объекта Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин.

- **Запустить проверку важных областей**. Если выбран этот вариант действия, то Kaspersky Endpoint Security запускает задачу *Проверка важных областей*. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

- **Выполнять только во время простоя компьютера**. Отложенный запуск задачи, если ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка. Если вы прервали выполнение задачи и, например, разблокировали компьютер, Kaspersky Endpoint Security запустит задачу автоматически с того же места, где проверка была прервана. Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.

6. Сохраните внесенные изменения.

Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты**. Информацию об обнаруженных индикаторах компрометации вы можете посмотреть в свойствах задачи **Параметры приложения → Результаты поиска IOC**.

Срок хранения результатов поиска IOC составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет старые записи.

Руководство по миграции с KEA на KES для Kaspersky Sandbox

В Kaspersky Endpoint Security для Windows включен встроенный агент для работы решения Kaspersky Sandbox. Теперь вам не нужно отдельное приложение Kaspersky Endpoint Agent для работы Kaspersky Sandbox. Все функции Kaspersky Endpoint Agent будет выполнять Kaspersky Endpoint Security.

При развертывании Kaspersky Endpoint Security на компьютеры с установленным приложением Kaspersky Endpoint Agent решение Kaspersky Sandbox продолжит работу с Kaspersky Endpoint Security. Также приложение Kaspersky Endpoint Agent будет удалено с компьютера. Такое же поведение в системе будет при обновлении Kaspersky Endpoint Security до версии 11.7.0 или выше.

Kaspersky Endpoint Security несовместим с Kaspersky Endpoint Agent. Установить оба этих приложения на одном компьютере невозможно.

Для работы Kaspersky Endpoint Security в составе Kaspersky Sandbox должны быть выполнены следующие условия:

- Kaspersky Sandbox версии 2.0 или выше.

- Kaspersky Security Center версии 13.2 или выше (включая Агент администрирования). В более ранних версиях Kaspersky Security Center невозможно активировать функциональность Kaspersky Sandbox.

- Управление Kaspersky Sandbox доступно только в Kaspersky Security Center Web Console.

- Передача данных на Сервер администрирования включена. Данные нужны для получения информации о помещенных на компьютере файлах на карантин в Web Console.
- Установлено фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования. Для работы Kaspersky Sandbox с Сервером администрирования через Kaspersky Security Center Web Console вам нужно установить новое безопасное соединение – *фоновое соединение*.

Этапы миграции конфигурации [KES+KEA] на [KES+встроенный агент] для Kaspersky Sandbox

1. **Обновление веб-плагина Kaspersky Endpoint Security**

   Управление компонентом Kaspersky Sandbox доступно с помощью веб-плагина Kaspersky Endpoint Security версии 11.7.0 или выше.

2. **Миграция политик и задач**

   Перенесите параметры работы Kaspersky Endpoint Agent в приложение Kaspersky Endpoint Security для Windows. Для этого в Web Console предназначен Мастер миграции с Kaspersky Endpoint Agent.

   Как перенести параметры политик и задач с помощью Мастера миграции с Kaspersky Endpoint Agent в Web Console

   В главном окне Web Console выберите **Операции** → **Миграция с Kaspersky Endpoint Agent**.

   В результате запустится мастер миграции политик и задач. Следуйте его указаниям.

   Шаг 1. Миграция политик

   Мастер миграции создает новую политику, в которой будут объединены параметры политик Kaspersky Endpoint Security и Kaspersky Endpoint Agent. В списке политик выберите политики Kaspersky Endpoint Agent, параметры которых вы хотите объединить с политикой Kaspersky Endpoint Security. Нажмите на политику Kaspersky Endpoint Agent, чтобы выбрать политику Kaspersky Endpoint Security, с которой вы хотите объединить параметры. Убедитесь, что политики выбраны верно и перейдите к следующем шагу.

   Шаг 2. Миграция задач

   Мастер миграции создает новые задачи для Kaspersky Endpoint Security. В списке задач выберите задачи Kaspersky Endpoint Agent, которые вы хотите создать для Kaspersky Endpoint Security. Перейдите к следующему шагу.

   Шаг 3. Завершение работы мастера

   Завершите работу мастера. В результате работы мастера будут выполнены следующие действия:

   - Создана новая политика Kaspersky Endpoint Security.

В политике объединены параметры Kaspersky Endpoint Security и Kaspersky Endpoint Agent. Политика называется *<Название политики Kaspersky Endpoint Security> & <Название политики Kaspersky Endpoint Agent>*. Новая политика имеет статус *Неактивна*. Для продолжения работы измените статусы политик Kaspersky Endpoint Agent и Kaspersky Endpoint Security на *Неактивна* и активируйте новую объединенную политику.

После миграции из Kaspersky Endpoint Agent на Kaspersky Endpoint Security для Windows убедитесь, что в новой политике настроены функции передачи данных на Сервер администрирования: данные о файлах карантина и данные о цепочке развития угрозы. Значения параметров передачи данных не мигрируют из политики Kaspersky Endpoint Agent.

- Созданы новые задачи Kaspersky Endpoint Security.

  Новые задачи представляют собой копии задач Kaspersky Endpoint Agent. При этом мастер оставляет задачи Kaspersky Endpoint Agent без изменений.

3 Лицензирование функции Kaspersky Sandbox

Для активации Kaspersky Endpoint Security в составе решения Kaspersky Sandbox вам потребуется отдельная лицензия Kaspersky Sandbox Add-on. Вы можете добавить ключ с помощью задачи *Добавление ключа*. Таким образом, в приложение будет добавлено два ключа: *Kaspersky Endpoint Security* и *Kaspersky Sandbox*.

4 Установка / Обновление версии приложения Kaspersky Endpoint Security

Для миграции функций Kaspersky Sandbox во время установки или обновления приложения рекомендуется использовать задачу удаленной установки. При создании задачи удаленной установки вам нужно выбрать компонент Kaspersky Sandbox в параметрах инсталляционного пакета.

Также вы можете обновить приложение следующими способами:

- Через службу обновлений "Лаборатории Касперского".
- Локально с помощью мастера установки.

Kaspersky Endpoint Security поддерживает автоматический выбор компонентов при обновлении приложения на компьютере с установленным приложением Kaspersky Endpoint Agent. Автоматический выбор компонентов зависит от прав учетной записи пользователя, который обновляет приложение.

Если вы обновляете Kaspersky Endpoint Security с помощью EXE-файла или с помощью MSI-файла под системной учетной записью (SYSTEM), Kaspersky Endpoint Security получает доступ к действующим лицензиям решений "Лаборатории Касперского". Таким образом, если на компьютере, например, установлено приложение Kaspersky Endpoint Agent и активировано решение Kaspersky Sandbox, установщик Kaspersky Endpoint Security автоматически сконфигурирует набор компонентов и выберет компонент Kaspersky Sandbox. При этом Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent. Запуск установщика MSI под системной учетной записью (SYSTEM) обычно выполняется при обновлении через службу обновлений "Лаборатории Касперского" или при развертывании инсталляционного пакета через Kaspersky Security Center.

Если вы обновляете Kaspersky Endpoint Security с помощью MSI-файла под учетной записью непривилегированного пользователя, у Kaspersky Endpoint Security отсутствует доступ к действующим лицензиям решений "Лаборатории Касперского". При этом Kaspersky Endpoint Security автоматически выбирает компоненты на основании конфигурации Kaspersky Endpoint Agent. Далее Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent.

Kaspersky Endpoint Security поддерживает обновление без перезагрузки компьютера. Вы можете выбрать режим обновления приложения в параметрах политики.

5. **Проверка работы приложения**

   Если после установки или обновления приложения компьютер имеет статус *Критический* в консоли Kaspersky Security Center, выполните следующие действия:

   - Убедитесь, что на компьютере установлен Агент администрирования версии 13.2 или выше.
   - Проверьте статус работы встроенного агента с помощью отчета *Отчет о статусе компонентов приложения*. Если компонент имеет статус *Не установлен*, установите компонент с помощью задачи *Изменение состава компонентов приложения*. Если компонент имеет статус *Не поддерживается лицензией*, убедитесь, что вы активировали функцию встроенного агента.
   - Убедитесь, что вы приняли условия Положения о Kaspersky Security Network в новой политике Kaspersky Endpoint Security для Windows.

Работа с карантином

Карантин – это специальное локальное хранилище на компьютере. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства. Kaspersky Endpoint Security использует карантин только при работе с решениями Detection and Response от "Лаборатории Касперского". В остальных случаях Kaspersky Endpoint Security помещает файл в резервное хранилище. Подробнее о работе с карантином в составе решений см. в справке Kaspersky Sandbox, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Endpoint Detection and Response Expert, Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Detection and Response Expert (on-premises).

Kaspersky Endpoint Security помещает файлы на карантин под системной учетной записью (SYSTEM).

Вы можете настроить параметры карантина только в консоли Kaspersky Security Center. Также в консоли Kaspersky Security Center вы можете выполнить действия с объектами на карантине (восстановить, удалить, добавить и другие). Локально на компьютере вы можете только восстановить объект из командной строки.

Настройка максимального размера карантина

По умолчанию размер карантина ограничен 1024 МБ. После достижения максимального размера Kaspersky Endpoint Security прекращает отправлять файлы и формирует событие *Недостаточно места в хранилище карантина*. Чтобы не допустить переполнение карантина вы можете задать пороговое значение, при котором Kaspersky Endpoint Security будет формировать событие *В хранилище карантина скоро закончится место*. Настроить срок хранения файлов в карантине для автоматического удаления файлов невозможно.

Если в вашей организации развернуто решение Kaspersky Anti Targeted Attack Platform (EDR), мы рекомендуем увеличить размер карантина. При сканировании YARA приложение может обнаружить дамп памяти большого размера. Если размер дампа памяти превышает размер карантина, приложение завершит сканирование YARA с ошибкой и дамп памяти не будет помещен на карантин. Мы рекомендуем задать размер карантина равным размеру оперативной памяти компьютера (например, 8 ГБ) или выключить ограничение размера карантина.

Как настроить максимальный размер карантина в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки → Отчеты и хранилище**.
4. В блоке **Карантин** настройте размер карантина:

   - **Ограничить размер карантина до N МБ**. Если флажок установлен, то максимальный размер карантина ограничен заданным значением. По умолчанию максимальный размер составляет 1024 МБ. При достижении максимального размера карантина Kaspersky Endpoint Security отправляет событие в Kaspersky Security Center *Недостаточно места в хранилище карантина* и публикует событие в Журнале событий Windows. При этом приложение прекращает помещать новые объекты на карантин. Вам нужно вручную очистить карантин.

     Если флажок снят, размер карантина ограничен размером свободного пространства на диске.

   - **Уведомлять при заполнении карантина на N процентов**. Пороговое значение карантина. Например, вы можете задать пороговое значение карантина 50 %. При достижении порогового значения карантина, Kaspersky Endpoint Security отправляет соответствующее событие в Kaspersky Security Center и публикует событие в Журнале событий Windows. При этом приложение продолжает помещать новые объекты на карантин.

     Если флажок снят, приложение не формирует события при достижении порогового значения карантина.

5. Сохраните внесенные изменения.

Как настроить максимальный размер карантина в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки → Отчеты и хранилище**.

5. В блоке **Карантин** настройте размер карантина:

   - **Ограничить размер карантина**. Если флажок установлен, то размер карантина ограничен указанным значением. Если флажок снят, размер карантина ограничен свободным пространством на диске. Это может понадобится при YARA-проверке, так как приложение может сохранять дамп памяти большого размера.

   - **Максимальный размер карантина (МБ)**. Если флажок установлен, то максимальный размер карантина ограничен заданным значением. По умолчанию максимальный размер составляет 1024 МБ. При достижении максимального размера карантина Kaspersky Endpoint Security отправляет событие в Kaspersky Security Center *Недостаточно места в хранилище карантина* и публикует событие в Журнале событий Windows. При этом приложение прекращает помещать новые объекты на карантин. Вам нужно вручную очистить карантин.

     Если флажок снят, размер карантина ограничен размером свободного пространства на диске.

   - **Уведомлять при заполнении карантина на (%)**. Пороговое значение карантина. Например, вы можете задать пороговое значение карантина 50 %. При достижении порогового значения карантина, Kaspersky Endpoint Security отправляет соответствующее событие в Kaspersky Security Center и публикует событие в Журнале событий Windows. При этом приложение продолжает помещать новые объекты на карантин.

6. Сохраните внесенные изменения.

Передача данных о файлах на карантине в Kaspersky Security Center

Для выполнения действий с объектами на карантине в Web Console вам нужно включить передачу данных на Сервер администрирования о файлах на карантине. В Web Console вы можете, например, загрузить файл из карантина на компьютер для анализа. Передача данных о файлах на карантине должна быть включена для работы всех функций решений Kaspersky Sandbox и Kaspersky Endpoint Detection and Response.

Как включить передачу данных о файлах на карантине в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки → Отчеты и хранилище**.
4. В блоке **Передача данных на Сервер администрирования** нажмите на кнопку **Настройка**.
5. В открывшемся окне установите флажок **Файлы карантина**.
6. Сохраните внесенные изменения.

Как включить передачу данных о файлах на карантине в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки** → **Интеграция с KSC**.

5. В блоке **Передача данных на Сервер администрирования** установите флажок **О файлах карантина**.

6. Сохраните внесенные изменения.

В результате вы можете в консоли Kaspersky Security Center просматривать список файлов, помещенных на карантин на компьютере. В консоли Kaspersky Security Center вы можете выполнить действия с объектами на карантине (восстановить, удалить, добавить и другие). Подробнее о работе с карантином см. в справке Kaspersky Security Center.

Восстановление файлов из карантина

По умолчанию Kaspersky Endpoint Security восстанавливает файл в папку его исходного размещения. Если папка назначения удалена или у пользователя нет прав доступа к этой папке, приложение помещает файл в папку `%DataRoot%\QB\Restored`. Далее вам нужно вручную переместить файл в папку назначения.

Чтобы восстановить файлы из карантина, выполните следующие действия:

1. В главном окне Web Console выберите **Операции** → **Хранилища** → **Карантин**.

2. В открывшемся списке файлов карантина выберите файлы, которые вы хотите восстановить, и нажмите на кнопку **Восстановить**.

   Kaspersky Endpoint Security восстановит файл. Если в папке восстановление уже есть файл с таким же именем, приложение отменит восстановление файла. После восстановления файла приложение сохраняет копию файла на карантине. Для удаления файла вам нужно очистить карантин вручную.

Реагирование на IOA

IOA-правила (правила для индикаторов атак) позволяют выявлять подозрительные события в инфраструктуре организации и автоматически создавать алерты. Если активность на устройстве соответствует IOA-правилу, Kaspersky Endpoint Security автоматически выполняет предустановленное действие по реагированию.

Kaspersky Endpoint Security поддерживает IOA-правила для следующих EDR-решений:

- Kaspersky EDR Expert (on-premises);
- Kaspersky EDR Expert (cloud).

IOA-правила создают специалисты "Лаборатории Касперского" на базе экспертизы по целевым атакам (threat intelligence). Такие правила описывают подозрительную активность в системе, которая может быть признаком целевой атаки, и обычно привязаны к техникам MITRE. Kaspersky Endpoint Security получает правила автоматически после загрузки обновлений на Сервер администрирования Для этого запустите задачу Kaspersky Security Center *Загрузка обновлений в хранилище Сервера администрирования*.

Для формирования IOA-правил Kaspersky Endpoint Security отправляет телеметрию в EDR-решение. Kaspersky Endpoint Security позволяет настроить отправку телеметрии для IOA, а также добавить исключения для отдельных IOA-правил.

Управление IOA-правилами осуществляется в консоли OSMP. В политике Kaspersky Endpoint Security вы можете выполнять следующие действия:

- включать и выключать IOA-правило;
- включать и выключать действие по реагированию для IOA-правила;
- отслеживать действия, которые были выполнены при срабатывании IOA-правил.

Чтобы настроить работу IOA-правила, выполните следующие действия:

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Реагирование на IOA**.
   Откроется список IOA-правил "Лаборатории Касперского".
5. С помощью переключателя включите или выключите IOA-правило.
6. Для настройки действия по реагированию для IOA-правила:
   a. Выберите IOA-правило.
      Откроется список действия по реагированию для IOA-правила.
   b. Выберите действия по реагированию.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Мониторинг EDR-действий

В Kaspersky Endpoint Security для Windows версии 12.9 добавлен единый центр мониторинга EDR-действий. *Единый центр мониторинга EDR-действий* – это консоль, в которой представлена история реагирования на угрозы от всех решений Detection and Response от "Лаборатории Касперского". Если в вашей организации развернуто несколько решений Detection and Response (например, EDR Optimum и MDR), то Kaspersky Endpoint Security покажет историю реагирования на угрозы для всех решений. Таким образом, вы сможете проанализировать работу решений Detection and Response на отдельном компьютере и оптимизировать параметры этих решений.

Центр мониторинга предоставляет следующие данные:

- информация о задачах по реагированию на угрозы (например, задача *Завершение процесса*);
- изменения правил компонентов Сетевой изоляции и Запрета запуска объектов.

Если в процессе реагирования на угрозу возникает ошибка, связанная с доступом к сетевой папке, такая ошибка не будет отображаться в истории реагирования на угрозы.

Чтобы открыть Единый центр мониторинга EDR-действий, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите вкладку **Приложения**.
4. Нажмите на **Kaspersky Endpoint Security для Windows 14.2**.

   Откроются локальные параметры приложения.
5. Выберите вкладку **Параметры приложения**.
6. Перейдите в раздел **Встроенные агенты** → **История реагирования**.

Откроется консоль Единого центра мониторинга EDR-действий. В консоли вы можете просмотреть статус задач по реагированию на угрозы, время выполнения этих задач, изменения в правилах, а также данные об инициаторе.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security для Windows поддерживает работу с решением Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* – решение класса SIEM для управления информацией о безопасности и событиями безопасности в ИТ-инфраструктуре организации. KUMA позволяет обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб организации.

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Unified Monitoring and Analysis Platform (KUMA). KUMA показывает события в своей консоли в виде списка без разметки, как в журнале событий Windows.

Kaspersky Endpoint Security не выполняет все функции агента для KUMA. Приложение только отправляет в KUMA события без разметки. Для доступа ко всем функциям KUMA вам нужно приобрести лицензию на решение и развернуть решение в соответствии с Руководством администратора KUMA.

Интеграция Kaspersky Endpoint Security с KUMA

Интеграция KES с KUMA состоит из следующих шагов:

1. В консоли KUMA добавьте коллектор.
2. В консоли KUMA настройте коннектор для коллектора, чтобы получать события от KES.
3. В консоли KUMA включите использование двусторонней аутентификации (не обязательно).

4. В политике Kaspersky Endpoint Security для Windows настройте параметры подключения KES к KUMA.

5. В консоли KUMA убедитесь, что события от KES поступают в нужный тенант и обрабатываются нужными правилами корреляции.

Подготовка к интеграции KES с KUMA

Для работы KUMA должны быть выполнены следующие условия:

- Kaspersky Security Center версии 14.2 или выше. В более ранних версиях Kaspersky Security Center невозможно активировать функциональность интеграции с KUMA.
- Приложение активировано и функциональность входит в лицензию.
- Компонент интеграции с KUMA включен.

Подготовка к интеграции KES с KUMA состоит из следующих этапов:

1. **Установка компонента для интеграции с KUMA**

   Вы можете выбрать компонент для интеграции с KUMA во время установки или обновления приложения, а также с помощью задачи *Изменение состава компонентов приложения*.

   Для завершения обновления приложения с новым компонентом нужно перезагрузить компьютер.

2. **Активация KUMA**

   Кроме лицензии на приложение Kaspersky Endpoint Security (например, Kaspersky Endpoint Security для бизнеса Стандартный) вам потребуется отдельная лицензия для интеграции Kaspersky Endpoint Security с KUMA (Kaspersky Endpoint Security для Windows KUMA Integration Add-on).

   Функциональность будет доступна после добавления отдельного ключа KUMA. В результате на компьютере будет еще один активный ключ для интеграции Kaspersky Endpoint Security с KUMA.

   Лицензирование отдельной функциональности KUMA не отличается от лицензирования Kaspersky Endpoint Security.

   Убедитесь, что функциональность KUMA включена в лицензию и работает в локальном интерфейсе приложения.

Подключение KES к KUMA

Для подключения компьютера с установленным приложением Kaspersky Endpoint Security к решению KUMA вам нужно выполнить следующие действия:

1. В консоли KUMA добавьте коллектор с коннекторами типа **tcp**, **udp** или **http** и настройте сетевые параметры подключения. Подробнее о работе с коннекторами см. в справке Kaspersky Unified Monitoring and Analysis Platform.

2. В политике Kaspersky Endpoint Security добавьте адреса коллекторов KUMA и настройте сетевые параметры подключения.

Как подключить компьютер с Kaspersky Endpoint Security к KUMA в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Интеграция с KUMA**.
5. Установите флажок **Интеграция с KUMA**.
6. В блоке **Настройки интеграции** установите флажок **Включить отправку событий Windows на сервер KUMA**.
7. Добавьте серверы KUMA:

   a. Нажмите на кнопку **Добавить**.

   Откроется форма добавления сервера KUMA.

   b. Выберите протокол для подключения к серверу KUMA:

   - **TCP** – отправка необработанного потока данных о событиях по протоколу TCP.
   - **TCP / TLS** – отправка необработанного потока данных о событиях с использованием шифрования TLS.
   - **UDP** – отправка данных о событиях в формате UDP-пакетов.
   - **HTTP / HTTPS** – отправка данных о событиях в формате HTTP-сообщений по протоколу TCP. Для HTTPS используется TLS-шифрование.

   Протокол для подключения к коллектору в Kaspersky Endpoint Security должен соответствовать типу коннектора в KUMA: **http**, **tcp** или **udp**.

   > При выборе протокола UDP могут быть потери данных из-за потерь трафика в силу особенности протокола.

   c. Введите адрес сервера (IPv4, IPv6, FQDN), а также порт подключения к серверу (по умолчанию 443).

   При вводе адреса сервера учитывайте следующие особенности:

   - **TCP**. Вы можете указывать как IP-адрес, так и FQDN-имя сервера.
   - **TCP / TLS**. Необходимо указывать только FQDN-имя сервера.
   - **UDP**. Протокол UDP не поддерживает шифрование TLS. Вы можете указывать как IP-адрес, так и FQDN-имя сервера.
   - **HTTP / HTTPS**. Вам необходимо вручную указать протокол (HTTP или HTTPS) в адресе сервера (например, `https://server.com` или `http://10.10.10.100`).

   Вы можете посмотреть адрес сервера в свойствах коннектора в консоли KUMA. Подробнее о коннекторах KUMA см. в справке Kaspersky Unified Monitoring and Analysis Platform.

d. При использовании протоколов TCP или TCP/TLS, вы можете настроить метод сжатия передаваемых данных:

- **Выключено** – отправка данных без сжатия;
- **GZIP** – сжатие передаваемых данных с использованием метода GZIP.

> Сжатие телеметрии для протоколов TCP и TCP/TLS доступно для Kaspersky Endpoint Security версии 14.3 и выше. Для более ранних версий приложения мы рекомендуем также настроить подключение к данном серверу с использованием протокола HTTPS, так как некоторые данные телеметрии могут быть потеряны.

e. Нажмите на кнопку **OK**.

Вы можете добавить несколько серверов. Kaspersky Endpoint Security подключается к первому серверу из списка. Если подключение не удалось выполнить, Kaspersky Endpoint Security подключается ко второму серверу и так далее по списку.

8. Если требуется, в блоке **Настройка передачи данных** настройте параметр **Максимальная задержка отправки событий (сек.)**. По истечении указанного времени Kaspersky Endpoint Security повторно пробует подключиться к тому же коллектору или подключается к следующему в списке коллектору, если их несколько. По умолчанию установлено значение 30 секунд.

9. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как подключить компьютер с Kaspersky Endpoint Security к KUMA в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты → Интеграция с KUMA**.
5. Включите переключатель **Интеграция с KUMA ВКЛЮЧЕНА**.
6. Выберите вкладку **События Windows**.
7. Добавьте серверы KUMA:

   a. Нажмите на кнопку **Добавить**.

   Откроется форма добавления сервера KUMA.

   b. Выберите протокол для подключения к серверу KUMA:

   - **TCP** – отправка необработанного потока данных о событиях по протоколу TCP.
   - **TCP / TLS** – отправка необработанного потока данных о событиях с использованием шифрования TLS.

- **UDP** – отправка данных о событиях в формате UDP-пакетов.
- **HTTP/HTTPS** – отправка данных о событиях в формате HTTP-сообщений по протоколу TCP. Для HTTPS используется TLS-шифрование.

Протокол для подключения к коллектору в Kaspersky Endpoint Security должен соответствовать типу коннектора в KUMA: **http**, **tcp** или **udp**.

> При выборе протокола UDP могут быть потери данных из-за потерь трафика в силу особенности протокола.

c. Введите адрес сервера (IPv4, IPv6, FQDN), а также порт подключения к серверу (по умолчанию 443).

При вводе адреса сервера учитывайте следующие особенности:

- **TCP**. Вы можете указывать как IP-адрес, так и FQDN-имя сервера.
- **TCP / TLS**. Необходимо указывать только FQDN-имя сервера.
- **UDP**. Протокол UDP не поддерживает шифрование TLS. Вы можете указывать как IP-адрес, так и FQDN-имя сервера.
- **HTTP/HTTPS**. Вам необходимо вручную указать протокол (HTTP или HTTPS) в адресе сервера (например, `https://server.com` или `http://10.10.10.100`).

Вы можете посмотреть адрес сервера в свойствах коннектора в консоли KUMA. Подробнее о коннекторах KUMA см. в справке Kaspersky Unified Monitoring and Analysis Platform.

d. При использовании протоколов TCP или TCP/TLS, вы можете настроить метод сжатия передаваемых данных:

- **Выключено** – отправка данных без сжатия;
- **GZIP** – сжатие передаваемых данных с использованием метода GZIP.

> Сжатие телеметрии для протоколов TCP и TCP/TLS доступно для Kaspersky Endpoint Security версии 14.3 и выше. Для более ранних версий приложения мы рекомендуем также настроить подключение к данном серверу с использованием протокола HTTPS, так как некоторые данные телеметрии могут быть потеряны.

e. Нажмите на кнопку **OK**.

Вы можете добавить несколько серверов. Kaspersky Endpoint Security подключается к первому серверу из списка. Если подключение не удалось выполнить, Kaspersky Endpoint Security подключается ко второму серверу и так далее по списку.

8. Если требуется, в блоке **Настройки подключения к серверам** настройте параметр **Максимальная задержка отправки событий (сек.)**. По истечении указанного времени Kaspersky Endpoint Security повторно пробует подключиться к тому же коллектору или подключается к следующему в списке коллектору, если их несколько. По умолчанию установлено значение 30 секунд.
9. Сохраните внесенные изменения.

Вы можете проверить, что настройка интеграции с KUMA выполнена правильно, в консоли KUMA (см. в справке Kaspersky Unified Monitoring and Analysis Platform). Проверьте статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения* в консоли Kaspersky Security Center. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Интеграция с KUMA**.

Установка доверенного соединения между KES и KUMA

Вы можете установить доверенное соединение между Kaspersky Endpoint Security и коллектором KUMA с коннектором типа tcp или http. Установить доверенное соединение с коннектором типа udp невозможно.

Для установки доверенного соединения вам нужно настроить режим TLS в параметрах коннектора. Предусмотрены следующие режимы TLS:

- **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию.
- **Включено** – использовать шифрование TLS, но без верификации сертификатов.
- **Нестандартный PFX с аутентификацией клиента** – использовать шифрование TLS с PFX-секретом. В этом режиме выполняется аутентификация клиента по сертификату. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации.

Kaspersky Endpoint Security не поддерживает режим TLS коннектора **Нестандартный PFX**. При интеграции KES с KUMA с PFX обязательна аутентификация пользователя по паролю.

Для настройки доверенного соединения вам нужен TLS-сертификат – *CA-сертификат микросервиса*. Вы можете получить TLS-сертификат в консоли KUMA. Подробнее о загрузке TLS-сертификата см. справке Kaspersky Unified Monitoring and Analysis Platform. Далее вам нужно добавить TLS-сертификат в Kaspersky Endpoint Security (см. инструкцию ниже).

Чтобы сделать соединение более безопасным, вы можете включить дополнительную проверку компьютера в KUMA (двусторонняя аутентификация). Для включения такой проверки вам нужно сформировать криптоконтейнер во внешнем центре сертификации. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом в формате PKCS#12. Далее вам нужно включить двустороннюю аутентификацию в параметрах KUMA (режим TLS **Нестандартный PFX с аутентификацией клиента**), включить двустороннюю аутентификацию в Kaspersky Endpoint Security и добавить PFX-архив в консоли KUMA и в Kaspersky Endpoint Security.

Как настроить доверенное соединение между KES и KUMA в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Интеграция с KUMA**.
5. Установите флажок **Интеграция с KUMA**.

6. В блоке **Настройки подключения к серверам KUMA** установите флажок **Использовать шифрование TLS**.

7. Настройте доверенное соединение:

   a. Нажмите на кнопку **Настройки подключения к серверам KUMA**.

   b. Настройте параметры подключения к серверам:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера KUMA (по умолчанию 5 сек.). По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу KUMA.

   - **TLS-сертификат сервера**. TLS-сертификат предназначен для установки доверенного соединения с сервером KUMA. Вы можете получить TLS-сертификат в консоли Kaspersky Unified Monitoring and Analysis Platform (см. инструкцию в справке Kaspersky Unified Monitoring and Analysis Platform).

     Для установки доверенного соединения вам нужно в консоли KUMA в свойствах коннектора выбрать режим TLS **Включено**.

   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между KES и KUMA. Для использования двусторонней аутентификации вам нужно в консоли KUMA в параметрах коннектора выбрать режим TLS **Нестандартный PFX с аутентификацией клиента** (см. параметры коннектора в справке Kaspersky Unified Monitoring and Analysis Platform). Далее вам нужно загрузить сертификат сервера и установить пароль для защиты криптоконтейнера.

     > Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

   c. Нажмите на кнопку **OK**.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить доверенное соединение между KES и KUMA в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Встроенные агенты → Интеграция с KUMA**.

5. Включите переключатель **Интеграция с KUMA ВКЛЮЧЕНА**.

6. В блоке **Настройки подключения к серверам** включите переключатель **Использовать шифрование TLS**.

7. Настройте доверенное соединение:

   a. Нажмите на кнопку **Настройки подключения**.

   b. Настройте параметры подключения к серверам:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера KUMA (по умолчанию 5 сек.). По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу KUMA.
   - **TLS-сертификат сервера**. TLS-сертификат предназначен для установки доверенного соединения с сервером KUMA. Вы можете получить TLS-сертификат в консоли Kaspersky Unified Monitoring and Analysis Platform (см. инструкцию в справке Kaspersky Unified Monitoring and Analysis Platform).

     Для установки доверенного соединения вам нужно в консоли KUMA в свойствах коннектора выбрать режим TLS **Включено**.
   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между KES и KUMA. Для использования двусторонней аутентификации вам нужно в консоли KUMA в параметрах коннектора выбрать режим TLS **Нестандартный PFX с аутентификацией клиента** (см. параметры коннектора в справке Kaspersky Unified Monitoring and Analysis Platform). Далее вам нужно загрузить сертификат сервера и установить пароль для защиты криптоконтейнера.

     > Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

   c. Нажмите на кнопку **OK**.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Включение отправки телеметрии на Сервер KUMA

По умолчанию отправка событий на Сервер KUMA выключена. Для работы KUMA вам нужно включить отправку телеметрии. Для выбора источника событий доступны стандартные журналы: *Application*, *Security* или *System*.

Как включить отправку телеметрии в KUMA в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Общие настройки** → **Исключения и типы объектов**.
5. В блоке **Настройки телеметрии** → **Телеметрия KUMA** нажмите на кнопку **Настройка**.

6. Выберите журналы событий, которые вы хотите использовать в качестве источников событий: *Application*, *Security* или *System*.

   Кроме стандартных журналов вы можете указать журнал стороннего приложения.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как включить отправку телеметрии в KUMA в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки телеметрии**.
5. Выберите вкладку **Телеметрия KUMA**.
6. Выберите журналы событий, которые вы хотите использовать в качестве источников событий: *Application*, *Security* или *System*.

   Кроме стандартных журналов вы можете указать журнал стороннего приложения.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Добавление коннектора агентов KUMA

Коннекторы используются для получения событий от источников, чтобы в дальнейшем отправить эти события в KUMA. KUMA приводит эти события к общему виду, удобному для поиска корреляций, а также для хранения и ручного анализа.

Как добавить коннектор агентов KUMA в Web Console:

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Интеграция с KUMA**.
5. Выберите вкладку **Коннекторы агентов KUMA**.
6. Нажмите на кнопку **Добавить**.

   Откроется форма добавления коннектора агента KUMA.

7. Настройте параметры коннектора для выбранного типа:

   - **file**. Коннекторы с типом file используются для получения данных из текстовых файлов.
   - **tcp**. Коннекторы с типом tcp используются для пассивного получения событий по протоколу TCP.

- **udp**. Коннекторы с типом udp используются для пассивного получения событий по протоколу UDP.
- **http**. Коннекторы с типом http используются для получения событий по протоколу HTTP.
- **wec**. Коннекторы с типом wec используются для получения данных с помощью Windows Event Forwarding (WEF) и Windows Event Collector (WEC) или локальных журналов ОС компьютера.
- **etw**. Коннекторы с типом etw используются для получения расширенных журналов DNS-серверов.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Коннектор, тип file

Коннекторы с типом file используются для получения данных из текстовых файлов. Одна строка текстового файла считается одним событием. В качестве разделителя строк используется `\n`.

Параметры коннектора типа file

Параметр	Описание
Имя	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
Путь к файлу	Полный путь к файлу, с которым коннектор выполняет взаимодействие. Например, `C:\var\log\test123.log`. Недопустимо указывать пути, соответствующие следующим регулярным выражениям: • `(?i)^[a-zA-Z]:\\Program Files` • `(?i)^[a-zA-Z]:\\Program Files\(x86\)` • `(?i)^[a-zA-Z]:\\Windows` • `(?i)^[a-zA-Z]:\\ProgramData\\Kaspersky Lab\\KUMA` В приведенных регулярных выражениях двойные обратные косые черты (`\\`) используются системой в качестве части синтаксиса регулярного выражения для проверки пути и не должны указываться в самом пути вручную. Обязательный параметр.
Время ожидания изменений (сек.)	Время в секундах, в течение которого файл не должен обновляться, чтобы KUMA выполнила с ним действие, указанное в раскрывающемся списке **Действие после таймаута**. Значение по умолчанию: `0` – если файл не обновляется, KUMA не выполняет с ним никакого действия. Введенное значение не должно быть меньше значения, которое вы ввели на вкладке **Дополнительные параметры** в поле **Интервал запросов, мс**.
Действие после таймаута	Действие, которое KUMA выполняет с файлом по прошествии времени, указанного в поле **Время ожидания изменений, сек**: • **Ничего не делать**. Значение по умолчанию. • **Добавление суффикса** – добавить к названию файла расширение .kuma_processed и не обрабатывать файл даже при его обновлении. • **Удаление** – удалить файл.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Режим опроса файла/папки	Режим, в котором коннектор перечитывает файлы в директории: • **Отслеживать изменения** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, если файлы не обновляются. Значение по умолчанию. Например, если файлы постоянно обновляются, а в поле **Интервал запросов, мс** вы ввели `5000`, коннектор будет перечитывать файлы постоянно, а не с интервалом в 5000 миллисекунд. Если файлы не обновляются, коннектор будет перечитывать их с интервалом в 5000 миллисекунд. • **Отслеживать периодически** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, вне зависимости от того, обновляются файлы или нет.

Интервал запросов (мс)	Интервал в миллисекундах, с которым коннектор перечитывает файлы в директории. Значение по умолчанию: `0` – коннектор перечитывает файлы в директории каждые 700 миллисекунд. Вам нужно выбрать в раскрывающемся списке **Режим опроса файла/папки** режим, в котором коннектор перечитывает файлы в директории. Введенное значение не должно быть меньше значения, которое вы ввели в поле **Время ожидания изменений (сек.)**.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Точка назначения	*Точки назначения* задают сетевые параметры для передачи событий от источников в KUMA. Kaspersky Endpoint Security поддерживает передачу событий только по протоколу HTTP.

Коннектор, тип tcp

Коннекторы с типом tcp используются для пассивного получения событий по протоколу TCP.

Параметры коннектора типа tcp

Параметр	Описание
Имя	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `<FQDN>:<port>` • `<IP address>:<port>` • `:<port>` Обязательный параметр.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Режим TLS	Режим шифрования TLS. Доступные значения: • **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию. • **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации. • **Нестандартный PFX с аутентификацией клиента** – использовать шифрование TLS с PFX-секретом. В этом режиме выполняется аутентификация клиента по сертификату. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации.
Сжатие	Определяет метод распаковки данных, поступающих в коннектор. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
Точка назначения	*Точки назначения* задают сетевые параметры для передачи событий от источников в KUMA. Kaspersky Endpoint Security поддерживает передачу событий только по протоколу HTTP.

Коннектор, тип udp

Коннекторы с типом udp используются для пассивного получения событий по протоколу UDP.

Параметры коннектора типа udp

Параметр	Описание
Имя	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `<FQDN>:<port>` • `<IP address>:<port>` • `:<port>` Обязательный параметр.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Сжатие	Определяет метод распаковки данных, поступающих в коннектор. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
Точка назначения	*Точки назначения* задают сетевые параметры для передачи событий от источников в KUMA. Kaspersky Endpoint Security поддерживает передачу событий только по протоколу HTTP.

Коннектор, тип http

Коннекторы с типом http используются для получения событий по протоколу HTTP.

Параметры коннектора типа udp

Параметр	Описание
Имя	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `<FQDN>:<port>` • `<IP address>:<port>` • `:<port>` Обязательный параметр. Для того чтобы данные из источника событий отправлялись в коннектор, указанный вами URL-адрес должен оканчиваться на `/input`.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Режим TLS	Режим шифрования TLS. Доступные значения: • **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию. • **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации. • **Нестандартный PFX с аутентификацией клиента** – использовать шифрование TLS с PFX-секретом. В этом режиме выполняется аутентификация клиента по сертификату. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации.
Точка назначения	*Точки назначения* задают сетевые параметры для передачи событий от источников в KUMA. Kaspersky Endpoint Security поддерживает передачу событий только по протоколу HTTP.

Коннектор, тип wec

Коннекторы с типом wec используются для получения данных с помощью Windows Event Forwarding (WEF) и Windows Event Collector (WEC) или локальных журналов ОС компьютера.

Параметры коннектора типа wec

Параметр	Описание
Имя	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
Журналы Windows	Названия журналов Windows, которые требуется получить. По умолчанию в этом раскрывающемся списке отображаются только предварительно настроенные журналы, но вы можете расширить список пользовательскими журналами. Для этого введите название пользовательских журналов в поле **Журналы Windows**, после чего нажмите на клавишу **ENTER**. Конфигурация сервисов и ресурсов KUMA может потребовать дополнительных изменений для правильной обработки настраиваемых журналов. Преднастроенные журналы: • Application. • ForwardedEvents. • Security. • System. • HardwareEvents. Если неверно указать название хотя бы одного журнала, в этом случае агент, использующий коннектор, не будет получать события из всех журналов, даже если названия остальных журналов указаны верно. Обязательный параметр.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Точка назначения	*Точки назначения* задают сетевые параметры для передачи событий от источников в KUMA. Kaspersky Endpoint Security поддерживает передачу событий только по протоколу HTTP.

Коннектор, тип etw

Коннекторы с типом etw используются для получения расширенных журналов DNS-серверов.

Параметры коннектора типа etw

Параметр	Описание
Имя	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Имя сессии	Имя сессии, которое соответствует ETW-провайдеру Microsoft-Windows-DNSServer `{EB79061A-A566-4698-9119-3ED2807060E7}`. Если имя сессии указано неправильно, указан неправильный провайдер в сессии или указан неправильный режим отправки событий (для правильной отправки событий на стороне Windows Server должен быть указан режим Real time или File and Real time), от агента не будут поступать события, в журнале агента на Windows будет зарегистрирована ошибка, а статус агента будет зеленым. При этом попытки получить события каждые 60 сек не будет. Если вы изменяете параметры сессии на стороне Windows, вам нужно перезапустить агент и/или сессию, чтобы изменения были применены. Подробнее о настройке параметров сессии на стороне Windows для получения событий DNS-сервера, см. в справке Kaspersky Unified Monitoring and Analysis Platform. Обязательный параметр.
Извлекать информацию о событии	Извлечение минимального количества данных о событии, которое возможно без необходимости скачивать сторонние метаданные с диска. Такой способ позволяет сэкономить CPU на машине с агентом. По умолчанию этот переключатель включен и извлекаются все данные о событии.
Извлекать свойства события	Извлечение свойств событий. Если переключатель выключен, свойства события не будут извлечены и это позволит сэкономить CPU на машине с агентом. По умолчанию этот переключатель включен и свойства события извлекаются.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Точка назначения	*Точки назначения* задают сетевые параметры для передачи событий от источников в KUMA. Kaspersky Endpoint Security поддерживает передачу событий только по протоколу HTTP.

Добавление точки назначения

Точки назначения задают сетевые параметры для передачи событий от источников в KUMA. Kaspersky Endpoint Security поддерживает передачу событий только по протоколу HTTP.

Как добавить точку назначения в Web Console:

1. В главном окне Web Console выберите вкладку **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты → Интеграция с KUMA**.
5. Выберите вкладку **Точки назначения агентов KUMA**.
6. Нажмите на кнопку **Добавить**.

   Откроется форма добавления точки назначения агентов KUMA.
7. Введите имя точки назначения агентов KUMA.
8. Если нужно, введите описание точки назначения агентов KUMA.
9. Введите URL-адрес, с которым требуется установить связь.

   Поддерживаются следующие форматы URL-адресов:

   - `<FQDN>:<port>`
   - `<IP address>:<port>`

IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>]:<port>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`.

10. Настройте дополнительные параметры точки назначения:

- **Обработчики**. Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
- **Размер буфера (байт)**. Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
- **Интервал очистки буфера (сек.)**. Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
- **Ограничить размер дискового буфера**. Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
- **Режим TLS**. Режим шифрования TLS. Доступные значения:
  - **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию.
  - **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации.

    Для использования сертификатов KUMA на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.

  - **Нестандартный PFX с аутентификацией клиента** – использовать шифрование TLS с PFX-секретом. В этом режиме выполняется аутентификация клиента по сертификату. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации.
- **Прокси-сервер**. Прокси-сервер для точки назначения. Вы можете выбрать существующий прокси-сервер или создать новый прокси-сервер.

- **Политика выбора URL**. Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов:

  - **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию.

  - **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него.

  - **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле Размер буфера, а также указать интервал в секундах для отправки событий в точку назначения в поле Интервал очистки буфера.

- **Проверка работоспособности**. Переключатель, включающий проверку работоспособности. По умолчанию этот переключатель выключен.

- **Путь проверки работоспособности**. URL-адрес для отправки запросов для получения данных о работоспособности системы, с которой ресурс точки назначения устанавливает связь.

- **Время ожидания (сек.)**. Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.

11. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Настройка прокси для агентов KUMA

Прокси-серверы используются для хранения параметров конфигурации прокси-серверов, например в точках назначения. Поддерживается тип http.

Как настроить прокси-сервер для агентов KUMA в Web Console:

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Встроенные агенты** → **Интеграция с KUMA**.

5. Выберите вкладку **Прокси-серверы агентов KUMA**.

6. Нажмите на кнопку **Добавить**.

   Откроется форма добавления прокси-сервера агентов KUMA.

7. Введите имя прокси-сервера точки назначения агентов KUMA.

8. Введите адрес прокси-сервера.

9. Введите имя пользователя и пароль для аутентификации на прокси-сервере.

10. Если нужно, введите описание прокси-сервера агентов KUMA.

11. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Фильтрация событий для отправки в KUMA

По умолчанию отправка событий на Сервер KUMA выключена. Для работы KUMA вам нужно включить отправку телеметрии. Для выбора источника событий доступны стандартные журналы: *Application*, *Security* или *System*. Для повышения производительности и оптимизации отправки данных на Сервер KUMA вы можете вручную добавить или исключить отдельные события из телеметрии. Например, вы можете отменить отправку событий Sysmon.

Как сформировать список событий для отправки в KUMA в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите папку **Политики**.

3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

4. В окне политики выберите **Общие настройки** → **Исключения и типы объектов**.

5. В блоке **Настройки телеметрии** → **Телеметрия KUMA** нажмите на кнопку **Настройка**.

6. В открывшемся окне настройте фильтры событий для отправки в KUMA.

   Вы можете настроить фильтрацию событий для стандартных журналов *Application*, *Security*, *System* или добавить другой журнал вручную:

   a. Откройте свойства журнала или нажмите на кнопку **Добавить** и введите название журнала.

   b. Выберите режим отправки событий:

      - **Отправлять все события**. В этом режиме приложение отправляет все события журнала Windows кроме событий, добавленных в правила исключения.

      - **Отправлять только выбранные события**. В этом режиме приложение отправляет только события, добавленные в правила включения.

   c. Сформируйте списки правил исключения или правил включения для соответствующего режима отправки событий.

      Для добавления правил необходимо указать идентификатор события в журнале событий Windows. Вы можете перечислить несколько идентификаторов событий в одном правиле. Для указания нескольких идентификаторов событий используйте символ `,`.

   d. При необходимости включите отправку событий из журнала с помощью флажка рядом с названием журнала.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как сформировать список событий для отправки в KUMA в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки телеметрии**.
5. Выберите вкладку **Телеметрия KUMA**.
6. В открывшемся окне настройте фильтры событий для отправки в KUMA.

   Вы можете настроить фильтрацию событий для стандартных журналов *Application*, *Security*, *System* или добавить другой журнал вручную:

   a. Откройте свойства журнала или нажмите на кнопку **Добавить** и введите название журнала.

   b. Выберите режим отправки событий:

   - **Отправлять все события**. В этом режиме приложение отправляет все события журнала Windows кроме событий, добавленных в правила исключения.
   - **Отправлять только выбранные события**. В этом режиме приложение отправляет только события, добавленные в правила включения.

   c. Сформируйте списки правил исключения или правил включения для соответствующего режима отправки событий.

   Для добавления правил необходимо указать идентификатор события в журнале событий Windows. Вы можете перечислить несколько идентификаторов событий в одном правиле. Для указания нескольких идентификаторов событий используйте символ `,`.

   d. При необходимости включите отправку событий из журнала с помощью переключателя рядом с названием журнала.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Экспорт и импорт фильтров событий KUMA

Вы можете экспортировать список исключений в файл в формате JSON. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество идентификаторов событий. Также вы можете использовать функцию экспорта / импорта для резервного копирования фильтров событий или для миграции списка на другой сервер.

Использование слишком большого количества правил может привести к увеличению нагрузки на Сервер KUMA и снижению производительности компьютера. Рекомендуется добавлять только необходимые правила.

Как экспортировать / импортировать фильтры событий в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Политики**.
3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
4. В окне политики выберите **Общие настройки** → **Исключения и типы объектов**.
5. В блоке **Настройки телеметрии** → **Телеметрия KUMA** нажмите на кнопку **Настройка**.
6. Для экспорта фильтров событий выполните следующие действия:
   a. Выберите журналы событий с фильтрами, которые вы хотите экспортировать.
   b. Нажмите на кнопку → **Экспортировать**.
   c. В открывшемся окне введите имя файла формата JSON, в который вы хотите экспортировать фильтры событий, а также выберите папку, в которой вы хотите сохранить этот файл.
   d. Сохраните файл.

      Kaspersky Endpoint Security экспортирует фильтры событий в JSON-файл.
7. Для импорта фильтров событий выполните следующие действия:
   a. Нажмите на кнопку → **Импортировать**.
   b. В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать фильтры событий.
   c. Откройте файл.

      Если на компьютере уже есть правила фильтрации событий, Kaspersky Endpoint Security заменит их при импорте.
8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как экспортировать / импортировать фильтры событий в Web Console

1. В главном окне Web Console выберите вкладку **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки телеметрии**.
5. Выберите вкладку **Телеметрия KUMA**.
6. Для экспорта фильтров событий выполните следующие действия:
   a. Выберите журналы событий с фильтрами, которые вы хотите экспортировать.
   b. Нажмите на кнопку → **Экспортировать**.

c. В открывшемся окне введите имя файла формата JSON, в который вы хотите экспортировать фильтры событий, а также выберите папку, в которой вы хотите сохранить этот файл.

d. Сохраните файл.

Kaspersky Endpoint Security экспортирует фильтры событий в JSON-файл.

7. Для импорта фильтров событий выполните следующие действия:

a. Нажмите на кнопку → **Импортировать**.

b. В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать фильтры событий.

c. Откройте файл.

Если на компьютере уже есть правила фильтрации событий, Kaspersky Endpoint Security заменит их при импорте.

8. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Также вы можете экспортировать и импортировать фильтры событий из командной строки.

Руководство по миграции с KSWS на KES

Начиная с версии Kaspersky Endpoint Security для Windows 11.8.0 в приложении поддержаны основные функции решения Kaspersky Security для Windows Server (KSWS). *Kaspersky Security для Windows Server* защищает серверы, работающие под управлением операционных систем Microsoft Windows, и сетевые хранилища от вирусов и других угроз компьютерной безопасности, которым подвергаются серверы и сетевые хранилища в процессе обмена файлами. Подробную информацию о работе решения см. в справке Kaspersky Security для Windows Server. Начиная с Kaspersky Endpoint Security версии 11.8.0 вы можете мигрировать с Kaspersky Security для Windows Server на Kaspersky Endpoint Security для Windows и использовать единое решение для защиты рабочих станций и серверов.

Программные требования

Перед миграцией с KSWS на KES убедитесь, что сервер соответствует аппаратным и программным требованиям Kaspersky Endpoint Security для Windows. Списки поддерживаемых версий операционных систем KES и KSWS отличаются. Например, KES не поддерживает работу на серверах под управлением Windows Server 2003.

Минимальные программные требования для миграции с KSWS на KES:

- Kaspersky Endpoint Security для Windows 12.0.
- Kaspersky Security для Windows Server 11.0.1.

  Если у вас установлена более ранняя версия приложения Kaspersky Security для Windows Server, рекомендуем обновить версию приложения до последней. Мастер конвертации политик и задач не поддерживает Kaspersky Security для Windows Server более ранних версий.
- Kaspersky Security Center 14.2.

  Если у вас установлена более ранняя версия решения Kaspersky Security Center, рекомендуем обновить версию решения до 14.2 или выше. В этой версии Kaspersky Security Center мастер массовой конвертации политик и задач позволяет перенести политики в профиль, а не в политику. Также в этой версии Kaspersky Security Center мастер массовой конвертации политики и задач позволяет перенести больше параметров политики.
- Kaspersky Endpoint Agent 3.10.

  Если у вас установлена более ранняя версия приложения Kaspersky Endpoint Agent, рекомендуем обновить версию приложения до последней. Kaspersky Endpoint Security поддерживает миграцию конфигурации [KSWS+KEA] на [KES+встроенный агент] начиная с версии Kaspersky Endpoint Agent 3.10.

Рекомендации для миграции

При миграции с KSWS на KES воспользуйтесь следующими рекомендациями:

- Запланируйте время миграции с KSWS на KES. Выберите время, когда серверы наименее загружены, например, в выходные дни.
- После миграции включайте компоненты приложения постепенно. То есть, например, сначала включите только компонент Защита от файловых угроз, затем включите другие компоненты защиты, затем включите компоненты контроля и так далее. На каждом шаге вам нужно проверять корректную работу приложения и контролировать производительность сервера. Архитектура KES отличается от KSWS, поэтому поведение операционной системы может тоже отличаться.
- Выполняйте миграцию постепенно. Сначала выполните миграцию на одном сервере, затем на нескольких серверах, и далее выполните миграцию на всех серверах организации.
- Выполняйте миграцию для разных типов серверов раздельно. То есть, например, сначала выполните миграцию на серверах баз данных, затем выполните миграцию на почтовых серверах и так далее.
- Миграция на высоконагруженных серверах имеет особенности.

Этапы миграции

Миграция с KSWS на KES выполняется в полуавтоматическом режиме. Это связано с отличиями в архитектуре приложений. Для миграции параметров политики вам нужно запустить мастер массовой конвертации политик и задач (мастер миграции). После переноса параметров политики необходимо вручную настроить параметры, которые мастер миграции не может перенести (например, параметры Защиты паролем). Также после миграции рекомендуется проверить, что мастер миграции перенес параметры корректно.

Выполняйте миграцию с KSWS на KES в следующем порядке:

1. **Выполните миграцию политик и задач KSWS**

   После миграции политик и задач следует выполнить дополнительную настройку параметров. Также рекомендуем убедиться, что Kaspersky Endpoint Security обеспечивает необходимый уровень безопасности серверов после миграции с KSWS.

   > Мастер массовой конвертации политик и задач для Kaspersky Security для Windows Server доступен только в Консоли администрирования (MMC). Перенести параметры политик и задач в Web Console и Kaspersky Security Center Cloud Console невозможно.

2. **Установите Kaspersky Endpoint Security**

Вы можете установить Kaspersky Endpoint Security следующими способами:

- Установка KES после удаления KSWS (рекомендуется).

  Утилита kavremover не поддерживает работу с KSWS.

- Установка KES поверх KSWS.

3. **Активируйте KES ключом KSWS**

4. **Проверка работы приложения после миграции**

   После миграции с KSWS на KES убедитесь, что приложение работает корректно. Проверьте статус сервера в консоли (*OK*). Убедитесь в отсутствии ошибок в работе приложения, также проверьте время последнего соединения с Сервером администрирования, время последнего обновления баз и статус защиты сервера.

   Обратите внимание на миграцию списков исключений, доверенных приложений, доверенных веб-адресов, правил Контроля приложений.

Соответствие компонентов KSWS и KES

При миграции с KSWS на KES набор компонентов мигрирует только при локальной установке приложения.

Соответствие компонентов Kaspersky Security для Windows Server и Kaspersky Endpoint Security для Windows

Компонент Kaspersky Security для Windows Server	Компонент Kaspersky Endpoint Security для Windows
Основная функциональность	Ядро приложения
Анализ журналов	Анализ журналов
Контроль устройств	Контроль устройств
Управление сетевым экраном	*(не поддерживается)* Функции Сетевого экрана KSWS выполняет системный Сетевой экран. В KES функции Сетевого экрана выполняется отдельный компонент. После миграции вы можете настроить Сетевой экран Kaspersky Endpoint Security.
Мониторинг файловых операций	Контроль целостности системы
Защита от эксплойтов	Защита от эксплойтов
Значок в области уведомлений	*(не поддерживается)* Вы можете настроить взаимодействие с пользователем в параметрах интерфейса приложения.
Интеграция с Kaspersky Security Center	Коннектор к Агенту администрирования
Endpoint Agent	*(не поддерживается)* В Kaspersky Endpoint Security 11.9.0 дистрибутив приложения Kaspersky Endpoint Agent исключен из комплекта поставки Kaspersky Endpoint Security. Вам нужно загрузить дистрибутив Kaspersky Endpoint Agent отдельно.
Защита от сетевых угроз	Защита от сетевых угроз
Защита от шифрования	Анализ поведения
Защита от шифрования для NetApp	*(не поддерживается)*

Компонент Kaspersky Security для Windows Server	Компонент Kaspersky Endpoint Security для Windows
Защита трафика	Защита от веб-угроз Защита от почтовых угроз Веб-Контроль
Проверка по требованию	Ядро приложения
Защита ICAP-подключаемых сетевых хранилищ	*(не поддерживается)* Kaspersky Endpoint Security не поддерживает работу компонентов защиты подключаемых сетевых хранилищ. Если вам нужны эти компоненты, вы можете продолжить использование Kaspersky Security для Windows Server.
Защита RPC-подключаемых сетевых хранилищ	*(не поддерживается)* Kaspersky Endpoint Security не поддерживает работу компонентов защиты подключаемых сетевых хранилищ. Если вам нужны эти компоненты, вы можете продолжить использование Kaspersky Security для Windows Server.
Постоянная защита файлов	Защита от файловых угроз
Проверка скриптов	*(не поддерживается)* Проверку скриптов выполняют другие компоненты приложения, например, AMSI-защита.
Использование KSN	Kaspersky Security Network
Контроль запуска программ	Контроль приложений
Счетчики производительности	*(не поддерживается)*

Соответствие параметров KSWS и KES

При миграции политик и задач параметры KES будут настроены в соответствии с параметрами KSWS. Параметры компонентов, которых нет в KSWS, будут установлены с параметрами по умолчанию.

Параметры программы

Масштабируемость, интерфейс и настройки сканирования

Параметры программы не поддерживаются в Kaspersky Endpoint Security для Windows.

Параметры программы

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Параметры масштабируемости	*(не мигрирует)* Kaspersky Endpoint Security контролирует все рабочие процессы.
Показывать Значок области уведомлений	*(не мигрирует)* По умолчанию на клиентском компьютере доступно главное окно Kaspersky Endpoint Security и значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает уведомления над значком программы. Вы можете настроить взаимодействие с пользователем в параметрах интерфейса программы.
Восстанавливать атрибуты файлов после сканирования	*(не мигрирует)* Kaspersky Endpoint Security восстанавливает атрибуты файлов после проверки файла автоматически.
Ограничивать сканирующий поток в использовании CPU	*(не мигрирует)* Kaspersky Endpoint Security не ограничивает использование процессора компьютера при проверке. Вы можете настроить запуск задачи во время, когда компьютер наименее нагружен.

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Папка для временных файлов, создаваемых при сканировании	*(не мигрирует)* Kaspersky Endpoint Security помещает временные файлы в папку `C:\Windows\Temp`.
Параметры HSM-системы	*(не мигрирует)* Kaspersky Endpoint Security не поддерживает HSM-системы.

Безопасность и надежность

Параметры безопасности KSWS мигрируют в раздел **Общие настройки**, подразделы **Настройки приложения** и **Интерфейс**.

Параметры безопасности программы

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Защищать процессы программы от внешних угроз	**Включить самозащиту** (подраздел **Настройки приложения**)
Использовать защиту паролем	*(не мигрирует)* Kaspersky Endpoint Security имеет собственную функцию Защита паролем (подраздел **Интерфейс**).
Выполнять восстановление задач	*(не мигрирует)* Kaspersky Endpoint Security автоматически восстанавливает только задачи *Поиск вредоносного ПО*. Остальные задачи Kaspersky Endpoint Security запускает по расписанию.
Не запускать задачи проверки по расписанию	**Откладывать задачи по расписанию при работе от аккумулятора** (подраздел **Настройки приложения**)
Остановить выполняемые задачи проверки	*(не мигрирует)* При переходе компьютера на источник бесперебойного питания Kaspersky Endpoint Security продолжает выполнение запущенных задач проверки.

Параметры соединения

Параметры взаимодействия с Сервером администрирования мигрируют в раздел **Общие настройки**, подразделы **Настройки сети** и **Настройки приложения**.

Параметры взаимодействия с Сервером администрирования

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Параметры прокси-сервера	**Настройки прокси-сервера** (подраздел **Настройки сети**)
Не использовать прокси-сервер для локальных адресов	**Не использовать прокси-сервер для локальных адресов** (подраздел **Настройки сети**)
Параметры аутентификации на прокси-сервере	**Использовать аутентификацию на прокси-сервере** (подраздел **Настройки сети**) Пароль для аутентификации на прокси-сервере не мигрирует. После миграции политики вам нужно ввести пароль вручную.
Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы	**Использовать Kaspersky Security Center в качестве прокси-сервера для активации** (подраздел **Настройки приложения**)

Запуск локальных системных задач

Kaspersky Endpoint Security игнорирует параметры запуска локальных системных задач Kaspersky Security для Windows Server. Вы можете настроить использование локальных задач KES в разделе **Локальные задачи**, подраздел **Управление задачами**. Также вы можете настроить расписание запуска задач *Поиск вредоносного ПО* и *Обновление баз и модулей приложения* в свойствах задач.

Дополнительные возможности

Доверенная зона

Параметры доверенной зоны KSWS мигрируют в раздел **Общие настройки**, подраздел **Исключения**.

Параметры доверенной зоны

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Проверяемый объект (Исключения)	**Исключения из проверки** (Исключения из проверки) Способы выбора объектов в KSWS и KES отличаются. При миграции KES поддерживает исключения, заданные в виде отдельных файлов или пути к файлу / папке. Если в KSWS есть исключения, заданные в виде предопределенной области или веб-адреса скрипта, такие исключения не мигрируют. После миграции вам нужно добавить эти исключения вручную. Исключения в виде предопределенной области нужно настроить в свойствах задачи *Поиск вредоносного ПО*. Исключения в виде веб-адреса скрипта нужно добавить в доверенные веб-адреса для Защиты от веб-угроз.
Применять также к подпапкам (Исключения)	**Включить вложенные папки** (Исключения из проверки)
Обнаруживаемые объекты (Исключения)	**Тип обнаруживаемого объекта** (Исключения из проверки)
Область применения исключения (Исключения)	**Компоненты защиты** (Исключения из проверки) Если в KSWS выбран хотя бы один компонент, KES применяет исключение для всех компонентов программы.
Комментарий (Исключения)	**Комментарий** (Исключения из проверки)
Доверенные процессы (Доверенные процессы)	**Доверенные приложения** Способы выбора доверенных процессов / программ в KSWS и KES отличаются. При миграции KES поддерживает доверенные программы, заданные в виде пути к исполняемому файлу или маске. Если в KSWS есть доверенные процессы, заданные в виде хеша файла, такие доверенные процессы не мигрируют. После миграции вам нужно добавить эти доверенные процессы вручную.
Не проверять файловые операции резервного копирования (Доверенные процессы)	**Не контролировать активность приложения** (Доверенные приложения)

Проверка съемных дисков

Параметры проверки съемных дисков мигрируют в раздел **Локальные задачи**, подраздел **Проверка съемных дисков**.

Параметры проверки съемных дисков

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Проверять съемные диски при их подключении по USB	**Действие при подключении съемного диска**
Проверять, если объем содержащихся на диске данных не превышает порог (МБ)	**Максимальный размер съемного диска**

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Запускать проверку с уровнем безопасности: • **Максимальная защита**; • **Рекомендуемый**; • **Максимальное быстродействие**.	**Действие при подключении съемного диска**: • **Максимальная защита**; • **Рекомендуемый**. Уровни безопасности KSWS соответствуют режимам проверки KES следующим образом: • Максимальная защита – Максимальная защита. • Рекомендуемый – Рекомендуемый. • Максимальное быстродействие – Рекомендуемый.

Права пользователей на управление программой

Kaspersky Endpoint Security не поддерживает назначение прав пользователей на управление программой и службами программы. Вы можете настроить параметры доступа пользователей и групп пользователей на управление программой в Kaspersky Security Center.

Права пользователей на управление службой Kaspersky Security Service

Kaspersky Endpoint Security не поддерживает назначение прав пользователей на управление программой и службами программы. Вы можете настроить параметры доступа пользователей и групп пользователей на управление программой в Kaspersky Security Center.

Хранилища

Параметры хранилищ KSWS мигрируют в раздел **Общие настройки**, подраздел **Отчеты и хранилище**, и в раздел **Базовая защита**, подраздел **Защита от сетевых угроз**.

Параметры хранилищ

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Папка резервного хранилища	*(не мигрирует)* Kaspersky Endpoint Security сохраняет резервные копии файлов в папке `C:\ProgramData\Kaspersky Lab\KES.14.3\QB`.
Максимальный размер резервного хранилища (МБ)	**Ограничить размер хранилища до N МБ** (раздел **Общие настройки** → **Отчеты и хранилище**).
Порог доступного пространства (МБ)	*(не мигрирует)* Kaspersky Endpoint Security регистрирует событие *В хранилище карантина скоро закончится место* при достижении порога 50 %.
Папка, в которую восстанавливаются объекты	*(не мигрирует)* Kaspersky Endpoint Security восстанавливает файлы в папку исходного размещения.
Папка карантина	*(не мигрирует)* Kaspersky Endpoint Security сохраняет резервные копии файлов в папке `C:\ProgramData\Kaspersky Lab\KES.14.3\QB`.
Максимальный размер карантина (МБ)	*(не мигрирует)* Kaspersky Endpoint Security использует резервное хранилище для размещения возможно зараженных объектов. При миграции Kaspersky Endpoint Security игнорирует параметры карантина.
Порог доступного пространства (МБ)	*(не мигрирует)* Kaspersky Endpoint Security использует резервное хранилище для размещения возможно зараженных объектов. При миграции Kaspersky Endpoint Security игнорирует параметры карантина.
Папка, в которую восстанавливаются объекты	*(не мигрирует)* Kaspersky Endpoint Security восстанавливает файлы в папку исходного размещения.
Автоматически разблокировать через N	**Блокировать атакующие устройства на N мин** (раздел **Базовая защита** → **Защита от сетевых угроз**).

Постоянная защита сервера

Постоянная защита файлов

Параметры Постоянной защиты файлов KSWS мигрируют в раздел **Базовая защита**, подраздел **Защита от файловых угроз**.

Параметры Постоянной защиты файлов

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Режим защиты объектов: • **Интеллектуальный режим**; • **При выполнении**; • **При открытии**; • **При открытии и изменении**.	**Режим проверки**: • **Интеллектуальный**; • **При выполнении**; • **При доступе**; • **При доступе и изменении**.
Углубленный анализ запускаемых процессов	*(не мигрирует)* Kaspersky Endpoint Security поддерживает только один режим анализа – Оптимальный.
Эвристический анализатор: • **Поверхностный**; • **Средний**; • **Глубокий**.	**Эвристический анализ**: • **Поверхностный**; • **Средний**; • **Глубокий**.
Применять доверенную зону	*(не мигрирует)* Kaspersky Endpoint Security применяет доверенную зону для всех компонентов. Вы можете настроить исключения в параметрах доверенной зоны.
Использовать KSN для защиты	*(не мигрирует)* Kaspersky Endpoint Security использует KSN для всех компонентов приложения.
Блокировать доступ к сетевым файловым ресурсам для узлов, с которых ведется вредоносная активность	*(не мигрирует)* Kaspersky Endpoint Security по умолчанию блокирует доступ к сетевым файловым ресурсам для узлов, с которых ведется вредоносная активность.
Запустить сканирование важных областей при обнаружении активного заражения	*(не мигрирует)* Kaspersky Endpoint Security не запускает задачу проверки важных областей при обнаружении активного заражения.
Отправлять объекты в Kaspersky Sandbox	*(не мигрирует)* Kaspersky Endpoint Security по умолчанию отправляет объекты на проверку в Kaspersky Sandbox.
Область защиты	**Область защиты**
Параметры расписания	*(не мигрирует)* Kaspersky Endpoint Security использует собственное расписание приостановки Защиты от файловых угроз.

Использование KSN

Параметры Kaspersky Security Network KSWS мигрируют в раздел **Продвинутая защита**, подраздел **Kaspersky Security Network**.

Параметры Kaspersky Security Network

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Принять условия Положения о Kaspersky Security Network	**Положение о Kaspersky Security Network** Kaspersky Endpoint Security предлагает принять условия Положения о Kaspersky Security Network при установке программы, создании новой политики или включении использования Kaspersky Security Network.
Разрешить отправку данных о проверяемых файлах	*(не мигрирует)* Kaspersky Endpoint Security отправляет данные о проверяемых файлах автоматически, если использование KSN включено.
Разрешить отправку данных о запрашиваемых веб-адресах	*(не мигрирует)* Kaspersky Endpoint Security отправляет данные о запрашиваемых веб-адресах автоматически, если использование KSN включено.
Разрешить отправку статистики Kaspersky Security Network	**Включить расширенный режим KSN**
Принять условия Положения о Kaspersky Managed Protection	*(не мигрирует)* Служба KMP отсутствует в Kaspersky Endpoint Security.
Действия над объектами, недоверенными в KSN	*(не мигрирует)* Вы можете настроить действие при обнаружении угрозы в параметрах компонентов защиты и задач проверки.
Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает N МБ	*(не мигрирует)* Вы можете настроить ограничения проверки файлов большого размера в параметрах компонентов защиты и задач проверки.
Использовать Kaspersky Security Center в качестве прокси-сервера KSN	**Использовать Сервер администрирования как прокси-сервер KSN**
Параметры расписания	*(не мигрирует)* Настроить отдельное расписание работы для компонента невозможно. Компонент включен постоянно пока работает Kaspersky Endpoint Security.

Защита трафика

Параметры Защиты трафика KSWS мигрируют в раздел **Базовая защита**, подразделы **Защита от веб-угроз** и **Защита от почтовых угроз**, раздел **Контроль безопасности**, подраздел **Веб-Контроль**, раздел **Общие настройки**, подраздел **Настройки сети**.

Параметры Защиты трафика

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Применять правила контроля веб-страниц	**Веб-Контроль** (подраздел **Веб-Контроль**) Правила контроля веб-страниц мигрируют в Kaspersky Endpoint Security в отдельные правила.
Применять правила контроля сертификатов	*(не мигрирует)* Kaspersky Endpoint Security не поддерживает правила контроля сертификатов.
Применять правила категоризации веб-ресурсов	**Веб-Контроль** (подраздел **Веб-Контроль**) Запрещающие правила категоризации веб-ресурсов мигрируют в Kaspersky Endpoint Security в одно запрещающее правило. Kaspersky Endpoint Security игнорирует разрешающие правила категоризации. Соответствие категорий KSWS и KES представлено ниже.
Разрешать загрузку веб-страницы, если не удалось присвоить категорию	*(не мигрирует)* Kaspersky Endpoint Security разрешает загрузку веб-страницы, если не удалось присвоить категорию.
Разрешать загрузку легальных веб-ресурсов, которые могут быть использованы для нанесения вреда защищаемому устройству	*(не мигрирует)* Kaspersky Endpoint Security разрешает загрузку легальных веб-ресурсов, которые могут быть использованы для нанесения вреда защищаемому устройству.
Разрешать загрузку легальных рекламных веб-ресурсов	*(не мигрирует)* Вы можете управлять загрузкой легальных рекламных веб-ресурсов с помощью категории веб-ресурсов *Баннеры* в параметрах Веб-Контроля.

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Режим работы: • **Драйверный перехват**; • **Перенаправление трафика**; • **Внешний прокси-сервер**.	*(не мигрирует)* Kaspersky Endpoint Security работает только в режиме Драйверный перехват.
Параметры соединения с ICAP-службой	*(не мигрирует)* Kaspersky Endpoint Security не поддерживает защиту ICAP-подключаемых сетевых хранилищ.
Проверять безопасные соединения по протоколу HTTPS	**Проверять защищенные соединения** / режим **Всегда проверять защищенные соединения** (подраздел **Настройки сети**)
Использовать версию крипто-протокола TLS	*(не мигрирует)* Kaspersky Endpoint Security проверяет зашифрованный сетевой трафик, передаваемый по следующим протоколам: • SSL 3.0; • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Дополнительно вы можете заблокировать соединения по протоколу SSL 2.0 в параметрах проверки защищенных соединений.
Не доверять веб-серверу с невалидным сертификатом	**Адрес** (подраздел **Настройки сети**)
Перехватывать по портам (Область перехвата)	**Контролируемые порты** (подраздел **Настройки сети**) При миграции KES снимает флажки **Контролировать все порты для приложений из списка, рекомендованного "Лабораторией Касперского"** и **Контролировать все порты для указанных приложений**.
Исключать по портам (Область перехвата)	*(не мигрирует)*
Исключать IP-адреса (Область перехвата)	**Настроить доверенные адреса** (подраздел **Настройки сети**)
Исключать по приложениям (Область перехвата)	**Настроить доверенные приложения** (подраздел **Настройки сети**) При миграции KES настроит следующие параметры для доверенного приложения: • Установлен флажок **Не проверять сетевой трафик**. KES не проверяет весь сетевой трафик, для любых удаленных IP-адресов и любых портов. • Остальные флажки в параметрах доверенного приложения сняты.
Порт безопасности	*(не мигрирует)*
Проверять ссылки по базе вредоносных веб-адресов	**Проверять веб-адрес по базе вредоносных веб-адресов** (подраздел **Защита от веб-угроз**)
Проверять ссылки по базе фишинговых веб-адресов	**Проверять веб-адрес по базе фишинговых веб-адресов** (подраздел **Защита от веб-угроз**)
Использовать KSN для защиты	*(не мигрирует)* Kaspersky Endpoint Security использует KSN для всех компонентов приложения.
Использовать Доверенную зону	*(не мигрирует)* Kaspersky Endpoint Security применяет доверенную зону для всех компонентов. Вы можете настроить исключения в параметрах доверенной зоны.
Использовать эвристический анализатор	**Использовать эвристический анализ** (подразделы **Защита от веб-угроз** и **Защита от почтовых угроз**)
Уровень безопасности	*(не мигрирует)* Kaspersky Endpoint Security имеет собственные уровни безопасности для работы компонентов Защита от веб-угроз и Защита от почтовых угроз. По умолчанию Kaspersky Endpoint Security устанавливает рекомендуемый уровень безопасности.
Защищать устройство от почтовых угроз	**Защита от почтовых угроз** (подраздел **Защита от почтовых угроз**) **Подключить расширение для Microsoft Outlook** **Только входящие сообщения** (Область защиты) **Проверять при получении** (Защита почты)
Параметры расписания	*(не мигрирует)* Настроить отдельное расписание работы для компонента невозможно. Компонент включен постоянно пока работает Kaspersky Endpoint Security.

Защита от эксплойтов

Параметры Защиты от эксплойтов KSWS мигрируют в раздел **Продвинутая защита**, подраздел **Защита от эксплойтов**.

Параметры Защиты от эксплойтов

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Защищать процессы от эксплуатации уязвимостей в режиме: • **Завершать скомпрометированные процессы**; • **Только сообщать**.	**При обнаружении эксплойта**: • **Блокировать**; • **Информировать**.
Сообщать о скомпрометированных процессах посредством службы терминалов	*(не мигрирует)* Kaspersky Endpoint Security не поддерживает службы терминалов.
Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security Service	*(не мигрирует)* Kaspersky Endpoint Security защищает процессы от эксплуатации уязвимостей постоянно.
Защищаемые процессы	**Включить защиту памяти системных процессов** Kaspersky Endpoint Security не поддерживает выбор защищаемых процессов. Вы можете включить защиту памяти только системных процессов.
Техники защиты от эксплойтов: • **Применять все доступные техники защиты от эксплойтов**; • **Применять указанные техники защиты от эксплойтов**.	*(не мигрирует)* Kaspersky Endpoint Security использует все доступные техники защиты от эксплойтов.

Защита от сетевых угроз

Параметры Защиты от сетевых угроз KSWS мигрируют в раздел **Базовая защита**, подраздел **Защита от сетевых угроз**.

Параметры Защиты от сетевых угроз

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Режим работы: • **Не осуществлять мониторинг**; • **Только уведомлять об обнаруженных атаках**; • **Блокировать соединения при обнаружении атаки**.	**Защита от сетевых угроз** Если выбран режим **Не осуществлять мониторинг**, то Защита от сетевых угроз выключена. Если выбран режим **Только уведомлять об обнаруженных атаках** или **Блокировать соединения при обнаружении атаки**, то Защита от сетевых угроз включена. Kaspersky Endpoint Security работает только в режиме **Блокировать соединения при обнаружении атаки**.
Не останавливать анализ трафика, если задача не исполняется	*(не мигрирует)* Kaspersky Endpoint Security анализирует трафик постоянно, если компонент включен.
Не контролировать IP-адреса, указанные в исключениях	**Исключения**
Параметры расписания	*(не мигрирует)* Настроить отдельное расписание работы для компонента невозможно. Компонент включен постоянно пока работает Kaspersky Endpoint Security.

Проверка скриптов

Kaspersky Endpoint Security не поддерживает работу компонента Проверка скриптов. Проверку скриптов выполняют другие компоненты программы, например, AMSI-защита.

Категории веб-сайтов

Kaspersky Endpoint Security поддерживает не все категории Kaspersky Security для Windows Server. Категории, которых нет в Kaspersky Endpoint Security, не мигрируют. Таким образом, правила категоризации веб-ресурсов с неподдерживаемыми категориями не мигрируют.

Категории Kaspersky Security для Windows Server	Категории Kaspersky Endpoint Security для Windows
Wargaming	Видеоигры
Аборт	*(не мигрирует)*
Азартные игры (расширенная категория)	Азартные игры, лотереи, тотализаторы
Алкоголь	Алкоголь, табак, наркотики и психотропы
Анонимизация	Средства анонимного доступа
Анорексия	*(не мигрирует)*
Аренда недвижимости	*(не мигрирует)*
Аудио, видео и дистрибутивы	Программное обеспечение, аудио, видео
Банки	Банки
Блоги	Блоги
Вооруженные силы	Оружие, взрывчатые вещества, вооруженные силы
Дети	*(не мигрирует)*
Дискриминация	Насилие, разжигание вражды
Дом и семья	*(не мигрирует)*
Доменные и хостинговые сервисы	Общение в сети
Животные	*(не мигрирует)*
Закон и политика	Запрещено региональным законодательством
Запрещено Роскомнадзором (РФ)	Запрещено законодательством Российской Федерации
Запрещено Федеральным законом 436 (РФ)	Запрещено законодательством Российской Федерации
Запрещено законодательством РФ	Запрещено законодательством Российской Федерации
Запрещено мировым законодательством	Запрещено региональным законодательством
Знакомства для взрослых	Для взрослых
Интернет-сервисы	*(не мигрирует)*
Интим-магазины	Для взрослых
Информационные технологии	*(не мигрирует)*
Казино	Азартные игры, лотереи, тотализаторы
Книги	*(не мигрирует)*
Компьютерные игры	Видеоигры
Красота и здоровье	*(не мигрирует)*
Культура	*(не мигрирует)*
ЛГБТ	Для взрослых
Лотереи	Азартные игры, лотереи, тотализаторы
Медицина	*(не мигрирует)*
Мода	*(не мигрирует)*
Музыка	*(не мигрирует)*
Наркотики	Алкоголь, табак, наркотики и психотропы
Насилие	Насилие, разжигание вражды
Недовольство	*(не мигрирует)*
Незаконные препараты	Алкоголь, табак, наркотики и психотропы
Ненависть и дискриминация	Насилие, разжигание вражды

Категории Kaspersky Security для Windows Server	Категории Kaspersky Endpoint Security для Windows
Нецензурная брань	Нецензурная лексика
Нижнее белье	Для взрослых
Новости	Новостные ресурсы
Нудизм	Для взрослых
Образование	*(не мигрирует)*
Онлайн магазины	Интернет-магазины
Онлайн общение	Общение в сети
Онлайн оплата	Платежные системы
Онлайн шоппинг (собственные системы оплаты)	Интернет-магазины
Онлайн энциклопедии	*(не мигрирует)*
Онлайн-банкинг	Банки
Оружие	Оружие, взрывчатые вещества, вооруженные силы
Охота и рыбалка	*(не мигрирует)*
Платежные системы	Платежные системы
Поиск работы	Поиск работы
Поисковые системы	*(не мигрирует)*
Политическое решение (JP)	Запрещено полицией Японии
Получено доверенное заключение (KPSN)	*(не мигрирует)*
Получено недоверенное заключение (KPSN)	*(не мигрирует)*
Порно	Для взрослых
Потоковое вещание	Новостные ресурсы
Почтовые веб-сервисы	Веб-почта
Путешествия	*(не мигрирует)*
Радио и телевидение	Новостные ресурсы
Реклама	Баннеры
Религия	Религии, религиозные объединения
Рестораны, кафе, еда	*(не мигрирует)*
Сайты знакомств	Сайты знакомств
Секс-образование	Для взрослых
Социальные сети	Социальные сети
Спорт	*(не мигрирует)*
Ставки	Азартные игры, лотереи, тотализаторы
Суицид	Насилие, разжигание вражды
Табак	Алкоголь, табак, наркотики и психотропы
Торрент	Торренты
Упомянуто в Федеральном списке экстремистских материалов (РФ)	Запрещено законодательством Российской Федерации
Файловые обменники	Файловые обменники
Фармакология	*(не мигрирует)*
Хобби и развлечения	*(не мигрирует)*
Чаты и форумы	Чаты, форумы, IM
Школы и университеты	*(не мигрирует)*

Категории Kaspersky Security для Windows Server	Категории Kaspersky Endpoint Security для Windows
Эзотерика	*(не мигрирует)*
Экстремизм и расизм	Насилие, разжигание вражды
Электронная торговля	Интернет-магазины
Эротика	Для взрослых
Юмор	*(не мигрирует)*

Контроль активности на серверах

Контроль запуска программ

Параметры Контроля программ KSWS мигрируют в раздел **Контроль безопасности**, подраздел **Контроль приложений**.

Параметры Контроля запуска программ

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Режим работы: • **Только статистика**; • **Активный**.	**Действие** (Контроля приложений): • **Тестировать правила**; • **Применять правила**.
Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска	*(не мигрирует)* Kaspersky Endpoint Security проверяет программу при каждой попытке ее запуска.
Запрещать запуск командных интерпретаторов без команды к исполнению	*(не мигрирует)* Kaspersky Endpoint Security разрешает запуск командных интерпретаторов, если их запуск не запрещен правилами Контроля программ.
Правила	**Правила Контроля приложений** *(поддерживается с ограничениями)* В Kaspersky Endpoint Security 11.11.0 добавлена поддержка миграции правил Контроля запуска приложений. Миграция правил Контроля запуска приложений имеет ограничения. По умолчанию Контроль запуска программ KSWS включает в себя два правила: • **Разрешать к запуску скрипты и пакеты MSI, доверенные в ОС по сертификату**. • **Разрешать к запуску исполняемые файлы, доверенные в ОС по сертификату**. Если хотя бы одно исходное правило KSWS имело тип **Разрешающее**, при миграции KES создает новое разрешающее правило **Приложения с доверенными корневыми сертификатами**. То есть, Контроль приложений KES разрешает запуск доверенных скриптов, пакетов MSI и исполняемых файлов с помощью одного правила. Если оба исходных правила KSWS имели тип **Запрещающее**, KES не добавляет правил для управления приложениями с доверенными корневыми сертификатами.
Использовать правила для исполняемых файлов	*(не мигрирует)* Задать область применения правил в параметрах Контроля приложений KES невозможно. Контроль приложений KES применяет правила ко всем типам файлов: исполнительные файлы, скрипты и пакеты MSI. Если в KSWS в область применения правил включены все типы файлов, при миграции KES переносит правила KSWS. Если в KSWS из области применения правила исключен какой-то тип файлов, при миграции KES также переносит правила KSWS, но в качестве действия Контроля приложений выбирает **Тестировать правила**.
Контролировать загрузку DLL-модулей	**Контролировать загрузку динамических библиотек (значительно увеличивает нагрузку на систему)**
Использовать правила для скриптов и пакетов MSI	*(не мигрирует)* Задать область применения правил в параметрах Контроля приложений KES невозможно. Контроль приложений KES применяет правила ко всем типам файлов: исполнительные файлы, скрипты и пакеты MSI. Если в KSWS в область применения правил включены все типы файлов, при миграции KES переносит правила KSWS. Если в KSWS из области применения файла исключен какой-то тип файлов, при миграции KES переносит правила KSWS, но в качестве действия Контроля приложений выбирает **Тестировать правила**.

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Запрещать запуск программ, недоверенных в KSN	*(не мигрирует)* Kaspersky Endpoint Security не учитывает репутацию программ и разрешает или запрещает запуск программ в соответствии с правилами.
Разрешать запуск программ, доверенных в KSN	При миграции KES добавляет новое разрешающее правило. В качестве условия срабатывания правила указана KL-категория **Другие приложения\Приложения, доверенные согласно репутации в KSN**.
Пользователи и / или группы пользователей, которым разрешен запуск доверенных в KSN программ	**Пользователи и их права** в разрешающем правиле Контроля приложений, в которое включена KL-категория **Другие приложения\Приложения, доверенные согласно репутации в KSN**.
Автоматически разрешать распространение с помощью указанных программ и пакетов установки	Контроль пакетов установки KSWS и KES отличается. При миграции KES добавляет новые разрешающие правила с приложениями, для которых разрешено автоматическое распространение ПО. В качестве условия срабатывания правила указан хеш файла.
Всегда разрешать распространение программ с помощью установщика Windows	Контроль пакетов установки KSWS и KES отличается. При миграции KES добавляет новые разрешающие правила с приложениями, для которых разрешено автоматическое распространение ПО (**Список программ и пакетов установки, разрешенных к запуску**). В качестве условия срабатывания правила указан хеш файла. В свойствах правила установлен флажок **Доверенные приложения обновления**.
Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи	*(не мигрирует)*
Список программ и пакетов установки, разрешенных к запуску	Контроль пакетов установки KSWS и KES отличается. При миграции KES добавляет новые разрешающие правила с приложениями, для которых разрешено автоматическое распространение ПО. В качестве условия срабатывания правила указан хеш файла. В свойствах правила установлен флажок **Доверенные приложения обновления**.
Параметры расписания	*(не мигрирует)* Если в параметрах KSWS настроено расписание работы компонента, при миграции компонент Контроль приложений будет включен. Если расписание работы компонента не настроено, Контроль приложений будет выключен. Настроить отдельное расписание работы для компонента невозможно. Компонент включен постоянно пока работает Kaspersky Endpoint Security.

Контроль устройств

Параметры Контроля устройств KSWS мигрируют в раздел **Контроль безопасности**, подраздел **Контроль устройств**.

Параметры Контроля устройств

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Режим работы: • **Активный**; • **Только статистика**.	*(не мигрирует)* Контроль устройств работает в режиме *Активный*. Статистику подключения устройств предоставляет Аудит программы постоянно.
Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется	*(не мигрирует)* Контроль устройств работает постоянно, если запущена программа Kaspersky Endpoint Security.
Правила контроля устройств	**Доверенные устройства** При миграции Kaspersky Endpoint Security игнорирует выключенные правила KSWS.
Параметры расписания	*(не мигрирует)* Kaspersky Endpoint Security использует собственное расписание для доступа к некоторым типам устройств.

Защита сетевых хранилищ

Защита RPC-подключаемых сетевых хранилищ

Kaspersky Endpoint Security не поддерживает работу компонентов защиты подключаемых сетевых хранилищ. Если вам нужны эти компоненты, вы можете продолжить использование Kaspersky Security для Windows Server.

Защита ICAP-подключаемых сетевых хранилищ

Kaspersky Endpoint Security не поддерживает работу компонентов защиты подключаемых сетевых хранилищ. Если вам нужны эти компоненты, вы можете продолжить использование Kaspersky Security для Windows Server.

Защита от шифрования для NetApp

Kaspersky Endpoint Security не поддерживает работу компонента Защита от шифрования для NetApp. Защиту от шифрования выполняют другие компоненты программы, например, Анализ поведения.

Контроль активности в сети

Управление сетевым экраном

Kaspersky Endpoint Security не поддерживает управление сетевым экраном KSWS. Функции Сетевого экрана KSWS выполняет системный Сетевой экран. После миграции вы можете настроить Сетевой экран Kaspersky Endpoint Security.

Защита от шифрования

Параметры Защиты от шифрования KSWS мигрируют в раздел **Продвинутая защита**, подраздел **Анализ поведения**.

Параметры Защиты от шифрования

Параметры KSWS	Параметры KES
Режим работы: • **Только статистика**; • **Активный**.	**При обнаружении внешнего шифрования папок общего доступа**: • **Информировать**; • **Блокировать**.
Эвристический анализатор	*(не мигрирует)* Kaspersky Endpoint Security не использует технологию эвристического анализа для работы Анализа поведения.
Параметры области защиты: • **Все общие сетевые папки защищаемого устройства**; • **Только указанные общие папки**.	*(не мигрирует)* Kaspersky Endpoint Security защищает от шифрования все общие сетевые папки защищаемого компьютера.
Исключения	*(не мигрирует)* Kaspersky Endpoint Security имеет собственные исключения для компонента Анализ поведения. Вы можете добавить исключения вручную после миграции.
Параметры расписания	*(не мигрирует)* Настроить отдельное расписание работы для компонента невозможно. Компонент включен постоянно пока работает Kaspersky Endpoint Security.

Мониторинг файловых операций

Параметры компонента Мониторинг файловых операций KSWS мигрируют в раздел **Контроль безопасности**, подраздел **Контроль целостности системы**.

Параметры Мониторинга файловых операций

Параметры KSWS	Параметры KES
Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга	*(не мигрирует)* Kaspersky Endpoint Security не фиксирует события о файловых операциях, выполненных в период обрыва мониторинга.
Блокировать попытки компрометации журнала USN	*(не мигрирует)* Kaspersky Endpoint Security не блокирует попытки компрометации USN-журнала.
Область мониторинга	**Область мониторинга** → **Файл** *(поддерживается с ограничениями)* Выключенные записи области мониторинга не мигрирует в KES. Kaspersky Endpoint Security добавляет в область мониторинга только те записи, которые были включены.
Доверенные пользователи	**Доверенные пользователи и / или группы пользователей**
Маркеры файловых операций	**Маркеры файловых операций**
Рассчитывать контрольную сумму файла после файловой операции, если это возможно	**Хеширование**
Исключения	**Исключения** → **Файл**

Анализ журналов

Параметры Анализа журналов KSWS мигрируют в раздел **Контроль безопасности**, подраздел **Анализ журналов**.

Параметры Анализа журналов

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Применять пользовательские правила для анализа журналов	*(не мигрирует)* Kaspersky Endpoint Security применяет все пользовательские правила, которые включены.
Пользовательские правила	**Пользовательские правила** Предустановленное правило **В системе установлена служба (для Server 2003 ОС)** не мигрирует в KES.
Использовать предзаданные правила для анализа журналов	*(не мигрирует)* Kaspersky Endpoint Security применяет все предустановленные правила, которые включены.
Предзаданные правила	**Предустановленные правила**
Обработка подбора пароля	**Обработка подбора пароля**
Обработка атипичной аутентификации	**Обработка атипичной аутентификации**
Исключения (IP-адреса)	**Исключения** (IP-адрес)
Исключения (пользователи)	**Исключения** (Пользователи)
Параметры расписания	*(не мигрирует)* Настроить отдельное расписание работы для компонента невозможно. Компонент включен постоянно пока работает Kaspersky Endpoint Security.

Журналы и уведомления

Журналы выполнения задач

Параметры журналов KSWS мигрируют в раздел **Общие настройки**, подразделы **Интерфейс** и **Отчеты и хранилище**.

Параметры журналов

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Запись событий в журнал	**Уведомления** (подраздел **Интерфейс**)
Папка с журналами	*(не мигрирует)* Kaspersky Endpoint Security сохраняет отчеты в папку `C:\ProgramData\Kaspersky Lab\KES.14.3\Report`.
Удалять журналы выполнения задач старше, чем N сут	*(не мигрирует)* Вы можете настроить срок хранения отчетов KES в разделе **Общие настройки**, подраздел **Отчеты и хранилище**.
Удалять события журнала системного аудита старше, чем N сут	*(не мигрирует)* Kaspersky Endpoint Security применяет ограничение хранения отчетов ко всем отчетам, включая отчеты системного аудита.
Интеграция с SIEM	*(не мигрирует)* Вы можете настроить интеграцию с SIEM в Kaspersky Security Center.

Уведомления о событиях

Параметры уведомлений KSWS мигрируют в раздел **Общие настройки**, подраздел **Интерфейс**.

Параметры уведомлений

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Уведомления	**Уведомления**
Уведомление пользователей: • **Средствами службы терминалов**; • **Средствами службы сообщений**.	*(не мигрирует)* Kaspersky Endpoint Security не поддерживает изменение текста уведомлений. Kaspersky Endpoint Security показывает стандартные уведомления программы.
Уведомление администраторов: • **Средствами службы сообщений**; • **Путем запуска исполняемого файла**; • **По электронной почте**.	В Kaspersky Endpoint Security мигрируют только параметры отправки уведомлений по электронной почте – **Настройка почтовых уведомлений** (блок **Уведомления**). Остальные способы уведомления администраторов не поддерживаются.
Базы программы устарели	**Отправлять уведомление "Базы устарели", если базы не обновлялись**
Базы программы сильно устарели	**Отправлять уведомление "Базы сильно устарели", если базы не обновлялись**
Проверка важных областей защищаемого устройства давно не выполнялась	*(не мигрирует)* Kaspersky Endpoint Security формирует событие пропущенной проверки важных областей через три дня.

Взаимодействие с Сервером администрирования

Параметры взаимодействия с Сервером администрирования KSWS мигрируют в раздел **Общие настройки**, подраздел **Отчеты и хранилище**.

Параметры взаимодействия с Сервером администрирования

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Данные об объектах карантина	**Файлы карантина**
Данные об объектах резервного хранилища	**Файлы резервного хранилища**
Данные о блокированных хостах	*(не мигрирует)* Kaspersky Endpoint Security отправляет данные о блокированных хостах автоматически.

Задачи

Активация программы

Kaspersky Endpoint Security не поддерживает работу задачи *Активация программы* (KSWS). Вы можете создать задачу *Добавление ключа* (KES), добавить лицензионный ключ в инсталляционный пакет или включить автоматическое распространение лицензионного ключа.

Копирование обновлений

Параметры задачи *Копирование обновлений* (KSWS) мигрируют в задачу *Обновление баз и модулей приложения* (KES).

Параметры задачи копирования обновлений

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Источник обновлений: • **Сервер администрирования Kaspersky Security Center**; • **Серверы обновлений "Лаборатории Касперского"**; • **Другие HTTP-, FTP-серверы или сетевые ресурсы**.	**Источник обновлений**: • **Kaspersky Security Center**; • **Серверы обновлений "Лаборатории Касперского"**; • **Заданы пользователем**.
Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны	*(не мигрирует)* Kaspersky Endpoint Security позволяет выбрать несколько источников обновлений, включая серверы обновлений "Лаборатории Касперского". Если первый источник обновлений не доступен, Kaspersky Endpoint Security позволяет получить обновления от другого источника из списка.
Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"	*(не мигрирует)* Kaspersky Endpoint Security использует прокси-сервер для работы всех компонентов. Вы можете настроить подключение к прокси-серверу в параметрах сети программы.
Использовать параметры прокси-сервера для соединения с другими серверами	*(не мигрирует)* Kaspersky Endpoint Security использует прокси-сервер для работы всех компонентов. Вы можете настроить подключение к прокси-серверу в параметрах сети программы.
Параметры копирования обновлений: • **Копировать обновления баз программы** • **Копировать критические обновления модулей программы** • **Копировать обновления баз программы и критические обновления модулей программы**	*(не мигрирует)* Kaspersky Endpoint Security копирует обновления баз и критические обновления модулей приложений в составе одного пакета.
Папка для локального хранения скопированных обновлений	**Копировать обновления в папку**

Мониторинг целостности файлов на основе эталона

Параметры задачи *Мониторинг целостности файлов на основе эталона* мигрируют в задачу *Проверка целостности системы* и в политику в раздел **Контроль безопасности**, подраздел **Контроль целостности системы**.

Параметры задачи мониторинга целостности файлов на основе эталона

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Алгоритм расчета контрольных сумм: • **MD5**; • **SHA256**.	*(не мигрирует)* Kaspersky Endpoint Security использует алгоритм SHA256 для расчета контрольной суммы.
Область проверки	**Область мониторинга** (подраздел **Контроль целостности системы**)

Обновление баз программы

Параметры задачи *Обновление баз программы* (KSWS) мигрируют в задачу *Обновление баз и модулей приложения* (KES).

Параметры задачи обновления баз программы

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Источник обновлений: • **Сервер администрирования Kaspersky Security Center**; • **Серверы обновлений "Лаборатории Касперского"**; • **Другие HTTP-, FTP-серверы или сетевые ресурсы**.	**Источник обновлений**: • **Kaspersky Security Center**; • **Серверы обновлений "Лаборатории Касперского"**; • **Заданы пользователем**.
Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны	*(не мигрирует)* Kaspersky Endpoint Security позволяет выбрать несколько источников обновлений, включая серверы обновлений "Лаборатории Касперского". Если первый источник обновлений не доступен, Kaspersky Endpoint Security позволяет получить обновления от другого источника из списка.
Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"	*(не мигрирует)* Kaspersky Endpoint Security использует прокси-сервер для работы всех компонентов. Вы можете настроить подключение к прокси-серверу в параметрах сети приложения.
Использовать параметры прокси-сервера для соединения с другими серверами	*(не мигрирует)* Kaspersky Endpoint Security использует прокси-сервер для работы всех компонентов. Вы можете настроить подключение к прокси-серверу в параметрах сети приложения.
Снизить нагрузку на дисковую подсистему	*(не мигрирует)*

Обновление модулей программы

Параметры задачи *Обновление модулей программы* (KSWS) мигрируют в задачу *Обновление баз и модулей приложения* (KES).

Параметры задачи обновления модулей программы

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Источник обновлений: • **Сервер администрирования Kaspersky Security Center**; • **Серверы обновлений "Лаборатории Касперского"**; • **Другие HTTP-, FTP-серверы или сетевые ресурсы**.	**Источник обновлений**: • **Kaspersky Security Center**; • **Серверы обновлений "Лаборатории Касперского"**; • **Заданы пользователем**.
Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны	*(не мигрирует)* Kaspersky Endpoint Security позволяет выбрать несколько источников обновлений, включая серверы обновлений "Лаборатории Касперского". Если первый источник обновлений не доступен, Kaspersky Endpoint Security позволяет получить обновления от другого источника из списка.

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"	*(не мигрирует)* Kaspersky Endpoint Security использует прокси-сервер для работы всех компонентов. Вы можете настроить подключение к прокси-серверу в параметрах сети программы.
Использовать параметры прокси-сервера для соединения с другими серверами	*(не мигрирует)* Kaspersky Endpoint Security использует прокси-сервер для работы всех компонентов. Вы можете настроить подключение к прокси-серверу в параметрах сети программы.
Копировать и устанавливать критические обновления модулей программы	**Устанавливать критические и одобренные обновления**
Только проверять наличие доступных критических обновлений модулей программы	*(не мигрирует)* Kaspersky Endpoint Security проверяет наличие доступных критических обновлений модулей приложений постоянно.
Разрешать перезагрузку операционной системы	*(не мигрирует)* Kaspersky Endpoint Security запрашивает у пользователя разрешение на перезагрузку компьютера.
Получать информацию о доступных плановых обновлениях модулей программы	*(не мигрирует)* Kaspersky Endpoint Security показывает уведомления об обновлениях программных модулей.

Откат обновления баз программы

Параметры задачи *Откат обновления баз программы* (KSWS) мигрируют в задачу *Откат обновления* (KES). Новая задача *Откат обновления* (KES) имеет расписание запуска задачи – *Вручную*.

Проверка по требованию

Параметры задачи *Проверка по требованию* (KSWS) мигрируют в задачу *Поиск вредоносного ПО* (KES).

Параметры задачи антивирусной проверки

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Область проверки	**Область проверки**
Уровень безопасности: • **Максимальная защита**; • **Рекомендуемый**; • **Максимальное быстродействие**.	**Уровень безопасности**: • **Высокий**; • **Рекомендуемый**; • **Низкий**. Параметры уровней безопасности KSWS и KES отличаются.
Объекты проверки: • **Все объекты**; • **Объекты, проверяемые по формату**; • **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**; • **Объекты, проверяемые по указанному списку расширений**.	**Типы файлов**: • **Все файлы**; • **Файлы, проверяемые по формату**; • **Файлы, проверяемые по расширению**. Kaspersky Endpoint Security не позволяет создавать пользовательские списки расширений. Вместо значения **Объекты, проверяемые по указанному списку расширений** Kaspersky Endpoint Security установит значение **Файлы, проверяемые по расширению**.
Вложенные папки	**Включить вложенные папки**
Вложенные файлы	*(не мигрирует)*
Загрузочные секторы дисков и MBR	*(не мигрирует)*
Альтернативные потоки NTFS	*(не мигрирует)*
Проверка только новых и измененных файлов	**Проверять только новые и измененные файлы**
Проверка составных объектов: • **Все архивы**; • **Все SFX-архивы**; • **Все почтовые базы**; • **Все упакованные объекты**; • **Все файлы почтовых форматов**; • **Все вложенные OLE-объекты**.	**Проверка составных файлов**: • **Проверять архивы**; • **Проверять архивы, защищенные паролем**; • **Проверять дистрибутивы**; • **Проверять файлы почтовых форматов**; • **Проверять файлы офисных форматов**.

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Действия над зараженными и другими обнаруженными объектами: • **Лечить**; • **Лечить. Удалять, если не удалось**; • **Удалять**; • **Выполнять рекомендуемое действие**; • **Только сообщать**.	**Действие при обнаружении угрозы**: • **Лечить. Удалять, если лечение невозможно**; • **Лечить. Информировать, если лечение невозможно**; • **Информировать**.
Действия над возможно зараженными объектами: • **Помещать на карантин**; • **Удалять**; • **Выполнять рекомендуемое действие**; • **Только сообщать**.	*(не мигрирует)* Kaspersky Endpoint Security применяет действие при обнаружении любой угрозы.
Выполнять действия в зависимости от типа обнаруженного объекта	*(не мигрирует)*
Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой	*(не мигрирует)*
Исключать файлы	*(не мигрирует)* Kaspersky Endpoint Security применяет доверенную зону для всех компонентов. Вы можете настроить исключения в параметрах доверенной зоны.
Не обнаруживать	*(не мигрирует)*
Останавливать проверку, если она длится более N сек	**Пропускать файлы, если их проверка длится более N сек**
Не проверять составные объекты размером более N МБ	**Не распаковывать составные файлы большого размера**
Использовать технологию iSwift	**Технология iSwift**
Использовать технологию iChecker	**Технология iChecker**
Действия над автономными файлами: • **Не проверять**; • **Проверять только резидентную часть файла**; • **Проверять файл полностью**; • **Только если к файлу производилось обращение в указанный период (сут)**; • **Не копировать файл на локальный жесткий диск, если возможно**.	*(не мигрирует)* Kaspersky Endpoint Security проверяет автономные файлы полностью.

Проверка целостности программы

Параметры задачи *Проверка целостности программы* (KSWS) мигрируют в задачу *Проверка целостности приложения* (KES).

Формирование правил контроля запуска программ

Kaspersky Endpoint Security не поддерживает работу задачи *Формирование правил контроля запуска программ*. Вы можете сформировать правила в параметрах Контроля программ.

Формирование правил контроля устройств

Kaspersky Endpoint Security не поддерживает работу задачи *Формирование правил контроля устройств*. Вы можете сформировать правила доступа в параметрах Контроля устройств.

Миграция компонентов KSWS

Перед локальной установкой Kaspersky Endpoint Security проверяет компьютер на наличие приложений "Лаборатории Касперского". Если на компьютере установлено приложение Kaspersky Security для Windows Server, KES определит набор компонентов KSWS, которые были установлены, и выбирает те же компоненты при установке.

Компоненты KES, которых нет в KSWS, будут установлены следующим образом:

- AMSI-защита, Предотвращение вторжений, Откат вредоносных действий – устанавливаются с параметрами по умолчанию.
- Защита от атак BadUSB, Адаптивный контроль аномалий, Шифрование данных, компоненты Detection and Response – игнорируются.

При дистанционной установке приложение KES игнорирует набор установленных компонентов KSWS. Инсталлятор устанавливает компоненты, которые вы выбрали в свойствах инсталляционного пакета. После установки Kaspersky Endpoint Security и миграции политик и задач параметры KES будут настроены в соответствии с параметрами KSWS.

Миграция политик и задач KSWS

Вы можете перенести параметры политик и задач KSWS следующими способами:

- С помощью мастера массовой конвертации политик и задач (далее также "мастер миграции").

  > Мастер миграции для KSWS доступен только в Консоли администрирования (MMC). Перенести параметры политик и задач в Web Console и Cloud Console невозможно.

  Работа мастера массовой конвертации для разных версий Kaspersky Security Center отличается. Рекомендуем обновить версию решения до 14.2 или выше. В этой версии Kaspersky Security Center мастер массовой конвертации политик и задач позволяет перенести политики в профиль, а не в политику. Также в этой версии Kaspersky Security Center мастер массовой конвертации политики и задач позволяет перенести больше параметров политики.

- С помощью мастера создания новой политики Kaspersky Endpoint Security для Windows.

  Мастер создания политики позволяет создать политику KES на основании политики KSWS.

Миграция политик KSWS с помощью мастера миграции и мастера создания политики отличается.

Мастер массовой конвертации политик и задач

Мастер миграции переносит параметры политики KSWS в профиль политики, а не в параметры политики KES. *Профиль политики* – это набор параметров политики, который активируется на компьютере, если компьютер удовлетворяет заданным правилам активации. В качестве условия срабатывания профиля политики выбран тег устройства `UpgradedFromKSWS`. Kaspersky Security Center автоматически добавляет тег `UpgradedFromKSWS` для всех компьютеров, на которых вы установили KES поверх KSWS с помощью задачи дистанционной установки. Если вы выбрали другой способ установки, вы можете вручную назначить тег устройствам.

Для добавления тега устройству вам нужно выполнить следующие действия:

1. Создайте новый тег для серверов – `UpgradedFromKSWS`.

   Подробнее о создании тегов для устройств см. в справке Kaspersky Security Center.

2. Создайте новую группу администрирования в консоли Kaspersky Security Center и добавьте в группу серверы, для которых вы хотите назначить тег.

   Для группировки серверов вы можете использовать инструмент выборки. Подробнее о работе с выборками см. в справке Kaspersky Security Center.

3. Выделите все серверы в группе администрирования в консоли Kaspersky Security Center, откройте свойства выделенных серверов и назначьте тег.

Если вы переносите несколько политик KSWS, то каждая политика будет сконвертирована в профиль внутри одной политики. Также, если политика KSWS уже содержит профили, эти профили также мигрируют в виде профилей. В результате вы получите одну политику, в которую включены соответствующие профили для всех политик KSWS.

Как перенести параметры политик KSWS с помощью мастера массовой конвертации политик и задач

1. В Консоли администрирования выберите Сервер администрирования и по правой клавише мыши откройте контекстное меню.

2. Выберите пункт **Все задачи** → **Мастер массовой конвертации политик и задач**.

В результате запустится мастер массовой конвертации политик и задач. Следуйте его указаниям.

Шаг 1. Выбор приложения, для которого нужно конвертировать политики и задачи

На этом шаге нужно выбрать приложение Kaspersky Endpoint Security для Windows. Перейдите к следующему шагу.

Шаг 2. Конвертация политик

Мастер миграции создает профили политики KSWS внутри политики KES. Выберите политики Kaspersky Security для Windows Server, которые вы хотите конвертировать в профили политики. Перейдите к следующему шагу.

Далее мастер миграции начнет конвертацию политик. Новые профили политик будут иметь имена соответствующие исходным политикам KSWS.

Шаг 3. Отчет о миграции политик

Мастер миграции создает отчет о миграции политик. Отчет о миграции политик содержит дату и время конвертации политик, имя исходной политики KSWS, имя целевой политики KES и имя нового профиля политики.

Шаг 4. Конвертация задач

Мастер миграции создает новые задачи для Kaspersky Endpoint Security для Windows. В списке задач выберите задачи KSWS, которые вы хотите создать для Kaspersky Endpoint Security. Новые задачи будут иметь имя *<Название задачи KSWS> (конвертированная)*. Перейдите к следующему шагу.

Шаг 5. Завершение работы мастера

Завершите работу мастера. В результате работы мастера будут выполнены следующие действия:

- В политику Kaspersky Endpoint Security добавлены новые профили политик.

  Политика включает профили с параметрами Kaspersky Security для Windows Server. Новая политика имеет статус *Активна*. При этом мастер оставляет политики KSWS без изменений.

- Созданы новые задачи Kaspersky Endpoint Security.

  Новые задачи представляют собой копии задач KSWS. При этом мастер оставляет задачи KSWS без изменений.

Новый профиль политики с параметрами KSWS будет иметь имя *UpgradedFromKSWS <Название политики Kaspersky Security для Windows Server>*. В свойствах профиля в качестве условия срабатывания мастер миграции автоматически выбирает тег устройства `UpgradedFromKSWS`. Таким образом, параметры из профиля политики будут применены на серверы автоматически.

Мастер создания политики на основании политики KSWS

При создании политики KES на основании политики KSWS мастер переносит параметры в политику соответственно. То есть одной политике KSWS будет соответствовать одна политика KES. Мастер не конвертирует политику в профиль.

Как перенести параметры политики KSWS с помощью мастера создания политик

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят интересующие вас клиентские компьютеры.

3. В рабочей области выберите вкладку **Политики**.

4. Нажмите на кнопку **Новая политика**.

   Запустится мастер создания политики.

5. Следуйте указаниям мастера создания политики.

Шаг 1. Выбор приложения для создания групповой политики

Выберите приложение **Kaspersky Endpoint Security для Windows (14.3)**.

Шаг 2. Определение названия для групповой политики

Введите имя групповой политики, например, *Политика для офиса*.

Установите флажок **Использовать параметры политики для предыдущей версии приложения**. Нажмите на кнопку **Обзор** и выберите политику KSWS.

Шаг 3. Участие в Kaspersky Security Network

Прочитайте и примите условия Положения о Kaspersky Security Network (KSN).

Шаг 4. Выбор режима использования приложения на компьютерах

Выберите **Стандартный режим для защиты устройств**. Kaspersky Endpoint Security предоставляет единую политику для всех режимов использования приложения и типов ОС.

> Рекомендуется использовать разные политики для разных режимов использования и разных типов операционных систем.

Шаг 5. Импорт настроек

> Этот шаг доступен, если на шаге 4 вы выбрали настройку параметров политики вручную.

Вы можете создать политику на основе параметров Kaspersky Endpoint Security из конфигурационного файла CFG. Мастер создания политики не поддерживает зашифрованные конфигурационные файлы. При экспорте конфигурационного файла пропустите шаг шифрования файла.

При импорте конфигурационного файла CFG приложения мастеру доступны не все параметры политики. Например, в параметрах приложения отсутствуют профили политики. Если вы хотите перенести в политику все параметры и профили, вы можете использовать импорт другой политики из KLP-файла.

При импорте конфигурационного файла Kaspersky Endpoint Security не переносит пароли криптоконтейнеров. Если вы используете двустороннюю аутентификацию для подключения к серверам, вам нужно заново указать пароли к криптоконтейнерам.

Шаг 6 - 10. Настройка параметров политики

Этот шаг доступен, если на шаге 4 вы выбрали настройку параметров политики вручную.

Настройте параметры политики по шагам.

Шаг 11. Настройка доверенной зоны

Настройте доверенную зону. Вы можете добавить предустановленные исключения из проверки и доверенные приложения. Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах. Также предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в режиме Легкого агента в виртуальных средах Citrix и VMware.

Шаг 12. Выбор состояния политики

- **Активна**. После следующей синхронизации политика будет использоваться на компьютере в качестве действующей.

  Параметры активной политики во время синхронизации сохраняются на клиентских компьютерах. К одному компьютеру нельзя одновременно применить несколько политик, поэтому в каждой группе активной может быть только одна политика.

- **Неактивна**. Резервная политика. При необходимости неактивную политику можно сделать активной.

  Вы можете создать неограниченное количество неактивных политик. Неактивная политика не влияет на параметры приложения на компьютерах в сети. Неактивные политики предназначены для подготовки к нештатным ситуациям, например, в случае вирусной атаки. В случае атаки через флеш-накопители вы можете активировать политику, блокирующую доступ к флеш-накопителям. При этом активная политика автоматически становится неактивной.

- **Для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организации.

Завершите работу мастера.

Дополнительная настройка политик и задач после миграции

Так как состав компонентов и набор параметров политики KSWS и KES отличаются, после миграции вам нужно проверить параметры политики на соответствие требованиям корпоративной безопасности.

Проверьте следующие основные параметры политики:

- Защита паролем. Параметры Защиты паролем KSWS не мигрируют. Kaspersky Endpoint Security имеет собственную функцию Защита паролем. Если требуется, включите Защиту паролем и задайте пароль.

- Доверенная зона. Способы выбора объектов в KSWS и KES отличаются. При миграции KES поддерживает исключения, заданные в виде отдельных файлов или пути к файлу / папке. Если в KSWS есть исключения, заданные в виде предопределенной области или веб-адреса скрипта, такие исключения не мигрируют. После миграции вам нужно добавить эти исключения вручную.

  > Для корректной работы Kaspersky Endpoint Security на серверах рекомендуется добавить в доверенную зону файлы, важные для выполнения сервером своих функций. Для SQL-серверов вам нужно добавить файлы баз данных MDF и LDF. Для Microsoft Exchange-серверов вам нужно добавить файлы CHK, EDB, JRS, LOG и JSL. Вы можете использовать маски, например, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

  > Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах.

- Сетевой экран. Функции Сетевого экрана KSWS выполняет системный Сетевой экран. В KES функции Сетевого экрана выполняет отдельный компонент. После миграции вы можете настроить Сетевой экран Kaspersky Endpoint Security.

- Kaspersky Security Network. Kaspersky Endpoint Security не поддерживает настройку использования KSN для отдельных компонентов. Kaspersky Endpoint Security использует KSN для всех компонентов приложения. Для использования KSN вам нужно принять новые условия Положения о Kaspersky Security Network.

- Веб-Контроль. Запрещающие правила категоризации веб-ресурсов мигрируют в Kaspersky Endpoint Security в одно запрещающее правило. Kaspersky Endpoint Security игнорирует разрешающие правила категоризации. Kaspersky Endpoint Security поддерживает не все категории Kaspersky Security для Windows Server. Категории, которых нет в Kaspersky Endpoint Security, не мигрируют. Таким образом, правила категоризации веб-ресурсов с неподдерживаемыми категориями не мигрируют. Если требуется, добавьте правила Веб-Контроля.

- Прокси-сервер. Пароль для подключения к прокси-серверу не мигрирует. Введите пароль для подключения к прокси-серверу вручную.

- Расписание работы отдельных компонентов. Kaspersky Endpoint Security не поддерживает настройку расписания работы отдельных компонентов. Компоненты включены постоянно пока работает Kaspersky Endpoint Security.

- Состав компонентов. Набор доступных функций Kaspersky Endpoint Security зависит от типа операционной системы: рабочая станция или сервер. Например, из инструментов шифрования на серверах доступно только Шифрование диска BitLocker.

- Атрибут . Состояние атрибута не мигрирует. Атрибут будет иметь значение по умолчанию. По умолчанию почти на все параметры в новой политике наложен запрет на изменение параметров в дочерних политиках и локальном интерфейсе приложения. Атрибут имеет значение для параметров политики в разделе **Managed Detection and Response (Industrial CyberSecurity)** и в блоке **Поддержка пользователей** (раздел **Интерфейс**). Если требуется, настройте наследование параметров из родительской политики.

- Работа с активными угрозами. Лечение активного заражения для рабочих станций и серверов отличается. Вы можете настроить лечение активного заражения в свойствах задачи *Поиск вредоносного ПО* и в параметрах приложения.

- Обновление приложения. Для установки основных (major) обновлений и патчей без перезагрузки вам нужно изменить режим обновления приложения. По умолчанию функция обновления приложения без перезагрузки выключена.

- Kaspersky Endpoint Agent. Kaspersky Endpoint Security имеет встроенный агент для работы с решениями Detection and Response. Если требуется, перенесите параметры политики Kaspersky Endpoint Agent в политику Kaspersky Endpoint Security.

- Задачи *Обновление баз и модулей приложения*. Убедитесь, что параметры задачи *Обновление баз и модулей приложения* мигрировали корректно. Вместо трех задач KSWS в KES используется одна задача KES. Вы можете оптимизировать задачи *Обновление баз и модулей приложения* и удалить лишние задачи.

- Другие задачи. Работа компонентов Контроль приложений, Контроль устройств и Мониторинг файловых операций в KSWS и KES отличаются. KES не использует задачи *Мониторинг целостности файлов на основе эталона*, *Формирование правил контроля запуска программ*, *Формирование правил контроля устройств*. Таким образом, эти задачи не мигрируют. После миграции вы можете настроить параметры компонентов Мониторинг файловых операций, Контроль приложений, Контроль устройств.

Миграция доверенной зоны KSWS

Доверенная зона – это сформированный администратором системы список объектов и приложений, которые Kaspersky Endpoint Security не контролирует в процессе работы. Вы можете перенести объекты доверенной зоны из KSWS в KES с помощью *мастера массовой конвертации политик и задач* или *мастера создания новой политики KES на основании политики KSWS*. Так как состав компонентов и набор функций KSWS и KES отличаются, после миграции вам нужно проверить работу исключений на соответствие требованиям корпоративной безопасности. Также отличаются способы добавления исключений в доверенную зону для KES и KSWS. У мастера миграции нет инструментов для переноса всех исключений KSWS. Поэтому некоторые исключения KSWS после миграции вам нужно добавить вручную.

Для корректной работы Kaspersky Endpoint Security на серверах рекомендуется добавить в доверенную зону файлы, важные для выполнения сервером своих функций. Для SQL-серверов вам нужно добавить файлы баз данных MDF и LDF. Для Microsoft Exchange-серверов вам нужно добавить файлы CHK, EDB, JRS, LOG и JSL. Вы можете использовать маски, например, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах.

Способы формирования доверенной зоны KES и KSWS

KSWS		KES
Проверяемый объект		
• Предопределенная область	*(не мигрирует)*	
• Диск, папка или сетевой объект	→	**Файл или папка**
• Файл	→	**Файл или папка**
• Файл или веб-адрес скрипта	*(не мигрирует)*	
Обнаруживаемый объект	→	**Тип обнаруживаемого объекта**
Доверенные процессы	→	**Доверенные приложения**

Миграция проверяемых объектов

Исключения KSWS, в свойствах которых выбран способ **Проверяемый объект**, мигрируют в исключения KES, в свойствах которых выбран способ **Файл или папка**, с ограничениями. Перенос исключения зависит от способа выбора объекта:

- Предопределенная область – *не мигрирует*.

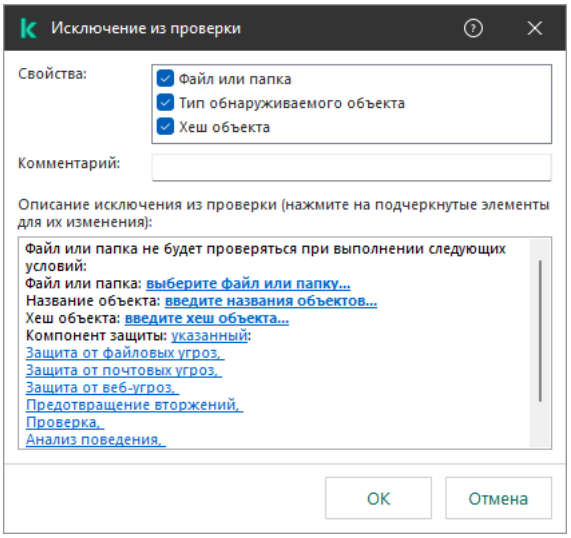
  После миграции вам нужно добавить эти исключения вручную. Исключения в виде предопределенной области нужно настроить в свойствах задачи *Поиск вредоносного ПО*.

- Диск, папка или сетевой объект – мигрируют в исключения KES, в свойствах которых выбран способ Файл или папка.

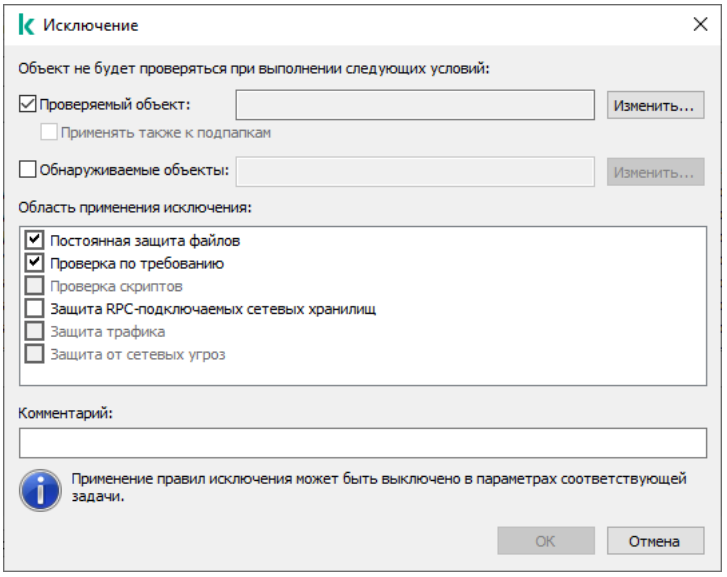
- Файл – мигрируют в исключения KES, в свойствах которых выбран способ Файл или папка.
- Файл или веб-адрес скрипта – *не мигрирует*.

  После миграции вам нужно добавить эти исключения вручную. Исключения в виде веб-адреса скрипта нужно добавить в доверенные веб-адреса для Защиты от веб-угроз.

Если для проверяемого объекта установлен флажок **Применять также к подпапкам**, этот параметр мигрирует в исключения KES (флажок **Включить вложенные папки**).



Параметры исключений KES



Параметры исключений KSWS

Миграция обнаруживаемых объектов

Исключения KSWS, в свойствах которых выбран способ **Обнаруживаемый объект**, мигрируют в исключения KES, в свойствах которых выбран способ **Тип обнаруживаемого объекта**. Имя обнаруживаемого объекта соответствует классификации Энциклопедии "Лаборатории Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`). Kaspersky Endpoint Security поддерживает маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов).

Миграция области применения исключения

Область применения исключения представляет собой набор компонентов, на которые распространяется исключение. Так как наборы компонентов KES и KSWS отличаются, мастер миграции не может перенести область исключений. Поэтому если в области исключений KSWS выбран хотя бы один компонент, KES применяет исключение для всех компонентов приложения.

Вы можете настроить область применения исключения KSWS не только в свойствах доверенной зоны, но и в параметрах компонентов защиты KSWS. Для этого в соответствующем разделе политики предусмотрен флажок **Применять доверенную зону**. В параметрах компонентов защиты KES такого флажка нет. То есть при миграции статус доверенной зоны в параметрах отдельного компонента будет утерян. После миграции выберите компоненты, на которые распространяется исключение, в параметрах доверенной зоны в политике KES.

Миграция комментариев

Комментарии из доверенной зоны KSWS мигрируют в комментарии исключений KES без изменений.

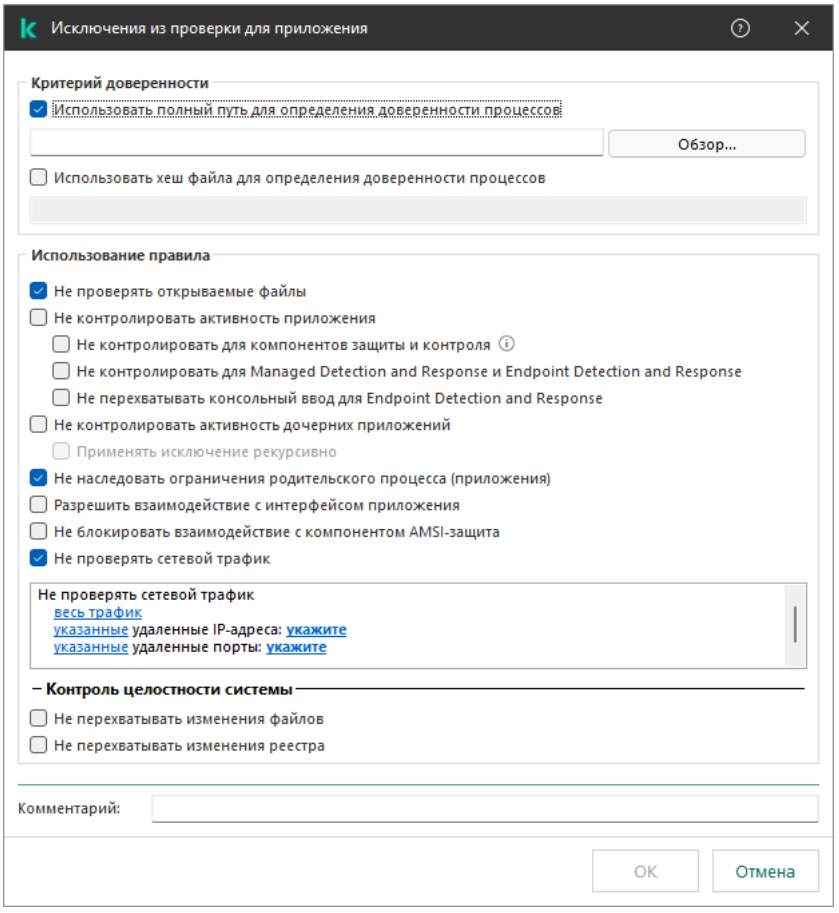
Миграция доверенных процессов

Доверенные процессы KSWS мигрируют в доверенные приложения KES с ограничениями. Перенос доверенных процессов зависит от способа выбора объекта:

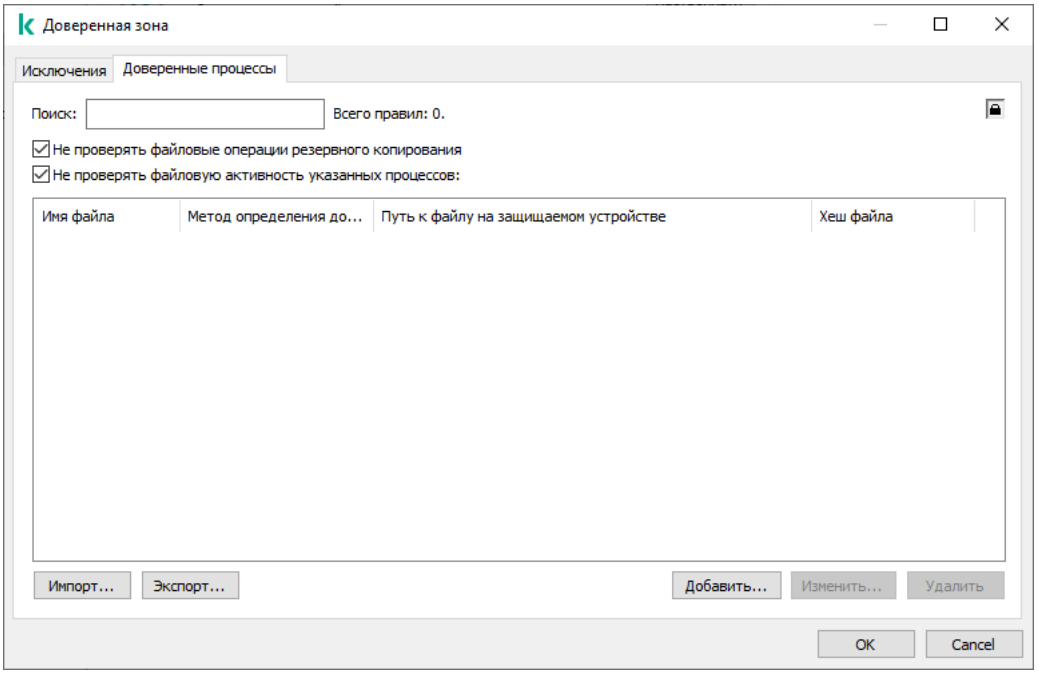
- Путь к файлу на защищаемом устройстве – мигрируют в доверенные приложения KES.
- Хеш файла – *не мигрирует*.

Если в KSWS есть доверенные процессы, заданные в виде хеша файла, такие доверенные процессы не мигрируют. После миграции вам нужно добавить эти доверенные процессы вручную.

Если в параметрах доверенных процессов установлен флажок **Не проверять файловые операции резервного копирования**, этот параметр мигрирует в доверенные приложения KES (флажок **Не контролировать активность приложения**).



Параметры доверенного приложения KES



Параметры доверенного процесса KSWS

Миграция правил Контроля запуска программ KSWS

Контроль запуска программ KSWS работает по принципу запрета по умолчанию. То есть Контроль запуска программ автоматически блокирует все приложения, не указанные в правилах в качестве разрешенных. Поэтому мастер миграции для Контроля приложений KES автоматически устанавливает режим контроля **Список разрешенных**, который соответствует принципу запрета по умолчанию.

Вы можете перенести правила из KSWS в KES с помощью *мастера массовой конвертации политик и задач* или *мастера создания новой политики KES на основании политики KSWS*.

Миграция режима работы Контроля запуска программ

Режим работы Контроль запуска программ KSWS мигрирует в Контроль приложений KES следующим образом:

- **Только статистика** → **Тестировать правила**;
- **Активный** → **Применять правила**.

Миграция предустановленных правил Контроля запуска программ KSWS

По умолчанию Контроль запуска программ KSWS включает в себя два правила:

- **Разрешать к запуску скрипты и пакеты MSI, доверенные в ОС по сертификату**.
- **Разрешать к запуску исполняемые файлы, доверенные в ОС по сертификату**.

Предустановленные правила разрешают запуск *скриптов*, *пакетов MSI* и *исполняемых файлов*, подписанных доверенным корневым сертификатом. Если хотя бы одно предустановленное правило KSWS имеет тип **Разрешающее**, мастер миграции создает новое разрешающее правило **Приложения с доверенными корневыми сертификатами**. То есть, Контроль приложений KES разрешает запуск доверенных скриптов, пакетов MSI и исполняемых файлов с помощью одного правила.

Если оба предустановленных правила KSWS имеют тип **Запрещающее**, KES игнорирует предустановленные правила.

Миграция пользовательских правил Контроля запуска программ KSWS

Правила Контроля запуска программ KSWS регулируют запуск файлов по следующим критериям:

- подпись цифровым сертификатом;
- SHA256-хеш;
- путь к файлу.

Так как способ формирования правил в KSWS и KES отличается, мастер миграции создает *категории приложений*, включающие условия и исключения из правил KSWS, и добавляет эти категории приложений в правила KES. Мастер использует в категориях приложений условия **Сертификат**, **Путь к папке** и **Хеш файла**. Новые категории приложений доступны в Консоли администрирования Kaspersky Security Center в разделе **Управление приложениями → Категории приложений**.

Мастер миграции группирует правила KSWS по типу и пользователям. Далее мастер создает категории приложений, включающие в себя условия и исключения из правил KSWS, и добавляет категории приложений в новые правила KES. Названия правил KSWS мастер миграции указывает в поле **Описание** правила KES.

Миграция дополнительных параметров Контроля запуска программ KSWS

Так как работа Контроля запуска программ KSWS и Контроля приложений KES отличается, мастер миграции может перенести ограниченное количество параметров.

Параметры Контроля запуска программ

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска	*(не мигрирует)* Kaspersky Endpoint Security проверяет программу при каждой попытке ее запуска.
Запрещать запуск командных интерпретаторов без команды к исполнению	*(не мигрирует)* Kaspersky Endpoint Security разрешает запуск командных интерпретаторов, если их запуск не запрещен правилами Контроля программ.
Использовать правила для исполняемых файлов	*(не мигрирует)* Задать область применения правил в параметрах Контроля приложений KES невозможно. Контроль приложений KES применяет правила ко всем типам файлов: исполнительные файлы, скрипты и пакеты MSI. Если в KSWS в область применения правил включены все типы файлов, при миграции KES переносит правила KSWS. Если в KSWS из области применения правила исключен какой-то тип файлов, при миграции KES также переносит правила KSWS, но в качестве действия Контроля приложений выбирает **Тестировать правила**.
Контролировать загрузку DLL-модулей	**Контролировать загрузку динамических библиотек (значительно увеличивает нагрузку на систему)**
Использовать правила для скриптов и пакетов MSI	*(не мигрирует)* Задать область применения правил в параметрах Контроля приложений KES невозможно. Контроль приложений KES применяет правила ко всем типам файлов: исполнительные файлы, скрипты и пакеты MSI. Если в KSWS в область применения правил включены все типы файлов, при миграции KES переносит правила KSWS. Если в KSWS из области применения файла исключен какой-то тип файлов, при миграции KES переносит правила KSWS, но в качестве действия Контроля приложений выбирает **Тестировать правила**.

Параметры Kaspersky Security для Windows Server	Параметры Kaspersky Endpoint Security для Windows
Запрещать запуск программ, недоверенных в KSN	*(не мигрирует)* Kaspersky Endpoint Security не учитывает репутацию программ и разрешает или запрещает запуск программ в соответствии с правилами.
Разрешать запуск программ, доверенных в KSN	При миграции KES добавляет новое разрешающее правило. В качестве условия срабатывания правила указана KL-категория **Другие приложения\Приложения, доверенные согласно репутации в KSN**.
Пользователи и / или группы пользователей, которым разрешен запуск доверенных в KSN программ	**Пользователи и их права** в разрешающем правиле Контроля приложений, в которое включена KL-категория **Другие приложения\Приложения, доверенные согласно репутации в KSN**.
Автоматически разрешать распространение с помощью указанных программ и пакетов установки	Контроль пакетов установки KSWS и KES отличается. При миграции KES добавляет новые разрешающие правила с приложениями, для которых разрешено автоматическое распространение ПО. В качестве условия срабатывания правила указан хеш файла.
Всегда разрешать распространение программ с помощью установщика Windows	Контроль пакетов установки KSWS и KES отличается. При миграции KES добавляет новые разрешающие правила с приложениями, для которых разрешено автоматическое распространение ПО (**Список программ и пакетов установки, разрешенных к запуску**). В качестве условия срабатывания правила указан хеш файла. В свойствах правила установлен флажок **Доверенные приложения обновления**.
Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи	*(не мигрирует)*
Список программ и пакетов установки, разрешенных к запуску	Контроль пакетов установки KSWS и KES отличается. При миграции KES добавляет новые разрешающие правила с приложениями, для которых разрешено автоматическое распространение ПО. В качестве условия срабатывания правила указан хеш файла. В свойствах правила установлен флажок **Доверенные приложения обновления**.
Параметры расписания	*(не мигрирует)* Если в параметрах KSWS настроено расписание работы компонента, при миграции компонент Контроль приложений будет включен. Если расписание работы компонента не настроено, Контроль приложений будет выключен. Настроить отдельное расписание работы для компонента невозможно. Компонент включен постоянно пока работает Kaspersky Endpoint Security.

Установка KES вместо KSWS

Вы можете установить Kaspersky Endpoint Security следующими способами:

- Установка KES после удаления KSWS (рекомендуется).
- Установка KES поверх KSWS.

Удаление Kaspersky Security для Windows Server

Вы можете удалить приложение дистанционно с помощью задачи *Удаленная деинсталляция приложения* или локально на сервере. После удаления KSWS может потребоваться перезагрузка сервера. Если вы хотите установить Kaspersky Endpoint Security без перезагрузки, рекомендуется убедиться, что приложение Kaspersky Security для Windows Server удалено полностью. Если приложение удалено не полностью, после установки Kaspersky Endpoint Security могут возникнуть сбои в работе сервера. Также рекомендуется убедиться, что приложение удалено полностью, если вы использовали утилиту kavremover. Утилита kavremover не поддерживает работу с KSWS.

Если для ограничения доступа к KSWS включена Защита паролем, введите пароль деинсталляции в параметрах инсталляционного пакета KES.

После удаления KSWS установите приложение Kaspersky Endpoint Security для Windows любым доступным образом.

Установка Kaspersky Endpoint Security

При дистанционной установке KES на сервер будут установлены компоненты, которые вы выбрали в свойствах инсталляционного пакета. Рекомендуем в свойствах инсталляционного пакета выбрать компоненты по умолчанию. При установке KES поверх KSWS перезагрузка не требуется.

Перед локальной установкой Kaspersky Endpoint Security проверяет компьютер на наличие приложений "Лаборатории Касперского". Если на компьютере установлено приложение Kaspersky Security для Windows Server, KES определит набор компонентов KSWS, которые были установлены, и выбирает те же компоненты при установке. При установке KES поверх KSWS перезагрузка не требуется.

Если установка KES поверх KSWS не удалась, вы можете откатить установку. После отката установки рекомендуется перезагрузить сервер и повторить попытку.

Параметры KSWS и задачи не мигрируют при установке Kaspersky Endpoint Security для Windows. Для переноса параметров и задач запустите мастер массовой конвертации политик и задач.

Вы можете проверить список установленных компонентов в интерфейсе приложения в разделе **Безопасность**, с помощью команды `status` или в консоли Kaspersky Security Center в свойствах компьютера. Вы можете изменить набор компонентов после установки с помощью задачи *Изменение состава компонентов приложения*.

Миграция конфигурации [KSWS+KEA] на [KES+встроенный агент]

Для работы Kaspersky Endpoint Security для Windows в составе решений EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA и MDR в приложение добавлен встроенный агент. Теперь вам не нужно отдельное приложение Kaspersky Endpoint Agent для работы этих решений.

При миграции с KSWS на KES решения EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA и MDR продолжат работу со встроенными агентами Kaspersky Endpoint Security. Также приложение Kaspersky Endpoint Agent будет удалено с компьютера.

Миграция конфигурации [KSWS+KEA] на [KES+встроенный агент] состоит из следующих этапов:

1. **Миграция с KSWS на KES**

   Миграция с KSWS на KES включает в себя установку Kaspersky Endpoint Security вместо Kaspersky Security для Windows Server.

   Как правило, для ограничения доступа к KSWS и KEA администраторы включают Защиту паролем. Начиная с версии Kaspersky Security Center Linux 15.1 вы можете ввести пароль деинсталляции приложения в параметрах задачи *Удаленная установка приложения*. Задача позволяет ввести только один пароль деинсталляции. То есть, если для KSWS и KEA установлен одинаковый пароль, удаление приложений KSWS и KEA будет выполнено успешно. Если пароли отличаются, то удаление одного из приложений будет завершено с ошибкой доступа. Для миграции вам нужно выключить Защиту паролем для приложения, пароль от которого не удалось ввести в параметрах задачи *Удаленная установка приложения*.

   При миграции вам нужно выбрать соответствующие компоненты для работы решений Detection and Response в составе Kaspersky Endpoint Security. После установки приложения Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent.

2. **Миграция политики и задач**

   Миграция политик и задач из [KSWS+KEA] в [KES+встроенный агент] состоит из следующих этапов:

   1. Миграция политик и задач из KSWS в KES с помощью мастера массовой конвертации политик и задач (доступно только в Консоли администрирования (MMC)).

      В результате в политику KES будет добавлен профиль политики с именем *UpgradedFromKSWS <Название политики Kaspersky Security для Windows Server>*. Также будут созданы новые задачи KES с именем *<Название задачи KSWS> (конвертированная)*.

   2. Миграция политик и задач из KEA в KES с помощью мастера миграции с Kaspersky Endpoint Agent (доступно только в Web Console и Cloud Console).

      В результате будут создана новая политика с именем *<Название политики Kaspersky Endpoint Security> & <Название политики Kaspersky Endpoint Agent>*. Также будут созданы новые задачи и задачи KES.

3. **Лицензирование функций**

Если для активации Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Agent у вас общая лицензия Kaspersky Endpoint Detection and Response Optimum или Kaspersky Optimum Security, после обновления приложения до версии 11.7.0 активация функции EDR Optimum будет выполнена автоматически. Дополнительных действий не требуется.

Если для активации функциональности EDR Optimum у вас отдельная лицензия Kaspersky Endpoint Detection and Response Optimum Add-on, вам нужно убедиться, что ключ EDR Optimum Add-on добавлен в хранилище Kaspersky Security Center и функция автоматического распространения лицензионного ключа включена. После обновления приложения до версии 11.7.0 активация функции EDR Optimum будет выполнена автоматически.

Если для активации Kaspersky Endpoint Agent у вас лицензия Kaspersky Endpoint Detection and Response Optimum или Kaspersky Optimum Security, а для активации Kaspersky Endpoint Security для Windows у вас другая лицензия, вам нужно заменить ключ для Kaspersky Endpoint Security для Windows на общий ключ Kaspersky Endpoint Detection and Response Optimum или Kaspersky Optimum Security. Вы можете заменить ключ с помощью задачи *Добавление ключа*.

Функциональность Kaspersky Sandbox активировать не требуется. Функциональность Kaspersky Sandbox будет доступна сразу после обновления и активации Kaspersky Endpoint Security для Windows.

Для активации Kaspersky Endpoint Security в составе решения Kaspersky Anti Targeted Attack Platform доступна только лицензия Kaspersky Anti Targeted Attack Platform. После обновления приложения до версии 12.1 активация функции EDR (KATA) будет выполнена автоматически. Дополнительных действий не требуется.

4. **Проверка работы Kaspersky Endpoint Detection and Response Optimum и Kaspersky Sandbox**

   Если после обновления приложения компьютер имеет статус *Критический* в консоли Kaspersky Security Center, выполните следующие действия:

   - Убедитесь, что на компьютере установлен Агент администрирования версии 13.2 или выше.
   - Проверьте статус работы встроенного агента с помощью отчета *Отчет о статусе компонентов приложения*. Если компонент имеет статус *Не установлен*, установите компонент с помощью задачи *Изменение состава компонентов приложения*.
   - Убедитесь, что вы приняли условия Положения о Kaspersky Security Network в новой политике Kaspersky Endpoint Security для Windows.

   Убедитесь в том, что функция EDR Optimum активирована с помощью отчета *Отчет о статусе компонентов приложения*. Если компонент имеет статус *Не поддерживается лицензией*, убедитесь, что функция автоматического распространения лицензионного ключа EDR Optimum включена.

Проверка удаления приложения Kaspersky Security для Windows Server

Убедитесь, что приложение Kaspersky Security для Windows Server удалено полностью:

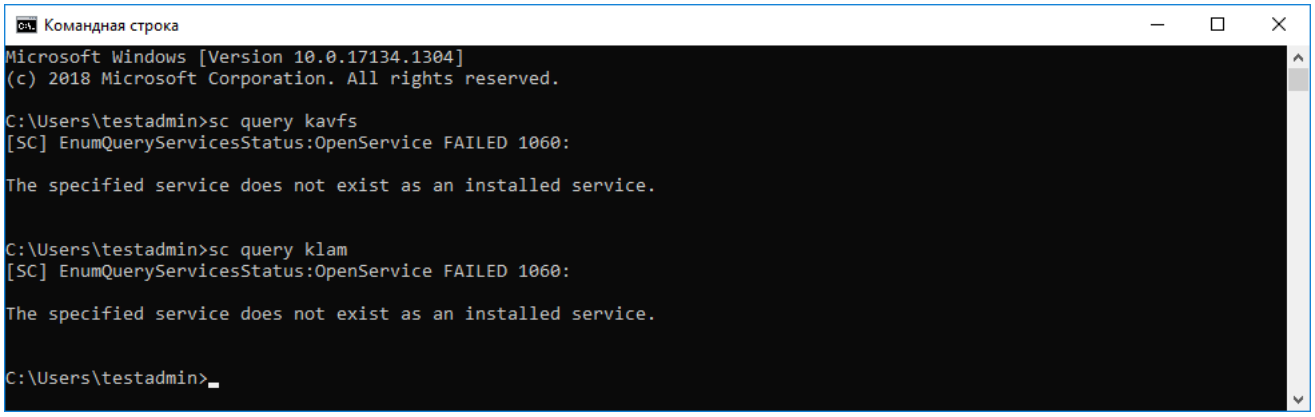
- Отсутствует папка `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\`.
- Отсутствуют службы:
  - Kaspersky Security Service (KAVFS).
  - Служба Kaspersky Security Management (KAVFSGT).

- Служба Kaspersky Security Exploit Prevention (KAVFSSLP).
- Служба Kaspersky Security Script Checker (KAVFSSCS).

Вы можете проверить запущенные службы в Диспетчере задач или с помощью команды `sc query` (см. рис. ниже).

- Отсутствуют драйвера:
  - klam.sys;
  - klflt.sys;
  - klramdisk.sys;
  - klelaml.sys;
  - klfltdev.sys;
  - klips.sys;
  - klids.sys;
  - klwtpee.

Вы можете проверить установленные драйвера в папке `C:\Windows\System32\drivers` или с помощью команды `sc query`. Если служба или драйвер отсутствует, вы получите следующий ответ:



Проверка удаления служб и драйверов Kaspersky Security для Windows Server

Если на сервере остались файлы приложения или драйвера, удалите файлы вручную. Если на сервере остались запущенные службы Kaspersky Security для Windows Server, остановите (`sc stop`) и удалите (`sc delete`) службы вручную. Для остановки драйвера klam.sys используйте команду `fltmc unload klam`.

Активация KES ключом KSWS

После установки приложения вы можете активировать Kaspersky Endpoint Security для Windows (KES) лицензионным ключом Kaspersky Security для Windows Server (KSWS). Активация приложения после миграции отличается в зависимости от способа активации KSWS (см. таблицу ниже).

Kaspersky Endpoint Security не поддерживает лицензию *Kaspersky Security для систем хранения данных*. Для работы с этой лицензией необходимо использовать приложение Kaspersky Security для Windows Server.

Для активации KES ключом KSWS вы можете использовать только код активации. Если вы используете файл ключа для активации приложения, вам нужно обратиться в Службу технической поддержки за файлом ключа Kaspersky Endpoint Security.

Активация Kaspersky Endpoint Security для Windows ключом Kaspersky Security для Windows Server

Способ активации Kaspersky Security для Windows Server	Миграция ключа в Kaspersky Endpoint Security для Windows
Автоматическое распространение лицензионного ключа KSWS на компьютеры.	Если в свойствах лицензионного ключа KSWS включено автоматическое распространение ключа, KES будет автоматически активирован ключом KSWS.
Ключ KSWS добавлен с помощью задачи.	Если вы активировали KSWS с помощью задачи, лицензионный ключ KSWS будет удален при миграции с KSWS. Вам нужно будет активировать приложение заново. Например, вы можете добавить лицензионный ключ в инсталляционный пакет Kaspersky Endpoint Security для Windows.
Ключ KSWS добавлен локально в интерфейсе приложения.	Если вы активировали KSWS локально с помощью мастера активации приложения, лицензионный ключ KSWS будет удален при миграции с KSWS. Вам нужно будет активировать приложение заново. Например, вы можете добавить лицензионный ключ в инсталляционный пакет Kaspersky Endpoint Security для Windows.
Ключ KSWS добавлен в инсталляционный пакет.	Если вы активировали KSWS с помощью ключа из инсталляционного пакета, лицензионный ключ KSWS будет удален при миграции с KSWS. Вам нужно будет активировать приложение заново. Например, вы можете добавить лицензионный ключ в инсталляционный пакет Kaspersky Endpoint Security для Windows.
Платный образ виртуальной машины (Amazon Machine Image – AMI) в Amazon Web Services (AWS).	Если вы приобрели Kaspersky Security Center в виде платного образа виртуальной машины (Amazon Machine Image – AMI) в Amazon Web Services (AWS), активация KES не требуется. В этом случае Kaspersky Security Center использует подписку AWS, которая уже добавлена в приложение.
Готовый бесплатный образ Kaspersky Security Center с собственной лицензией (модель Bring Your Own License – BYOL).	При использовании в облачном окружении готового бесплатного образа Kaspersky Security Center с собственной лицензией (модель Bring Your Own License – BYOL), вам нужно будет активировать приложение любым доступным способом. Для лицензирования необходима лицензия Kaspersky Security для виртуальных и облачных сред.

Особенности миграции на высоконагруженных серверах

На высоконагруженных серверах важно контролировать производительность и не допускать сбоев. После миграции на Kaspersky Endpoint Security для Windows рекомендуется временно выключить компоненты приложения, которые используют значительные ресурсы сервера, по сравнению с остальными компонентами. После того, как вы убедитесь, что сервер выполняет свои функции в обычном режиме, вы можете включать необходимые компоненты приложения.

Рекомендуем выполнять миграцию на высоконагруженных серверах в следующем порядке:

1. Создайте политику Kaspersky Endpoint Security с параметрами по умолчанию.

   Параметры приложения по умолчанию считаются оптимальными. Эти параметры рекомендованы специалистами "Лаборатории Касперского". Параметры по умолчанию обеспечивают рекомендуемый уровень защиты и оптимальное потребление ресурсов компьютера.

2. В параметрах политики выключите следующие компоненты: Защита от сетевых угроз, Анализ поведения, Защита от эксплойтов, Откат вредоносных действий, Контроль приложений.

   Если в вашей организации развернуто решение Kaspersky Managed Detection and Response (MDR), загрузите конфигурационный файл BLOB в политике Kaspersky Endpoint Security.

3. Удалите Kaspersky Security для Windows Server с сервера.

4. Установите Kaspersky Endpoint Security для Windows с набором компонентов по умолчанию.

   Если в вашей организации развернуты решения Detection and Response, выберите соответствующие компоненты в свойствах инсталляционного пакета.

5. Проверьте параметры приложения:

   - Приложение активировано лицензионным ключом KSWS.
   - Новая политика применена. Выбранные раннее компоненты выключены.

6. Проверьте работу сервера. Убедитесь, что Kaspersky Endpoint Security для Windows использует ресурсы сервера в пределах 1%.

7. Если требуется, создайте исключения из проверки, добавьте доверенные приложения, сформируйте список доверенных веб-адресов.

8. Включите компоненты Анализ поведения, Защита от эксплойтов, Откат вредоносных действий. Убедитесь, что Kaspersky Endpoint Security для Windows использует ресурсы сервера в пределах 1%.

9. Включите компонент Защита от сетевых угроз. Убедитесь, что Kaspersky Endpoint Security для Windows использует ресурсы сервера в пределах 2%.

10. Включите компонент Контроль приложений в режиме тестирования правил.

11. Проверьте работу Контроля приложений. Если требуется, добавьте новые правила Контроля приложений и после проверки работы Контроля приложений выключите режим тестирования правил.

После миграции с KSWS на KES убедитесь, что приложение работает корректно. Проверьте статус сервера в консоли (*OK*). Убедитесь в отсутствии ошибок в работе приложения, также проверьте время последнего соединения с Сервером администрирования, время последнего обновления баз и статус защиты сервера.

Управление приложением на сервере в режиме Server Core

На сервере в режиме основных серверных компонентов (англ. Server Core Mode) отсутствует графический интерфейс. Поэтому вы можете управлять приложением только удаленно из консоли Kaspersky Security Center или локально из командной строки.

Управление приложением из консоли Kaspersky Security Center

Установка приложения из консоли Kaspersky Security Center ничем не отличается от обычной установки. При создании инсталляционного пакета вы можете добавить лицензионный ключ для активации приложения. Вы можете использовать ключ Kaspersky Endpoint Security для Windows или ключ Kaspersky Security для Windows Server.

На сервере в режиме Server Core недоступны следующие компоненты приложения: Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль, Защита от атак BadUSB, Шифрование файлов (FLE), Шифрование диска Kaspersky (FDE).

При установке Kaspersky Endpoint Security перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые приложения. Также перезагрузка может потребоваться при обновлении версии приложения. У приложения нет возможности показать окно запроса для перезагрузки сервера. Вы можете узнать о необходимости перезагрузки сервера из отчетов в консоли Kaspersky Security Center.

Управление приложением на серверах в режиме Server Core ничем не отличается от управления компьютером. Вы можете использовать политики и задачи для настройки приложения.

Управление приложением на серверах в режиме Server Core имеет следующие особенности:

- Так как на сервере в режиме Server Core отсутствует графический интерфейс, то Kaspersky Endpoint Security не показывает предупреждение о необходимости лечения активного заражения. Для устранения угрозы вам необходимо включить технологию лечения активного заражения в параметрах приложения и включить немедленное лечение активного заражения в свойствах задачи *Поиск вредоносного ПО*. Далее вам нужно запустить задачу *Поиск вредоносного ПО*.

- Шифрование диска BitLocker доступно только с помощью доверенного платформенного модуля (TPM). Использовать PIN / пароль при шифровании невозможно, так как у приложения нет возможности показать окно запроса пароля для предзагрузочной аутентификации. Если в операционной системе включен режим совместимости с Федеральным стандартом обработки информации (FIPS), вам нужно подключить съемный диск для сохранения ключа шифрования до начала шифрования диска.

Управление приложением из командной строки

При отсутствии графического интерфейса вы можете управлять Kaspersky Endpoint Security из командной строки.

Для установки приложения на сервер в режиме Server Core выполните следующую команду:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Для активации приложения выполните следующую команду:

```
avp.com license /add <activation code or key file>
```

Для проверки статусов профилей приложения выполните следующую команду:

```
avp.com status
```

Для просмотра списка команд для управления приложением выполните следующую команду:

```
avp.com help
```

Пример миграции с [KSWS+KEA] на [KES+встроенный агент]

При миграции с Kaspersky Security для Windows Server (KSWS) на Kaspersky Endpoint Security (KES) вы можете использовать следующие рекомендации для настройки защиты серверов и оптимизации производительности. Рассмотрим миграцию на примере одной организации.

Инфраструктура организации

В компании установлено следующее оборудование:

- Kaspersky Security Center 14.2;

  Администратор управляет решениями Kaspersky с помощью Консоли администрирования (MMC). Также развернуто решение Kaspersky Endpoint Detection and Response Optimum (EDR Optimum).

  В Kaspersky Security Center созданы три группы администрирования, в которые добавлены серверы организации: две группы администрирования для SQL-серверов и группа администрирования для Microsoft Exchange-серверов. Каждая группа администрирования находится под управлением отдельной политики. Для всех серверов организации созданы задачи *Обновление баз программы* и *Проверка по требованию*.

  Ключ для активации KSWS добавлен в Kaspersky Security Center. Включена функция автоматического распространения ключа.

- SQL-серверы с установленным Kaspersky Security для Windows Server 11.0.1 и Kaspersky Endpoint Agent 3.11. SQL-серверы объединены в два кластера.

  KSWS находится под управлением политик *Политика_SQL(1)* и *Политика_SQL(2)*. Также созданы задачи *Обновление баз программы*, *Проверка по требованию*.

- Microsoft Exchange-сервер с установленным Kaspersky Security для Windows Server 11.0.1 и Kaspersky Endpoint Agent 3.11.

  KSWS находится под управлением политики *Политика_Exchange*. Также созданы задачи *Обновление баз программы*, *Проверка по требованию*.

Планирование миграции

Миграции состоит из следующих этапов:

1. Миграция политик и задач KSWS с помощью мастера массовой конвертации политик и задач.
2. Миграция политики Kaspersky Endpoint Agent с помощью мастера массовой конвертации политик и задач.
3. Активация профилей политик в свойствах новой политики с помощью тегов.
4. Установка KES вместо KSWS.
5. Активация EDR Optimum.
6. Проверка работы KES.

Сценарий миграции сначала будет выполнен на одном кластере SQL-серверов. Далее сценарий миграции будет выполнен на втором кластере SQL-серверов. Далее сценарий миграции будет выполнен на Microsoft Exchange-сервере.

Миграция политик и задач KSWS с помощью мастера массовой конвертации политик и задач

Для миграции политик и задач KSWS вы можете использовать мастер массовой конвертации политик и задач (мастер миграции). В результате вместо политик *Политика_SQL(1)*, *Политика_SQL(2)* и *Политика_Exchange* вы получите одну политику с тремя профилями для SQL- и Microsoft Exchange-серверов. Новый профиль политики с параметрами KSWS будет иметь имя *UpgradedFromKSWS <Название политики Kaspersky Security для Windows Server>*. В свойствах профиля в качестве условия срабатывания мастер миграции автоматически выбирает тег устройства `UpgradedFromKSWS`. Таким образом, параметры из профиля политики будут применены на серверы автоматически.

Миграция политики Kaspersky Endpoint Agent с помощью мастера массовой конвертации политик и задач

Для миграции политики Kaspersky Endpoint Agent вы можете использовать мастер массовой конвертации политик и задач. Мастер миграции политик и задач для Kaspersky Endpoint Agent доступен только в Web Console.

Активация профилей политик в свойствах новой политики с помощью тегов

В качестве условия активация профиля нужно выбрать тег устройства, который вы назначили ранее. Нужно открыть свойства политики и выбрать условие активации профиля *Общие правила активации профиля политики*.

Установка KES вместо KSWS

Перед установкой KES нужно выключить Защиту паролем в свойствах политики KSWS.

Установка KES состоит из следующих действий:

1. Подготовьте инсталляционный пакет. В свойствах инсталляционного пакета выберите дистрибутив Kaspersky Endpoint Security для Windows 12.0, выберите набор компонентов по умолчанию.
2. Создайте задачу *Удаленная установка приложения* для одной группы администрирования SQL-серверов.
3. В свойствах задачи выберите инсталляционный пакет и файл лицензионного ключа.
4. Дождитесь успешного выполнения задачи.
5. Повторите установку KES для оставшихся групп администрирования.

Kaspersky Security Center автоматически добавит тег `UpgradedFromKSWS` к именам компьютеров в консоли после завершения установки KES.

Для проверки установки KES вы можете использовать *Отчет о развертывании защиты*. Также вы можете проверить статус устройства. Для проверки активации приложения вы можете использовать *Отчет об использовании лицензионных ключей*.

Активация EDR Optimum

Для активации функциональности EDR Optimum предназначена отдельная лицензия Kaspersky Endpoint Detection and Response Optimum Add-on. Вам нужно проверить, что ключ EDR Optimum добавлен в хранилище Kaspersky Security Center и функция автоматического распространения лицензионного ключа включена.

Для проверки активации EDR Optimum вы можете использовать *Отчет о статусе компонентов приложения*.

Проверка работы KES

Для проверки работы KES вы можете убедиться в отсутствии ошибок. Статус устройства должен быть *OK*. Задачи обновления и поиска вредоносного ПО выполнены успешно.

Режим Легкого агента для защиты виртуальных машин

Начиная с версии Kaspersky Endpoint Security для Windows 12.8 вы можете использовать приложение в составе решения Kaspersky Security для виртуальных сред Легкий агент. *Kaspersky Security для виртуальных сред Легкий агент* – интегрированное решение, обеспечивающее комплексную защиту виртуальных машин от различных видов информационных угроз, сетевых и мошеннических атак. Для работы с этим решением вам нужно установить приложение в режиме Легкого агента.

Установка Kaspersky Endpoint Security в режиме Легкого агента на виртуальные машины с Arm-архитектурой не поддерживается.

Вы можете использовать Kaspersky Endpoint Security в режиме Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент начиная с версии 6.2.

При запуске Легкий агент устанавливает и поддерживает соединение с виртуальной машиной SVM (Secure Virtual Machine). На SVM развернут Сервер защиты. *Сервер защиты* – компонент решения Kaspersky Security для виртуальных сред Легкий агент, который выполняет проверку файлов на наличие вирусов и других вредоносных приложений, обновляет антивирусные базы и управляет лицензионными ключами. Легкий агент отправляет на SVM файлы или их фрагменты, которые необходимо проверять. Результаты проверки доступны для всех виртуальных машин с установленным Легким агентом благодаря технологии SharedCache. Эта технология повышает эффективность работы решения и обеспечивает более высокую скорость реакции на угрозы.

В инфраструктуре организации может быть много виртуальных машин с установленным Легким агентом и много SVM. Взаимодействие между виртуальными машинами и SVM осуществляется с помощью Сервера интеграции. *Сервер интеграции* – компонент решения Kaspersky Security для виртуальных сред Легкий агент, который формирует список доступных SVM и передает эти данные Легким агентам, участвует в обнаружении SVM Легкими агентами, обеспечивает защиту соединения между Легкими агентами и SVM, а также выполняет другие функции.

Особенности работы приложения в режиме Легкого агента

Управление Kaspersky Endpoint Security в стандартном режиме и режиме Легкого агента осуществляется с помощью политик и задач Kaspersky Endpoint Security. Из-за особенностей работы Легкого агента некоторые компоненты и функции приложения недоступны.

Обновление баз и модулей приложения

Kaspersky Endpoint Security в режиме Легкого агента использует специальные базы вредоносного ПО, необходимые для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Kaspersky Endpoint Security получает от Сервера защиты обновления баз и программных модулей.

Обновление баз и модулей на защищенных виртуальных машинах выполняется с помощью специальной локальной задачи *Обновление баз и модулей приложения*, в которой в качестве источника обновлений указана папка на SVM. Легкий агент запускает задачу *Обновление баз и модулей приложения* автоматически. Выбрать другой источник обновления, настроить расписание запуска задачи и удалить задачу невозможно.

Откат последнего обновления баз вредоносного ПО также выполняется на стороне Сервера защиты. После отката обновления баз и программных модулей на SVM на защищенной виртуальной машине автоматически запускается специальная локальная задача *Обновление баз и модулей приложения*. В результате выполнения задачи Легкий агент возвращается к использованию предыдущего набора баз вредоносного ПО.

Kaspersky Endpoint Security в режиме Легкого агента не поддерживает задачу *Откат обновления*.

Активация Легкого агента

Для активации приложения вам нужно добавить лицензионный ключ на SVM, к которому подключен Легкий агент. Отдельно активировать приложение не требуется.

Другие особенности работы приложения в режиме Легкого агента

- При создании политики для приложения рекомендуется выбрать режим Легкого агента. В этом режиме мастер создания политики предлагает настроить параметры подключения к SVM. Эти параметры являются обязательными для работы приложения в режиме Легкого агента.
- Установить компоненты шифрования данных и Адаптивный контроль аномалий в режиме Легкого агента невозможно. Также набор компонентов зависит от типа гостевой операционной системы: рабочая станция или сервер.
- Приложение в режиме Легкого агента поддерживает интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premises). Интеграция с облачными решениями Kaspersky Endpoint Detection and Response Expert и Kaspersky Endpoint Detection and Response Expert (cloud) не поддерживается.
- Управление Легким агентом доступно в Консоли администрирования (MMC) и Kaspersky Security Center Web Console. Управлять Легким агентом в Kaspersky Security Center Cloud Console невозможно.
- Kaspersky Endpoint Security взаимодействует с серверами KSN с помощью прокси-сервера KSN. Взаимодействие с KSN напрямую не поддерживается.
- Облачный режим Kaspersky Security Network не поддерживается.
- Использование прокси-сервера приложения при подключении к Серверу интеграции (VIIS), к Серверу защиты (SVM) и серверам KSN не поддерживается.

Предварительная настройка виртуальной машины

Вы можете установить Kaspersky Endpoint Security на виртуальную машину, на которой используются технологии виртуальных платформ. Kaspersky Endpoint Security поддерживает виртуальные платформы VMware, Microsoft Hyper-V, Citrix. Перед установкой нужно выполнить предварительную настройку виртуальных машин.

Совместимость с технологией Citrix App Layering

Если для сохранения состояния временных виртуальных машин вы планируете использовать полный пользовательский слой (Full User Layer), перед установкой на шаблоне виртуальных машин вам нужно выполнить следующие действия:

1. Создать файл C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt и добавить в него следующие исключения:
   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`
2. В реестре операционной системы в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unifltr создать новый ключ типа DWORD с именем MiniFilterBypass и значением 1.
3. В реестре операционной системы в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd создать новый ключ типа MULTI_SZ с именем ExcludeKey со следующими значениями (две строки):
   - \Registry\Machine\SOFTWARE\KasperskyLab
   - \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab
4. Перезагрузить виртуальную машину.

Для установки на виртуальных машинах в инфраструктуре, в которой используется технология Citrix App Layering, вам нужно выполнить следующие действия:

1. Установить Агент администрирования Kaspersky Security Center и Kaspersky Endpoint Security для Windows на шаблоне виртуальных машин на слой приложений (Application Layer).
2. Создать образ виртуальной машины, состоящий из нескольких слоев.
3. Развернуть созданный образ на гипервизорах, которые поддерживают решение Citrix App Layering.
4. Настроить создание временных виртуальных машин из созданного образа.

Подробнее об установке антивирусного ПО совместно с Citrix App Layering см. в документации Citrix App Layering.

Совместимость с технологией Citrix Provisioning (Citrix Provisioning Services)

Чтобы обеспечить совместимость программы с технологией Citrix Provisioning (Citrix Provisioning Services), необходимо выполнить следующие действия:

- Если на виртуальной машине установлено программное обеспечение Citrix Provisioning Target Device, требуется удалить его перед началом установки приложения Kaspersky Endpoint Security (подробнее см. на сайте службы технической поддержки Citrix). После установки приложения необходимо заново установить Citrix Provisioning Target Device. Переустановка Citrix Provisioning Target Device также необходима при восстановлении приложения – в том числе при обновлении операционной системы.

  Обновление операционной системы состоит из следующих этапов:

  1. Удалите Citrix Provisioning Target Device.
  2. Обновите операционную систему.
  3. После запуска виртуальной машины убедитесь, что приложение Kaspersky Endpoint Security запущено и работает корректно.
  4. Установите Citrix Provisioning Target Device повторно.

- При установке приложения с помощью мастера установки или удаленно через Kaspersky Security Center необходимо установить флажок **Обеспечить совместимость с Citrix PVS**.

Совместимость с технологией Omnissa App Volumes

Перед установкой на шаблоне виртуальных машин вам нужно создать файл %SVAgent%\Config\Custom\snapvol.cfg и добавить в него следующие исключения:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`

- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

Подробнее см. в документации Omnissa.

Установка Легкого агента

Установка Kaspersky Endpoint Security в режиме Легкого агента на виртуальные машины с Arm-архитектурой не поддерживается.

Установка приложения в режиме Легкого агента не отличается от установки приложения в стандартном режиме. Перед установкой Легкого агента на виртуальной машине должен быть установлен Агент администрирования Kaspersky Security Center. *Агент администрирования* обеспечивает взаимодействие между Сервером администрирования и виртуальной машиной.

Легкий агент может быть установлен на виртуальную машину следующими способами:

- удаленно с помощью Kaspersky Security Center;
- локально с помощью мастера установки;
- локально с помощью командной строки.

Для установки Легкого агента нужно выбрать соответствующую конфигурацию в параметрах инсталляционного пакета или мастере установки приложения.

При установке Легкого агента на сервер из конфигурации приложения по умолчанию исключены компоненты продвинутой защиты (Анализ поведения, Защита от эксплойтов, Откат вредоносных действий). Конфигурация приложения по умолчанию обеспечивает рекомендуемый уровень защиты и оптимальное потребление ресурсов сервера. При установке Легкого агента на рабочую станцию компоненты продвинутой защиты включены в конфигурацию приложения по умолчанию.

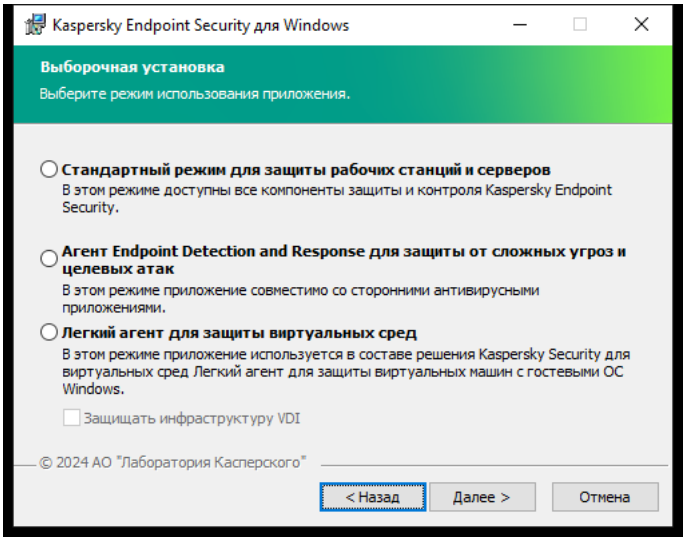
При установке Легкого агента рекомендуется выбрать предустановленные исключения и доверенные приложения для соответствующей виртуальной среды. Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения и избежать проблем совместимости с виртуальной средой. Вы также можете настроить предустановленные исключения из проверки и доверенные приложения после установки в политике.

Как установить Легкий агент с помощью мастера установки

1. Скопируйте папку комплекта поставки на виртуальную машину.
2. Запустите файл setup_kes.exe.

   Запустится мастер установки приложения.

Конфигурация Kaspersky Endpoint Security



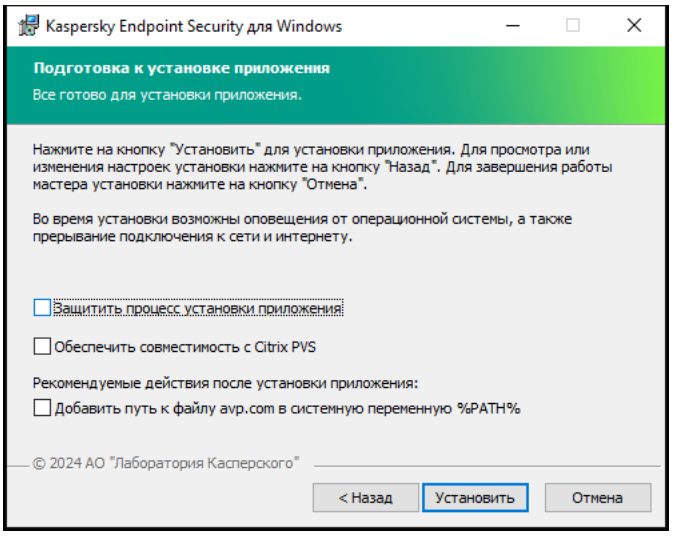
Выбор конфигурации приложения

Выберите конфигурацию **Легкий агент для защиты виртуальных сред**. Эта конфигурация предназначена для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Легкий агент должен быть установлен на каждой виртуальной машине, которую требуется защищать с помощью решения. В этой конфигурации недоступны компоненты шифрования данных и Адаптивный контроль аномалий. Если вы устанавливаете Легкий агент на шаблон виртуальных машин, из которого вы будете создавать *временные виртуальные машины*, установите флажок **Защищать инфраструктуру VDI** (Virtual Desktop Infrastructure). Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. В этом режиме Легкий агент отклоняет обновления приложения, требующие перезагрузки виртуальной машины. При получении обновлений приложения, требующих перезагрузки, Легкий агент формирует событие о необходимости обновить шаблон защищенных виртуальных машин.

Компоненты Kaspersky Endpoint Security

Выберите компоненты, которые вы хотите установить (см. рис. ниже). Вы можете изменить состав компонентов после установки приложения. Для этого вам нужно запустить мастер установки повторно и выбрать операцию изменения состава компонентов.

Дополнительные параметры



Дополнительные параметры установки приложения

Защитить процесс установки приложения. Защита установки включает в себя защиту от подмены дистрибутива вредоносными приложениями, блокирование доступа к папке установки Kaspersky Endpoint Security и блокирование доступа к разделу системного реестра с ключами приложения. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку приложения (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop).

Обеспечить совместимость с Citrix PVS. Вы можете включить поддержку Citrix Provisioning Services для установки Kaspersky Endpoint Security на виртуальную машину.

Добавить путь к файлу avp.com в системную переменную %PATH%. Вы можете добавить путь установки в переменную %PATH% для удобства использования интерфейса командной строки.

Как установить Легкий агент с помощью командной строки

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security.
3. Выполните команду:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
   ```

   или

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
   ```

   Параметр `VDI` включает режим защиты инфраструктуры VDI (Virtual Desktop Infrastructure). Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. В этом режиме Легкий агент отклоняет обновления приложения, требующие перезагрузки виртуальной машины. При получении обновлений приложения, требующих перезагрузки, Легкий агент формирует событие о необходимости обновить шаблон защищенных виртуальных машин. По умолчанию режим защиты инфраструктуры VDI выключен.

В результате Легкий агент будет установлен на виртуальную машину с набором компонентов по умолчанию. Вы можете изменить набор компонентов и настроить дополнительные параметры с помощью файла setup.ini. Также вы можете указать параметры установки в командной строке.

Как установить Легкий агент через Консоль администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.
3. Откройте свойства инсталляционного пакета Kaspersky Endpoint Security для Windows.

   Если требуется, создайте новый инсталляционный пакет.
4. Перейдите в раздел **Настройки**.
5. Выберите конфигурацию **Легкий агент для защиты виртуальных сред**. Эта конфигурация предназначена для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Легкий агент должен быть установлен на каждой виртуальной машине, которую требуется защищать с помощью решения. В этой конфигурации недоступны компоненты шифрования данных и Адаптивный контроль аномалий. Если вы устанавливаете Легкий агент на шаблон виртуальных машин, из которого вы будете создавать *временные виртуальные машины*, установите флажок **Защищать инфраструктуру VDI** (Virtual Desktop Infrastructure). Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. В этом режиме Легкий агент отклоняет обновления приложения, требующие перезагрузки виртуальной машины. При получении обновлений приложения, требующих перезагрузки, Легкий агент формирует событие о необходимости обновить шаблон защищенных виртуальных машин.
6. Выберите компоненты, которые вы хотите установить.

   Вы можете изменить состав компонентов после установки приложения.

7. Настройте доверенную зону. Выберите предустановленные исключения из проверки и доверенные приложения для виртуальной среды, в которой вы устанавливаете приложение.

   Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения и избежать проблем совместимости с виртуальной средой.

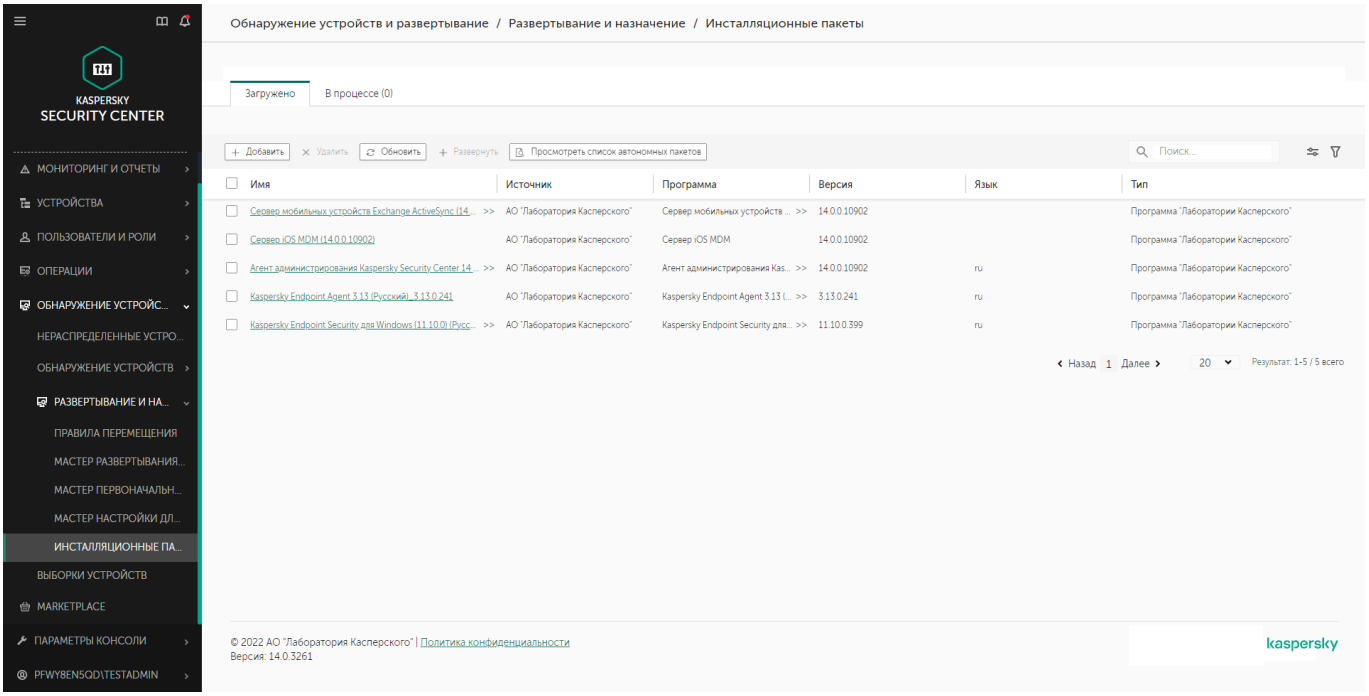
8. Сохраните внесенные изменения.

9. Создайте задачу удаленной установки. В свойствах задачи выберите созданный инсталляционный пакет.

Как установить Легкий агент через Web Console

1. В главном окне Web Console выберите **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.



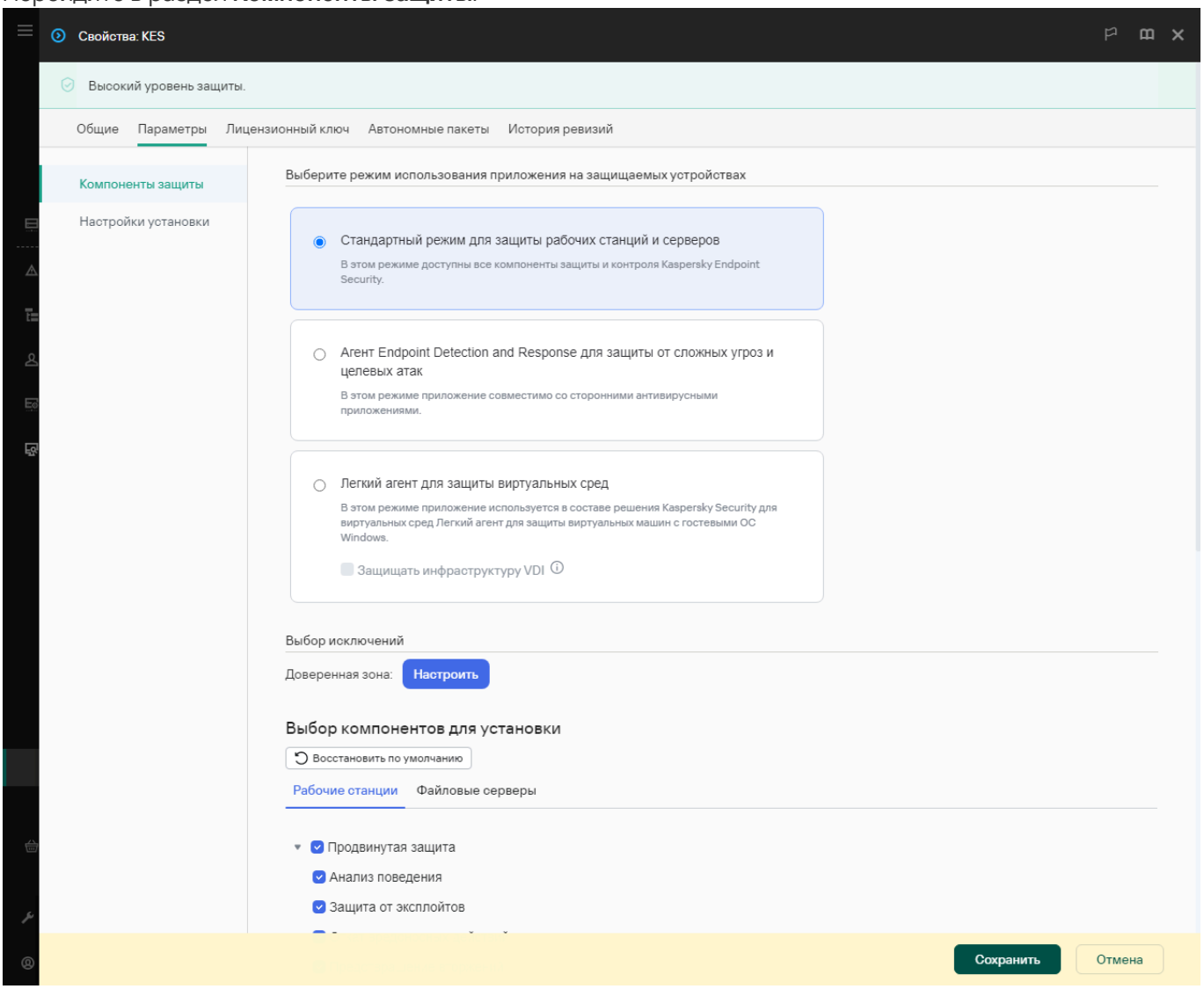
Список инсталляционных пакетов

2. Откройте свойства инсталляционного пакета Kaspersky Endpoint Security для Windows.

   Если требуется, создайте новый инсталляционный пакет.

3. Выберите вкладку **Параметры**.

4. Перейдите в раздел **Компоненты защиты**.



Состав компонентов в инсталляционном пакете

5. Выберите конфигурацию **Легкий агент для защиты виртуальных сред**. Эта конфигурация предназначена для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Легкий агент должен быть установлен на каждой виртуальной машине, которую требуется защищать с помощью решения. В этой конфигурации недоступны компоненты шифрования данных и Адаптивный контроль аномалий. Если вы устанавливаете Легкий агент на шаблон виртуальных машин, из которого вы будете создавать *временные виртуальные машины*, установите флажок **Защищать инфраструктуру VDI** (Virtual Desktop Infrastructure). Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. В этом режиме Легкий агент отклоняет обновления приложения, требующие перезагрузки виртуальной машины. При получении обновлений приложения, требующих перезагрузки, Легкий агент формирует событие о необходимости обновить шаблон защищенных виртуальных машин.

6. Выберите компоненты, которые вы хотите установить.

   Вы можете изменить состав компонентов после установки приложения.

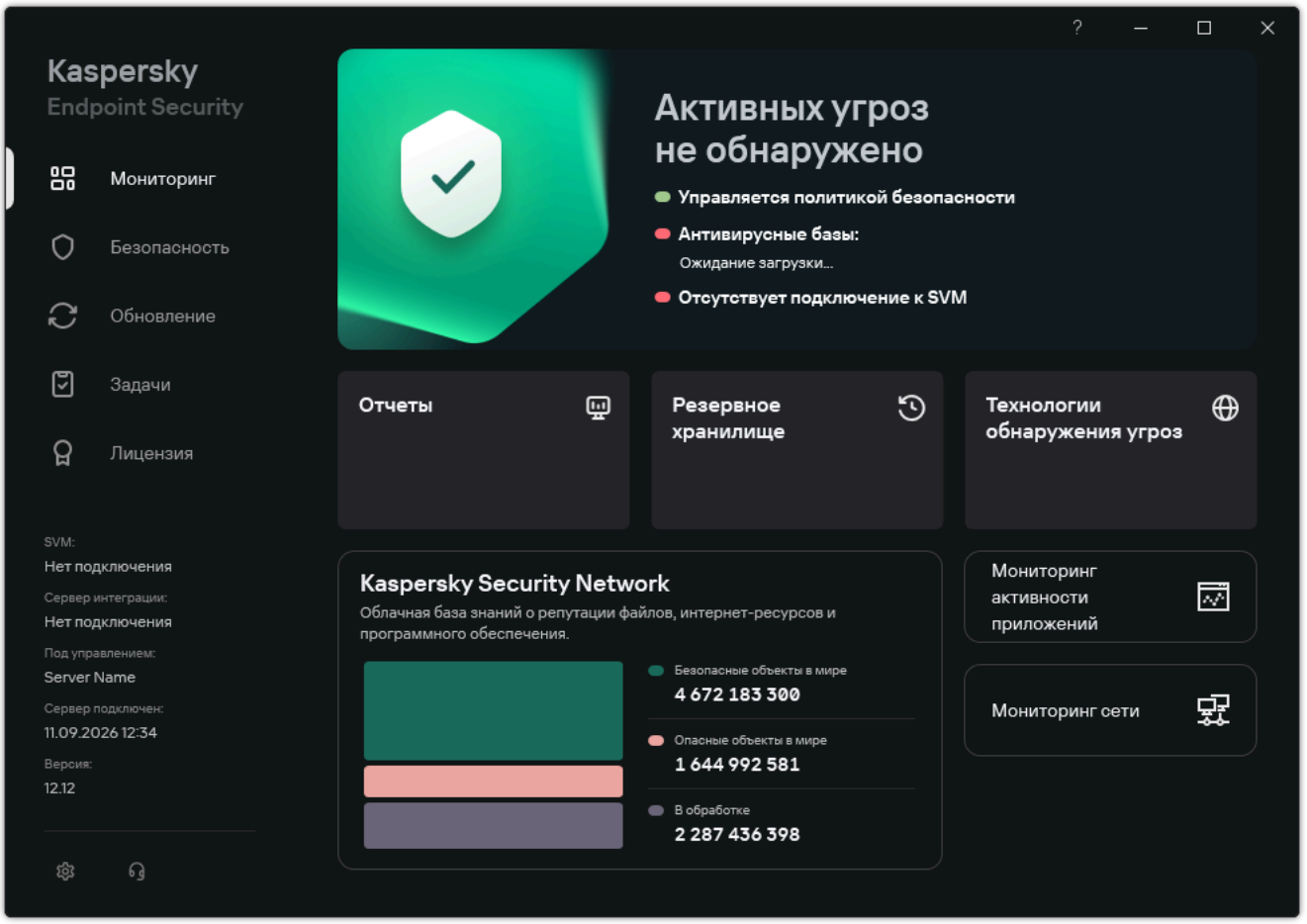
7. Настройте доверенную зону. Выберите предустановленные исключения из проверки и доверенные приложения для виртуальной среды, в которой вы устанавливаете приложение.

   Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения и избежать проблем совместимости с виртуальной средой.

8. Сохраните внесенные изменения.

9. Создайте задачу удаленной установки. В свойствах задачи выберите созданный инсталляционный пакет.

В результате Легкий агент будет установлен на виртуальную машину. Вам доступен интерфейс приложения, а также значок приложения в области уведомлений . Теперь вам нужно настроить подключение Легкого агента к SVM.



Главное окно Легкого агента

Подключение Легкого агента к SVM

Для работы решения Kaspersky Security для виртуальных сред Легкий агент требуется постоянное взаимодействие между Легким агентом и SVM. Это нужно для проверки файлов, отправленных Легким агентом, на наличие вирусов и других вредоносных приложений. Если соединение с SVM отсутствует, у Легкого агента отсутствует возможность отправлять файлы на проверку. Если соединение отсутствует более пяти минут, проверка завершается с ошибкой.

Подключение Легкого агента к SVM состоит из следующих этапов:

1. Легкий агент получает список доступных SVM.

2. Легкий агент определяет оптимальный для подключения Сервер защиты (SVM) из числа доступных для подключения в соответствии с алгоритмом выбора SVM.

3. Легкий агент проверяет дополнительные параметры для подключения к SVM: теги, статус защиты подключения, доступные по лицензии функции приложения.

4. Подключение Легкого агента к SVM.

Вы можете получить информацию о состоянии подключения Легкого агента к SVM в интерфейсе Kaspersky Endpoint Security или с помощью команды приложения. Приложение формирует события о потере и восстановлении соединения Легкого агента с SVM и отправляет события в Kaspersky Security Center. Если вы используете Сервер интеграции для обнаружения SVM, вы можете получать информацию о состоянии SVM и количестве подключенных Легких агентов в Консоли Сервера интеграции. Подробнее о мониторинге состояния SVM см. в справке Kaspersky Security для виртуальных сред Легкий агент.

Обнаружение SVM

Вы можете выбрать один из способов обнаружения SVM Легким агентом:

- С помощью Сервера интеграции (VIIS).

  Сервер интеграции – компонент решения, который обеспечивает взаимодействие между решением Kaspersky Security для виртуальных сред Легкий агент и виртуальной инфраструктурой и формирует список доступных для подключения SVM. Легкий агент устанавливает соединение с Сервером интеграции и получает список адресов SVM.

  Сервер интеграции удобно использовать в больших виртуальных инфраструктурах, так как он автоматически распределяет нагрузку между SVM, получает информацию о доступных SVM, анализирует эту информацию и предоставляет Легким агентам список Серверов защиты (SVM), оптимальных для подключения.

  Для получения списка SVM Легким агентом вам нужно только ввести адрес Сервера интеграции.

- С помощью отказоустойчивого кластера Серверов интеграции.

  Развертывание отказоустойчивого кластера Серверов интеграции доступно в Kaspersky Security для виртуальных сред Легкий агент начиная с версии 6.4. Отказоустойчивый кластер Серверов интеграции обеспечивает непрерывную защиту виртуальной среды за счет переключения SVM и Легких агентов на резервный Сервер интеграции при отказе главного Сервера интеграции. Переключение между серверами выполняет специальный компонент кластера – *балансировщик нагрузки*. Подробнее об отказоустойчивом кластере Серверов интеграции см. в справке Kaspersky Security для виртуальных сред Легкий агент.

  Для получения списка SVM Легким агентом вам нужно ввести адрес устройства, на котором установлен балансировщик нагрузки.

- С помощью списка адресов SVM.

  Если вам нужно указать для Легкого агента отдельные SVM для подключения, вы можете составить список вручную.

  Для получения списка SVM Легким агентом вам нужно перечислить адреса доступных SVM.

Как настроить обнаружение SVM Легким агентом в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите папку **Политики**.

3. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

4. В окне политики выберите **Режим Легкого агента** → **Настройки обнаружения SVM**.

5. Выберите способ обнаружения SVM:

- **Использовать Сервер интеграции**. Введите параметры подключения к Серверу интеграции в зависимости от вашей инфраструктуры:
  - **Одиночный Сервер интеграции**. Введите параметры подключения к Серверу интеграции: IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства.
  - **Отказоустойчивый кластер Серверов интеграции**. Введите IP-адрес и порт балансировщика нагрузки, который входит в состав кластера.
- **Использовать список адресов SVM, заданный вручную**. Сформируйте список SVM для подключения Легкого агента. Введите IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Каждый элемент списка нужно вводить с новой строки или отделять от предыдущего с помощью `;`.

  В списке адресов SVM требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе решения.

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить обнаружение SVM Легким агентом в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Режим Легкого агента** → **Настройки обнаружения SVM**.
5. Выберите способ обнаружения SVM:

- **Использовать Сервер интеграции**. Введите параметры подключения к Серверу интеграции в зависимости от вашей инфраструктуры:
  - **Одиночный Сервер интеграции**. Введите параметры подключения к Серверу интеграции: IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства.
  - **Отказоустойчивый кластер Серверов интеграции**. Введите IP-адрес и порт балансировщика нагрузки, который входит в состав кластера.
- **Использовать список адресов SVM, заданный вручную**. Сформируйте список SVM для подключения Легкого агента. Введите IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Каждый элемент списка нужно вводить с новой строки или отделять от предыдущего с помощью `;`.

  В списке адресов SVM требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе решения.

6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить обнаружение SVM Легким агентом в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения в блоке **Режим Легкого агента** нажмите на плитку **Настройки обнаружения SVM**.
3. Выберите способ обнаружения SVM:
   - **Использовать Сервер интеграции**. Введите параметры подключения к Серверу интеграции в зависимости от вашей инфраструктуры:
     - **Одиночный Сервер интеграции**. Введите параметры подключения к Серверу интеграции: IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства.
     - **Отказоустойчивый кластер Серверов интеграции**. Введите IP-адрес и порт балансировщика нагрузки, который входит в состав кластера.
   - **Использовать список адресов SVM, заданный вручную**. Сформируйте список SVM для подключения Легкого агента. Введите IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Каждый элемент списка нужно вводить с новой строки или отделять от предыдущего с помощью `;`.

     В списке адресов SVM требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе решения.
4. Сохраните внесенные изменения.

Настройка алгоритма выбора SVM для Легкого агента

В инфраструктуре организации может быть развернуто несколько SVM, к которым могут подключаться Легкие агенты. Для оптимизации нагрузки на сеть и ресурсы виртуальной инфраструктуры необходимо распределить Легкие агенты между SVM.

Алгоритмы выбора SVM

Легкие агенты могут применять следующие алгоритмы выбора SVM для подключения: Стандартный алгоритм (по умолчанию) и Расширенный алгоритм.

<table>
<tr><th>Стандартный алгоритм</th><th>Расширенный алгоритм</th></tr>
<tr><td>Если применяется этот алгоритм, после установки и запуска на виртуальной машине Легкий агент выбирает для подключения SVM, которая является локальной для Легкого агента.

Если нет доступных для подключения локальных SVM, Легкий агент выбирает SVM, к которой подключено наименьшее количество Легких агентов, независимо от расположения SVM в виртуальной инфраструктуре.

Локальность SVM относительно Легкого агента не определяется, если для Сервера защиты на этой SVM включен режим защиты больших инфраструктур. В этом случае рекомендуется использовать расширенный алгоритм выбора SVM и выбрать Сервер интеграции в качестве способа обнаружения SVM.

Локальность SVM относительно Легкого агента определяется в зависимости от вида виртуальной инфраструктуры.</td><td>Если применяется этот алгоритм, вы можете определять следующие параметры выбора SVM:

• учитывать или игнорировать расположение SVM в инфраструктуре при выборе SVM для подключения;
• если расположение SVM учитывается, как определять локальность SVM относительно Легкого агента.

Если Легкие агенты игнорируют расположение SVM в инфраструктуре, то Легкие агенты смогут подключаться к любым доступным для подключения SVM.

Если Легкие агенты должны учитывать расположение SVM в инфраструктуре, вам нужно выбрать тип расположения SVM, который будет учитываться при определении локальности SVM относительно Легкого агента. Локальность SVM относительно Легкого агента определяется по-разному в зависимости от виртуальной инфраструктуры.

Если Легкие агенты учитывают расположение SVM в инфраструктуре при выборе SVM для подключения, то Легкие агенты могут подключаться только к тем SVM, которые являются локальными.

Например, если вы указали в качестве типа расположения SVM кластер гипервизоров, то локальными для Легкого агента будут считаться все SVM, развернутые на этом кластере гипервизоров, и Легкий агент сможет подключаться только к одной из этих SVM. Если в том же кластере, в котором работает Легкий агент, нет доступных для подключения SVM, Легкий агент не будет подключаться к SVM.

При выборе SVM Легкие агенты также учитывают количество подключенных Легких агентов, чтобы обеспечить равномерное распределение Легких агентов между доступными для подключения SVM.

Если для Легкого агента применяется расширенный алгоритм выбора SVM и в качестве способа обнаружения SVM выбран список адресов SVM, а на SVM включен режим защиты больших инфраструктур, то подключение Легкого агента к этой SVM возможно, только если Легкий агент игнорирует расположение SVM.</td></tr>
<tr><th colspan="2">Базис Dynamix Enterprise</th></tr>
<tr><td>В виртуальной инфраструктуре на платформе Базис Dynamix Enterprise локальной для Легкого агента считается SVM, которая развернута на том же вычислительном узле, что и виртуальная машина с установленным Легким агентом.</td><td>В виртуальной инфраструктуре на платформе Базис Dynamix Enterprise SVM может считаться локальной для Легкого агента в одном из следующих случаев:

• SVM развернута на том же вычислительном узле, что и виртуальная машина с установленным Легким агентом.
• SVM развернута в той же зоне, что и виртуальная машина с установленным Легким агентом.
• SVM развернута в том же дата-центре (ЦОД), что и виртуальная машина с установленным Легким агентом.</td></tr>
<tr><th colspan="2">Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест"</th></tr>
</table>

Стандартный алгоритм	Расширенный алгоритм
В виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест" локальной для Легкого агента считается SVM, которая развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом.	В виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест" SVM может считаться локальной для Легкого агента в одном из следующих случаев: • SVM развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом (если гипервизор поддерживается и сконфигурирован в инфраструктуре). • SVM развернута на том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом (если кластер поддерживается и сконфигурирован в инфраструктуре). • SVM развернута в том же дата-центре, что и виртуальная машина с установленным Легким агентом (если дата-центр поддерживается и сконфигурирован в инфраструктуре).
OpenStack	
В виртуальной инфраструктуре под управлением платформы OpenStack вы можете указывать, как определяется локальность SVM относительно Легкого агента, с помощью параметра `StandardAlgorithmSvmLocality` в секции `HypervisorSpecificSettings:Openstack` в конфигурационном файле Сервера интеграции appsettings.json. В зависимости от версии Сервера интеграции файл расположен по следующему пути: • /var/opt/kaspersky/viis/common/ – файл Сервера интеграции на базе Linux. • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ – файл Сервера интеграции на базе Windows. Параметр `StandardAlgorithmSvmLocality` может принимать следующие значения: • `ServerGroup` – если установлено это значение, локальной для Легкого агента считается SVM, которая находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом. Это значение используется по умолчанию. • `Project` – если установлено это значение, локальной для Легкого агента считается SVM, которая развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом. • `AvailabilityZone` – если установлено это значение, локальной для Легкого агента считается SVM, которая расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом.	В виртуальной инфраструктуре под управлением платформы OpenStack SVM может считаться локальной для Легкого агента в одном из следующих случаев: • SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом. • SVM развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом. • SVM расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом.

Кроме алгоритмов подключения к SVM вы можете регулировать подключение Легких агентов к SVM с помощью тегов.

Настройка алгоритма выбора SVM

Как настроить алгоритм выбора SVM для Легкого агента в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Режим Легкого агента** → **Алгоритм выбора SVM**.

4. Выберите алгоритм:

- **Использовать стандартный алгоритм выбора SVM**. Легкий агент выбирает SVM, развернутые в том же гипервизоре.

- **Использовать расширенный алгоритм выбора SVM**. Легкий агент выбирает SVM, развернутые в выбранном типе расположения SVM (по умолчанию **Гипервизор**).

5. Если требуется, выберите расположение SVM для расширенного алгоритма выбора SVM:

- **Гипервизор**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

  - SVM развернуты на том же гипервизоре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест").

  - SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack).

  - SVM находится на том же вычислительном узле, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

  Если на том же гипервизоре или в той же Группе серверов, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Кластер**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

  - SVM развернуты в том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест").

  - SVM развернуты в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack).

  - SVM находится в той же зоне, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

  Если в том же кластере гипервизоров или в рамках того же проекта OpenStack, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Дата-центр**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

  - SVM развернуты в том же дата-центре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест").

  - SVM расположены в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack).

  - SVM находится в том же ЦОД, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

  Если в том же дата-центре или в той же Зоне доступности, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Игнорировать**. Легкий агент не учитывает расположение SVM для подключения к Серверу защиты. Легкий агент учитывает другие критерии: теги, количество Легких агентов, подключенных к SVM, и другие.

6. Сохраните внесенные изменения.

Как настроить алгоритм выбора SVM для Легкого агента в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Режим Легкого агента** → **Алгоритм выбора SVM**.

5. Выберите алгоритм:

   - **Использовать стандартный алгоритм выбора SVM**. Легкий агент выбирает SVM, развернутые в том же гипервизоре.

   - **Использовать расширенный алгоритм выбора SVM**. Легкий агент выбирает SVM, развернутые в выбранном типе расположения SVM (по умолчанию **Гипервизор**).

6. Если требуется, выберите расположение SVM для расширенного алгоритма выбора SVM:

- **Гипервизор**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

  - SVM развернуты на том же гипервизоре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест").

  - SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack).

  - SVM находится на том же вычислительном узле, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

  Если на том же гипервизоре или в той же Группе серверов, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Кластер**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

  - SVM развернуты в том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест").

  - SVM развернуты в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack).

  - SVM находится в той же зоне, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

  Если в том же кластере гипервизоров или в рамках того же проекта OpenStack, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Дата-центр**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

  - SVM развернуты в том же дата-центре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест").

  - SVM расположены в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack).

  - SVM находится в том же ЦОД, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

Если в том же дата-центре или в той же Зоне доступности, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Игнорировать**. Легкий агент не учитывает расположение SVM для подключения к Серверу защиты. Легкий агент учитывает другие критерии: теги, количество Легких агентов, подключенных к SVM, и другие.

7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить алгоритм выбора SVM для Легкого агента в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .

2. В окне параметров приложения в блоке **Режим Легкого агента** нажмите на плитку **Настройки обнаружения SVM**.

3. Выберите алгоритм:

   - **Использовать стандартный алгоритм выбора SVM**. Легкий агент выбирает SVM, развернутые в том же гипервизоре.

   - **Использовать расширенный алгоритм выбора SVM**. Легкий агент выбирает SVM, развернутые в выбранном типе расположения SVM (по умолчанию **Гипервизор**).

4. Если требуется, выберите расположение SVM для расширенного алгоритма выбора SVM:

   - **Гипервизор**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

     - SVM развернуты на том же гипервизоре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест").

     - SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack).

     - SVM находится на том же вычислительном узле, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

     Если на том же гипервизоре или в той же Группе серверов, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

   - **Кластер**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

     - SVM развернуты в том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест").

     - SVM развернуты в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack).

     - SVM находится в той же зоне, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

Если в том же кластере гипервизоров или в рамках того же проекта OpenStack, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Дата-центр**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

  - SVM развернуты в том же дата-центре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Базис Dynamix Standard, zVirt или ПК СВ "Брест").

  - SVM расположены в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack).

  - SVM находится в том же ЦОД, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

  Если в том же дата-центре или в той же Зоне доступности, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Игнорировать**. Легкий агент не учитывает расположение SVM для подключения к Серверу защиты. Легкий агент учитывает другие критерии: теги, количество Легких агентов, подключенных к SVM, и другие.

5. Сохраните внесенные изменения.

Распределение подключений Легких агентов к SVM (теги)

К SVM могут подключаться несколько Легких агентов. Для распределения подключения Легких агентов вы можете указать отдельный список SVM с помощью *тегов*. Для этого вам нужно присвоить тег Легкому агенту и указать этот тег в параметрах SVM. Подробнее об указании тегов в параметрах SVM см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Например, в вашей инфраструктуре развернуто решение Kaspersky Endpoint Detection and Response Optimum для выделенных узлов виртуальных машин. Тогда вы можете назначить Легкому агенту тег `[EDROptimum]` для подключения к SVM, на которых добавлен лицензионный ключ EDR Optimum (EDR Optimum Add-on). В результате вам будут доступны функции EDR Optimum на виртуальной машине с Легким агентом. При подключении Легкого агента к SVM без лицензионного ключа EDR Optimum, функции решения Kaspersky Endpoint Detection and Response Optimum недоступны.

Как присвоить тег Легкому агенту для подключения к SVM в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Режим Легкого агента** → **Тег для подключения к SVM**.

4. Установите флажок **Использовать тег для подключения** и введите тег для подключения к SVM.

   В качестве тега вы можете ввести текстовую строку длиной не более 255 символов. Вы можете использовать любые символы, кроме символа `;`.

5. Сохраните внесенные изменения.

Как присвоить тег Легкому агенту для подключения к SVM в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Режим Легкого агента** → **Тег для подключения к SVM**.
5. Установите флажок **Использовать тег для подключения** и введите тег для подключения к SVM.

   В качестве тега вы можете ввести текстовую строку длиной не более 255 символов. Вы можете использовать любые символы, кроме символа `;`.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как присвоить тег Легкому агенту для подключения к SVM в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .
2. В окне параметров приложения в блоке **Режим Легкого агента** нажмите на плитку **Тег для подключения к SVM**.
3. Установите флажок **Использовать тег для подключения** и введите тег для подключения к SVM.

   В качестве тега вы можете ввести текстовую строку длиной не более 255 символов. Вы можете использовать любые символы, кроме символа `;`.
4. Сохраните внесенные изменения.

Защита соединения между Легким агентом и SVM

Вы можете настроить защиту соединения между Легкими агентами и Сервером защиты с помощью шифрования. Для этого вам требуется включить шифрование канала передачи данных между Легким агентом и Сервером защиты в параметрах Сервера защиты на SVM и в параметрах Легкого агента.

Легкий агент, для которого включена защита соединения, может подключаться только к тем SVM, на которых включено шифрование канала передачи данных между Легким агентом и Сервером защиты. Легкий агент, для которого выключена защита соединения, может подключаться только к тем SVM, на которых шифрование канала выключено или разрешено незащищенное соединение между Сервером защиты и Легким агентом.

Подробнее о настройке защиты соединения на Сервере защиты см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Защита соединения с помощью шифрования может привести к снижению производительности работы решения Kaspersky Security для виртуальных сред Легкий агент.

Как настроить защиту соединения на Легком агенте в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Режим Легкого агента → Защита соединения**.
4. Установите флажок **Шифровать канал передачи данных между Легким агентом и Сервером защиты**.
5. Сохраните внесенные изменения.

Как настроить защиту соединения на Легком агенте в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Режим Легкого агента → Защита соединения**.
5. Установите флажок **Шифровать канал передачи данных между Легким агентом и Сервером защиты**.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить защиту соединения на Легком агенте в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку .
2. В окне параметров приложения в блоке **Режим Легкого агента** нажмите на плитку **Защита соединения**.
3. Установите флажок **Шифровать канал передачи данных между Легким агентом и Сервером защиты**.
4. Сохраните внесенные изменения.

Активация Легкого агента

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, отдельно активировать приложение не требуется. Для активации приложения вам нужно добавить лицензионный ключ на SVM. Вы можете добавить лицензионный ключ на SVM с помощью специальной задачи в консоли Kaspersky Security Center. В интерфейсе Легкого агента управление лицензионными ключами недоступно, но вы можете просматривать информацию о лицензии (см. рис. ниже). Также вы можете просмотреть информацию о лицензировании Легкого агента в командной строке (см. инструкцию ниже). Легкий агент получает эту информацию от SVM. Подробнее об активации решения и управлении лицензионными ключами см. в справке Kaspersky Security для виртуальных сред Легкий агент.

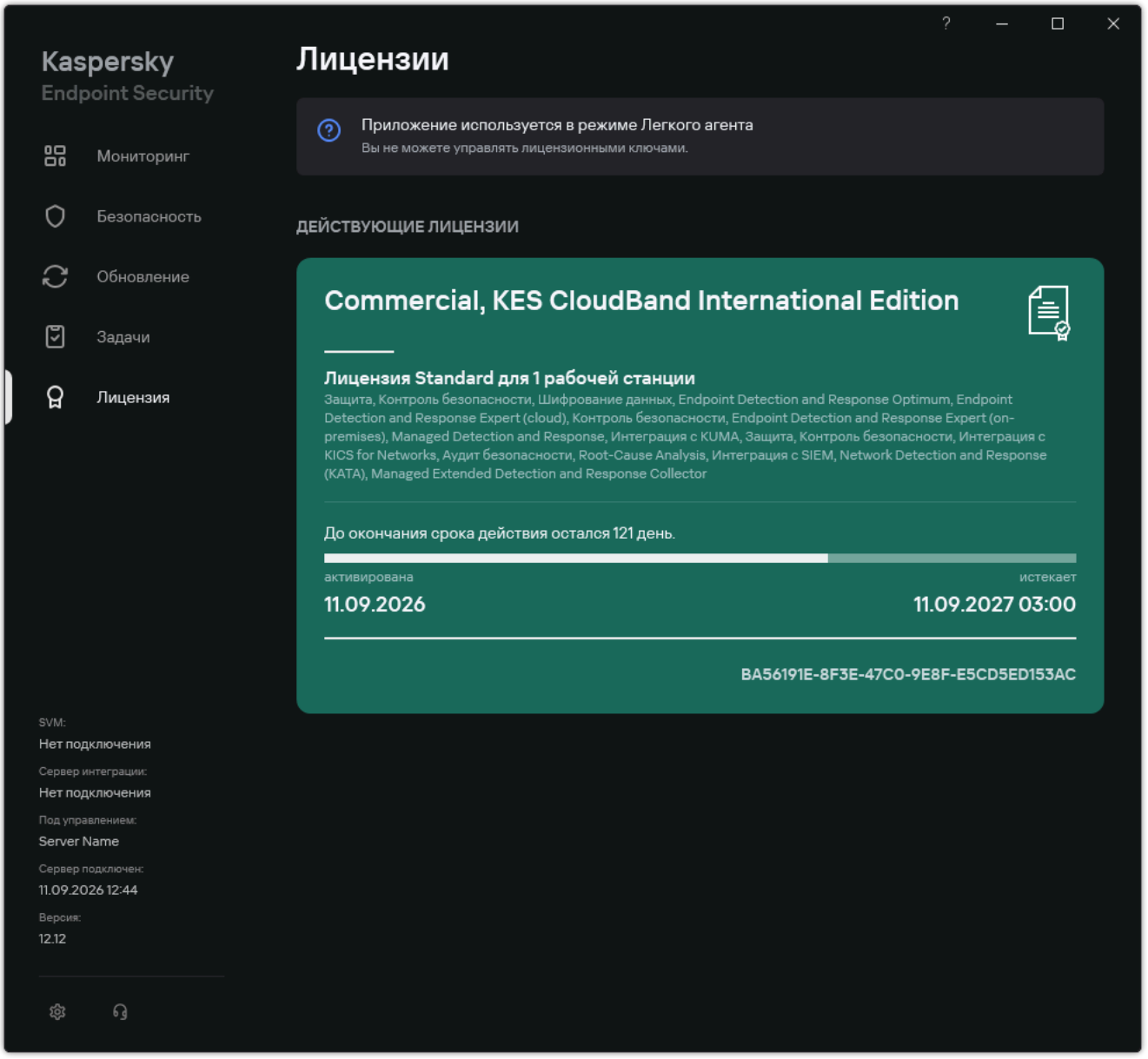
Чтобы просмотреть информацию о лицензировании Легкого агента, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

3. Выполните команду:

```
avp.com LICENSE /CHECK
```

В результате Kaspersky Endpoint Security покажет информацию о лицензии: адрес SVM, к которой подключен Легкий агент, название лицензии, количество дней до истечения лицензии и другая информация. При проблемах активации Легкого агента см. базу знаний Службы технической поддержки.



Окно Лицензирование

Руководство по миграции с Легкого агента KSVLA на Легкий агент KES

В состав Kaspersky Security для виртуальных сред Легкий агент версии 5.2 входит компонент Легкий агент для Windows 5.2 (далее также "Легкий агент KSVLA"). В Kaspersky Security для виртуальных сред Легкий агент версии 6.2 в состав решения в качестве компонента Легкий агент используется приложение Kaspersky Endpoint Security в режиме Легкого агента. Для обновления решения до версии 6.2 вам нужно выполнить миграцию с Легкого агента KSVLA версии 5.2 на Kaspersky Endpoint Security в режиме Легкого агента (далее также "Легкий агент KES"). Подробнее об обновлении версии решения Kaspersky Security для виртуальных сред Легкий агент см. в справке Kaspersky Security для виртуальных сред Легкий агент.

Программные требования

Перед миграцией с Легкого агента KSVLA на Легкий агент KES убедитесь, что виртуальная машина соответствует аппаратным и программным требованиям Kaspersky Endpoint Security для Windows. Списки поддерживаемых версий операционных систем KES и KSWS отличаются. Например, KES не поддерживает работу на серверах под управлением Windows Server 2003.

Минимальные программные требования для миграции с Легкого агента KSVLA на Легкий агент KES:

- Kaspersky Endpoint Security для Windows 12.8.
- Kaspersky Security для виртуальных сред 6.2 Легкий агент (включая компоненты Сервер защиты и Сервер интеграции).
- Kaspersky Security Center 14.2.

  Если у вас установлена более ранняя версия решения Kaspersky Security Center, рекомендуем обновить версию решения до 14.2 или выше. В этой версии Kaspersky Security Center мастер массовой конвертации политик и задач позволяет перенести политики в профиль, а не в политику. Также в этой версии Kaspersky Security Center мастер массовой конвертации политики и задач позволяет перенести больше параметров политики.

Этапы миграции

Миграция с Легкого агента KSVLA на Легкий агент KES выполняется в полуавтоматическом режиме. Это связано с отличиями в архитектуре приложений.

Выполняйте миграцию с Легкого агента KSVLA на Легкий агент KES в следующем порядке:

1. **Выполните миграцию политик и задач Легкого агента KSVLA**

   Для миграции параметров политики вам нужно запустить мастер массовой конвертации политик и задач (мастер миграции). После переноса параметров политики необходимо вручную настроить параметры, которые мастер миграции не может перенести (например, параметры обновления баз). Также после миграции рекомендуется проверить, что мастер миграции перенес параметры корректно.

   > Если для ограничения доступа к Легкому агенту KSVLA включена Защита паролем, перед установкой Легкого агента KES необходимо выключить Защиту паролем в политике Легкого агента KSVLA. Ввести пароль деинсталляции в параметрах инсталляционного пакета Легкого агента KES невозможно. После завершения установки Легкого агент KES поверх Легкого агента KSVLA необходимо включить Защиту паролем в политике KES.

2. **Установите Kaspersky Endpoint Security в режиме Легкого агента**

   Вы можете установить Легкий агент KES следующими способами:

   - Установка Легкого агента KES после удаления Легкого агента KSVLA (рекомендуется).
   - Установка Легкого агента KES поверх Легкого агента KSVLA.

3. **Проверка работы приложения после миграции**

   После миграции с Легкого агента KSVLA на Легкий агент KES убедитесь, что приложение работает корректно. Активируйте сконвертированную политику. Проверьте статус виртуальной машины в консоли Kaspersky Security Center (*OK*). Убедитесь в отсутствии ошибок в работе приложения, также проверьте время последнего соединения с SVM и статус защиты виртуальной машины. Активировать Легкий агент не требуется, так как лицензионный ключ добавлен на SVM.

Установка Легкого агента KES вместо Легкого агента KSVLA

Вы можете установить Легкий агент KES следующими способами:

- Установка Легкого агента KES после удаления Легкого агента KSVLA (рекомендуется).
- Установка Легкого агента KES поверх Легкого агента KSVLA.

Удаление Легкого агента KSVLA

Вы можете удалить приложение дистанционно с помощью задачи *Удаленная установка приложения*, локально на виртуальной машине или шаблоне виртуальных машин. После удаления Легкого агента KSVLA может потребоваться перезагрузка виртуальной машины.

После удаления Легкого агента KSVLA установите Легкий агент KES любым доступным образом.

Если для ограничения доступа к Легкому агенту KSVLA включена Защита паролем, перед установкой Легкого агента KES необходимо выключить Защиту паролем в политике Легкого агента KSVLA. Ввести пароль деинсталляции в параметрах инсталляционного пакета Легкого агента KES невозможно. После завершения установки Легкого агент KES поверх Легкого агента KSVLA необходимо включить Защиту паролем в политике KES.

При установке Kaspersky Endpoint Security нужно выбрать режим **Легкий агент для защиты виртуальных сред**. Перед установкой Легкого агента KES на виртуальную машину установщик определяет Легкий агент KSVLA как несовместимое ПО и удаляет приложение. Миграция конфигурации Легкого агента KSVLA не поддерживается. То есть при установке Легкого агента KES будет установлен тот набор компонентов, который вы выбрали в свойствах инсталляционного пакета или в мастере установки. После удаления Легкого агента KSVLA необходимо перезагрузить виртуальную машину.

Параметры Легкого агента KSVLA и задачи не мигрируют при установке Легкого агента KES. Для переноса параметров и задач запустите мастер массовой конвертации политик и задач.

Вы можете проверить список установленных компонентов в интерфейсе приложения в разделе **Безопасность**, с помощью команды `status` или в консоли Kaspersky Security Center в свойствах компьютера. Вы можете изменить набор компонентов после установки с помощью задачи *Изменение состава компонентов приложения*.

Соответствие компонентов Легкого агента KSVLA и Легкого агента KES

Наборы компонентов Легкого агента KSVLA и Легкого агента KES практически совпадают. Легкий агент KES имеет больше параметров чем Легкий агент KSVLA. После миграции новые параметры имеют значения по умолчанию.

Соответствие компонентов Легкого агента KSVLA и Легкого агента KES

Легкий агент 5.2	Легкий агент KES
Ядро проверки	Ядро приложения
Файловый антивирус	Защита от файловых угроз
Почтовый антивирус	Защита от почтовых угроз
Веб-Антивирус	Защита от веб-угроз
Сетевой экран	Сетевой экран
Защита от сетевых атак	Защита от сетевых угроз
Контроль активности программ	Предотвращение вторжений
Контроль запуска программ	Контроль приложений
Веб-Контроль	Веб-Контроль
Контроль устройств	Контроль устройств
Мониторинг системы	В Kaspersky Endpoint Security этот компонент разделен на следующие компоненты: • Защита от эксплойтов • Анализ поведения • Откат вредоносных действий

Легкий агент 5.2	Легкий агент KES
Контроль целостности системы	Контроль целостности системы
Интеграция с Kaspersky Endpoint Agent	*(не поддерживается)* Начиная с версии Kaspersky Endpoint Security для Windows 11.9.0 дистрибутив приложения Kaspersky Endpoint Agent исключен из комплекта поставки приложения.
AMSI-защита	AMSI-защита

Миграция политик и задач Легкий агент KSVLA

Вы можете перенести параметры политик и задач Легкого агента KSVLA с помощью мастера массовой конвертации политик и задач (далее также "мастер миграции").

Мастер миграции для Легкого агента KSVLA доступен только в Консоли администрирования (MMC). Перенести параметры политик и задач в Web Console и Cloud Console невозможно.

Миграция политик и задачи имеет следующие особенности:

- Новая политика имеет название *<Политика> (конвертированная)*.
- Новая политика имеет статус *Неактивная политика*.
- Запрет на изменение параметров ("замок") не мигрирует. Мастер миграции устанавливает значения по умолчанию.
- Профили политики не мигрируют. Вам нужно добавить профили политики вручную.
- Улучшено управление доверенной зоной. В Легком агенте KSVLA вы могли добавлять предустановленные исключения только при создании политики. Далее в свойствах политики у вас была возможность настраивать уже добавленные предустановленные исключения или добавлять исключения вручную. Добавить предустановленные исключения в свойствах политики невозможно. В Легком агенте KES предустановленные исключения доступны и при создании политики, и в свойствах созданной политики. Также теперь вы можете выбирать предустановленные исключения в инсталляционном пакете.
- Настройка отображения интерфейса приложения в Kaspersky Endpoint Security перенесена из установщика в политику. Если вам нужно, например, скрыть интерфейс приложения, настройте параметры политики.
- Набор функциональных областей Kaspersky Endpoint Security и Легкого агента KSVLA для настройки прав доступа пользователей (RBAC) отличаются. Вам нужно настроить права доступа пользователя к функциональным областям заново.

Как перенести параметры политик Легкого агента KSVLA с помощью мастера массовой конвертации политик и задач

1. В Консоли администрирования выберите Сервер администрирования и по правой клавише мыши откройте контекстное меню.
2. Выберите пункт **Все задачи → Мастер массовой конвертации политик и задач**.

В результате запустится мастер массовой конвертации политик и задач. Следуйте его указаниям.

Шаг 1. Выбор приложения, для которого нужно конвертировать политики и задачи

На этом шаге нужно выбрать приложение Kaspersky Endpoint Security для Windows. Перейдите к следующему шагу.

Шаг 2. Конвертация политик

Выберите политику Kaspersky Security для виртуальных сред 5.2 Легкий агент для Windows, которую вы хотите конвертировать. Перейдите к следующему шагу.

Далее мастер миграции начнет конвертацию политик. В процессе конвертации мастер предложит вам принять условия Положения о KSN. Новая политика имеет название *<Политика> (конвертированная)*.

Шаг 3. Конвертация задач

Мастер миграции создает новые задачи для Kaspersky Endpoint Security для Windows. В списке задач выберите задачи Легкого агента KSVLA, которые вы хотите создать для Kaspersky Endpoint Security. Новые задачи будут иметь имя *<Название задачи> (конвертированная)*. Перейдите к следующему шагу.

Шаг 4. Завершение работы мастера

Завершите работу мастера.

После миграции политики необходимо открыть свойства политики, проверить параметры и сохранить политику. Если вы не выполните эти действия, Легкий агент KES может проигнорировать сконвертированную политику.

Обратите внимание на миграцию параметров подключения Легкого агента к SVM, списков исключений, доверенных приложений, доверенных веб-адресов, правил Контроля приложений.

Миграция конфигурации [Легкий агент KSVLA+KEA] на [Легкий агент KES+встроенный агент]

Для работы Kaspersky Endpoint Security для Windows в составе решений EDR (KATA), EDR Optimum, Kaspersky Sandbox в приложение добавлен встроенный агент. Теперь вам не нужно отдельное приложение Kaspersky Endpoint Agent для работы этих решений.

При миграции с Легкого агента KSVLA на Легкий агент KES решения EDR (KATA), EDR Optimum, Kaspersky Sandbox продолжат работу со встроенными агентами Kaspersky Endpoint Security. Также приложение Kaspersky Endpoint Agent будет удалено с компьютера.

Перед миграцией с Легкого агента KSVLA на Легкий агент KES нужно обновить все компоненты Kaspersky Security для виртуальных сред до версии 6.2, включая Сервер защиты и Сервер интеграции. Подробнее об обновлении версии решения Kaspersky Security для виртуальных сред Легкий агент см. в справке Kaspersky Security для виртуальных сред Легкий агент.

Миграция конфигурации [Легкий агент KSWLA+KEA] на [Легкий агент KES+встроенный агент] состоит из следующих этапов:

1. **Миграция политики и задач**

   Миграция политик и задач из [Легкого агента KSVLA+KEA] в [Легкий агент KES+встроенный агент] состоит из следующих этапов:

   1. Миграция политик и задач из Легкого агента KSVLA в Легкий агент KES с помощью мастера массовой конвертации политик и задач (доступно только в Консоли администрирования (MMC)).

      В результате будет создана новая политика с именем *<Политика> (конвертированная)*. Также будут созданы новые задачи KES с именем *<Название задачи> (конвертированная)*.

   2. Миграция политик и задач из KEA в KES с помощью мастера миграции с Kaspersky Endpoint Agent (доступно только в Web Console и Cloud Console).

      В результате будут создана новая политика с именем *<Название политики Kaspersky Endpoint Security> & <Название политики Kaspersky Endpoint Agent>*. Также будут созданы новые задачи и задачи KES.

2. **Миграция с Легкого агента KSVLA на Легкий агент KES**

   Миграция с Легкого агента KSVLA на Легкий агент KES включает в себя установку Легкого агента KES вместо Легкого агента KSVLA.

   Как правило, для ограничения доступа к Легкому агенту KSVLA и KEA администраторы включают Защиту паролем. Вы можете ввести только пароль деинсталляции KEA в параметрах задачи *Удаленная установка приложения*. Для миграции вам нужно выключить Защиту паролем для Легкого агента KSVLA.

   При миграции вам нужно выбрать соответствующие компоненты для работы решений Detection and Response в составе Kaspersky Endpoint Security. После установки приложения Kaspersky Endpoint Security перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent.

3. **Лицензирование функций**

   Если приложение используется в режиме Легкого агента, активировать приложение не требуется. Для активации приложения вам нужно добавить лицензионный ключ на SVM. Лицензионный ключ для активации дополнительных функций (например, EDR Optimum) тоже нужно добавить на SVM. Таким образом, при миграции лицензирование функций выполняется автоматически.

4. **Проверка работы Kaspersky Endpoint Detection and Response Optimum и Kaspersky Sandbox**

Если после обновления приложения компьютер имеет статус *Критический* в консоли Kaspersky Security Center, выполните следующие действия:

- Убедитесь, что на компьютере установлен Агент администрирования версии 13.2 или выше.
- Проверьте статус работы встроенного агента с помощью отчета *Отчет о статусе компонентов приложения*. Если компонент имеет статус *Не установлен*, установите компонент с помощью задачи *Изменение состава компонентов приложения*.
- Убедитесь, что вы приняли условия Положения о Kaspersky Security Network в новой политике Kaspersky Endpoint Security для Windows.
- Убедитесь в том, что функция EDR Optimum активирована с помощью отчета *Отчет о статусе компонентов приложения*. Если компонент имеет статус *Не поддерживается лицензией*, убедитесь, что функция автоматического распространения лицензионного ключа EDR Optimum включена.
- Проверьте статус подключения виртуальной машины к SVM. Вы можете получить информацию о состоянии подключения Легкого агента к SVM в интерфейсе Kaspersky Endpoint Security или с помощью команды приложения.

Управление приложением из командной строки

Вы можете управлять Kaspersky Endpoint Security из командной строки. Вы можете просмотреть список команд для управления приложением с помощью команды `avp.com HELP`. Чтобы получить справку по синтаксису конкретной команды, введите `avp.com HELP <command>`.

Специальные символы в команде нужно экранировать. Для экранирования символов `&`, `|`, `(`, `)`, `<`, `>`, `^` используйте символ `^` (например, чтобы использовать символ `&` введите `^&`). Для экранирования символа `%`, введите `%%`.

Вместо значения `1` могут использоваться значения `yes`, `on`, `enable`, `enabled`, `true`. Вместо значения `0` могут использоваться значения `no`, `off`, `disable`, `disabled`, `false`.

Setup. Установка приложения

Установка приложения из командной строки состоит из следующих этапов:

1. **Выбор дистрибутива**

   "Лаборатория Касперского" предоставляет дистрибутивы для разных локализаций, совместимые с разными архитектурами процессоров и включающие различные модули шифрования.

   Комплект поставки содержит следующие дистрибутивы:

   - **AES256**

     Дистрибутив предназначен для установки на компьютеры с x86/x64-архитектурой. Дистрибутив содержит криптографические средства, реализующие криптографический алгоритм AES (Advanced Encryption Standard) с эффективной длиной ключа 256 бит.

   - **AES56**

     Дистрибутив предназначен для установки на компьютеры с x86/x64-архитектурой. Дистрибутив содержит криптографические средства, реализующие криптографический алгоритм AES с эффективной длиной ключа 56 бит.

   - **Arm64**

     Дистрибутив предназначен для установки на компьютеры с Arm-архитектурой. Дистрибутив не предназначен для установки на серверы.

2. **Перемещение дистрибутива приложения в память компьютера**

   Дистрибутив представляет собой самораспаковывающийся архив в формате EXE. Для просмотра содержания дистрибутива вам нужно распаковать архив в отдельную папку. Для установки приложения нужны все файлы дистрибутива, включая файл bases.cab.

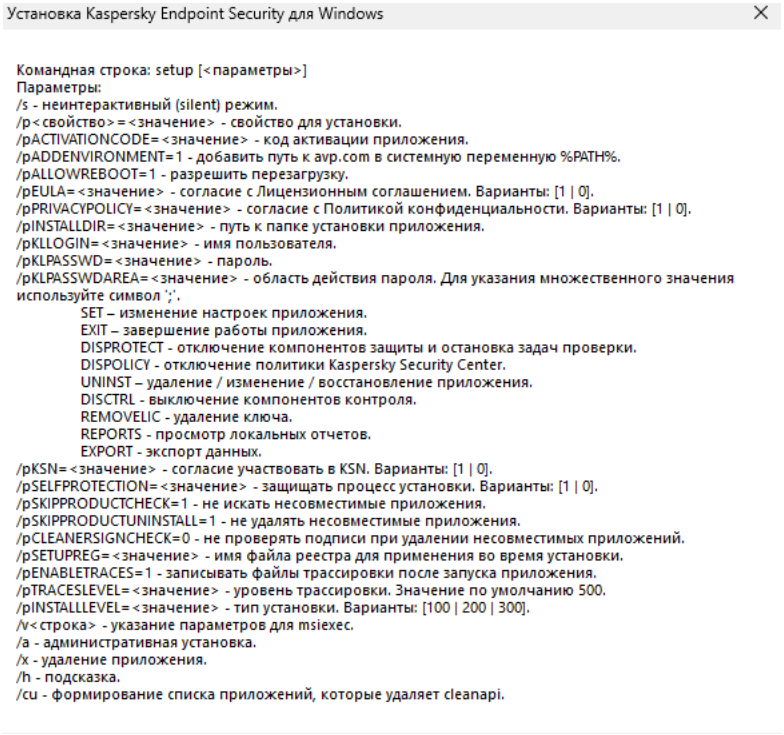
3. **Выполнение команды установки**

Установку Kaspersky Endpoint Security из командной строки можно выполнить в одном из следующих режимов:

- В интерактивном режиме с помощью мастера установки приложения.
- В тихом режиме. После запуска установки в тихом режиме ваше участие в процессе установки не требуется (тихая установка). Для установки приложения в тихом режиме используйте ключи `/s` и `/qn`.

Перед установкой приложения в тихом режиме откройте и прочитайте Лицензионное соглашение и текст Политики конфиденциальности. Лицензионное соглашение и текст Политики конфиденциальности входят в комплект поставки Kaspersky Endpoint Security. Приступайте к установке приложения, только если вы полностью прочитали, понимаете и принимаете положения и условия Лицензионного соглашения, если вы понимаете и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности, если вы полностью прочитали и понимаете Политику конфиденциальности. Если вы не принимаете положения и условия Лицензионного соглашения и Политику конфиденциальности, не устанавливайте и не используйте Kaspersky Endpoint Security.

Вы можете просмотреть список команд для установки приложения с помощью команды `/h`. Чтобы получить справку по синтаксису команды установки, введите `setup_kes.exe /h`. В результате инсталлятор покажет окно с описанием параметров команды (см. рис. ниже).



Описание параметров команды установки

Чтобы установить приложение или обновить предыдущую версию приложения, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security.

3. Выполните команду:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

или

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

В результате приложение будет установлено на компьютер. Вы можете убедиться, что приложение установлено, и проверить параметры приложения с помощью команды `status`.

Параметры установки приложения

`EULA=1`	Согласие с положениями Лицензионного соглашения. Текст Лицензионного соглашения входит в комплект поставки Kaspersky Endpoint Security. Согласие с положениями Лицензионного соглашения является необходимым условием для установки приложения или обновления версии приложения.
`PRIVACYPOLICY=1`	Согласие с Политикой конфиденциальности. Текст Политики конфиденциальности входит в комплект поставки Kaspersky Endpoint Security. Согласие с Политикой конфиденциальности является необходимым условием для установки приложения или обновления версии приложения.
`KSN`	Согласие или отказ участвовать в Kaspersky Security Network (KSN). Если параметр не указан, Kaspersky Endpoint Security запросит подтверждения участия в KSN при первом запуске приложения. Возможные значения: • `1` – согласие участвовать в KSN. • `0` – отказ участвовать в KSN (значение по умолчанию). Дистрибутив Kaspersky Endpoint Security оптимизирован для использования Kaspersky Security Network. Если вы отказались от участия в Kaspersky Security Network, то сразу после завершения установки обновите Kaspersky Endpoint Security.
`CONFIGPATH=<path to the configuration file>`	Установка приложение с заранее заданными параметрами. Для этого вам нужно загрузить файл, который задает параметры работы Kaspersky Endpoint Security. Вы можете создать конфигурационный файл в локальном интерфейсе приложения.
`ALLOWREBOOT=1`	Автоматическая перезагрузка компьютера после установки или обновления приложения, если требуется. Если параметр не задан, автоматическая перезагрузка компьютера запрещена. При установке Kaspersky Endpoint Security перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые приложения. Также перезагрузка может потребоваться при обновлении версии приложения.
`SKIPPRODUCTCHECK=1`	Выключение проверки установленного ПО. Список ПО, с которым могут быть проблемы совместимости, приведен в файле incompatible.txt в комплекте поставки. Если параметр не задан, при обнаружении приложения из списка установка Kaspersky Endpoint Security будет прекращена.
`SKIPPRODUCTUNINSTALL=1`	Запрет на автоматическое удаление найденных приложений из списка incompatible.txt. Если параметр не задан, Kaspersky Endpoint Security пытается удалить приложения, с которыми могут быть проблемы совместимости. Включить автоматическое удаление ПО при установке Kaspersky Endpoint Security с помощью установщика msiexec невозможно. Для автоматического удаления ПО, с которым могут быть проблемы совместимости, используйте файл setup_kes.exe.

`CLEANERSIGNCHECK=0|1`	Проверка цифровых подписей файлов найденного ПО из файла incompatible.txt. Для удаления ПО приложение Kaspersky Endpoint Security запускает файл инсталлятора программного обеспечения. Если у файла инсталлятора нет цифровой подписи, Kaspersky Endpoint Security считает такой файл недоверенным, и для предотвращения исполнения вредоносного кода приложение прекращает удаление ПО. Если приложение не может проверить цифровую подпись файла найденного ПО, установка Kaspersky Endpoint Security будет остановлена с ошибкой. Значение по умолчанию отличается в зависимости от способа установки приложения: • `0` – проверка цифровой подписи выключена (значение по умолчанию при развертывании через Kaspersky Security Center). • `1` – проверка цифровой подписи включена (значение по умолчанию при локальной установке приложения).
`STANDALONEMODE=1`	Установка приложения в конфигурации Endpoint Detection and Response агента (EDR-агент) для интеграции с решениями Kaspersky Endpoint Detection and Response (KATA) или Kaspersky Endpoint Detection and Response Expert (on-premises). Эта конфигурация нужна в том случае, если в вашей организации развернута система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков и решение класса Endpoint Detection and Response от "Лаборатории Касперского". Таким образом, Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента может быть совместим со сторонними EPP-приложениями.
`KLLOGIN`	Установка имени пользователя для доступа к управлению функциями и параметрами Kaspersky Endpoint Security (компонент Защита паролем). Имя пользователя устанавливается вместе с параметрами `KLPASSWD` и `KLPASSWDAREA`. По умолчанию используется имя пользователя KLAdmin.
`KLPASSWD`	Установка пароля для доступа к управлению функциями и параметрами Kaspersky Endpoint Security (пароль устанавливается вместе с параметрами `KLLOGIN` и `KLPASSWDAREA`). Если вы указали пароль, но не задали имя пользователя с помощью параметра `KLLOGIN`, то по умолчанию используется имя пользователя KLAdmin.
`KLPASSWDAREA`	Определение области действия пароля для доступа к Kaspersky Endpoint Security. При попытке пользователя выполнить действие из этой области Kaspersky Endpoint Security запрашивает учетные данные пользователя (параметры `KLLOGIN` и `KLPASSWD`). Для указания множественного значения используйте символ `;`. Возможные значения: • `SET` – изменение параметров приложения. • `EXIT` – завершение работы приложения. • `DISPROTECT` – выключение компонентов защиты и остановка задач проверки. • `DISPOLICY` – выключение политики Kaspersky Security Center. • `UNINST` – удаление приложения с компьютера. • `DISCTRL` – выключение компонентов контроля. • `REMOVELIC` – удаление ключа. • `REPORTS` – просмотр отчетов. • `EXPORT` – экспорт параметров приложения. Например, `KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT`. Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем. Поэтому настроить область действия пароля для учетной записи KLAdmin невозможно. Если вы попытаетесь настроить область действия пароля для учетной записи KLAdmin, приложение запретит перечисленные действия для группы "Все".
`PROTECTOSSERVICES`	Функция Защита сервисов операционной системы. Защита сервисов операционной системы предотвращает вмешательство сторонних приложений в работу сервисов операционной системы. К таким сервисам относится, например, сервис автозапуска приложений. • `1` – Защита сервисов операционной системы включена (значение по умолчанию). • `0` – Защита сервисов операционной системы выключена.
`ENABLETRACES`	Включение или выключение трассировки приложения. После запуска Kaspersky Endpoint Security приложение сохраняет файлы трассировки в папке `%ProgramData%\Kaspersky Lab\KES.14.3\Traces`. Возможные значения: • `1` – трассировка включена. • `0` – трассировка выключена (значение по умолчанию).
`TRACESLEVEL`	Уровень детализации трассировки. Возможные значения: • `100` (критический). Только сообщения о неустранимых ошибках. • `200` (высокий). Сообщения обо всех ошибках, включая неустранимые. • `300` (диагностический). Сообщения обо всех ошибках, а также предупреждения. • `400` (важный). Сообщения обо всех ошибках, предупреждения, а также дополнительная информация. • `500` (обычный). Сообщения обо всех ошибках, предупреждениях, а также подробная информация о работе приложения в нормальном режиме (значение по умолчанию). • `600` (низкий). Все сообщения.

ENABLEAZURESUPPORT	Включение или выключение режима совместимости с Azure WVD. Возможные значения: • 1 – режим совместимости с Azure WVD включен. • 0 – режим совместимости с Azure WVD выключен (значение по умолчанию). Функция позволяет корректно показывать состояние виртуальной машины Azure в консоли Kaspersky Anti Targeted Attack Platform. Для контроля за состоянием компьютера Kaspersky Endpoint Security отправляет на серверы KATA телеметрию. Телеметрия включает в себя идентификатор компьютера (Sensor ID). Режим совместимости с Azure WVD позволяет назначать постоянный уникальный Sensor ID для этих виртуальных машин. Если режим совместимости выключен, то из-за особенностей работы виртуальных машин Azure Sensor ID может изменяться после перезагрузки компьютера. Из-за этого возможно дублирование виртуальных машин в консоли.
AMPPL	Включение или выключение защиты процессов Kaspersky Endpoint Security с использованием технологии AM-PPL (Antimalware Protected Process Light). Подробнее о технологии AM-PPL см. на сайте Microsoft. Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019. Возможные значения: • 1 – защита процессов Kaspersky Endpoint Security с использованием технологии AM-PPL включена (значение по умолчанию). • 0 – защита процессов Kaspersky Endpoint Security с использованием технологии AM-PPL выключена.
UPGRADEMODE	Режим обновления приложения: • Seamless – обновление приложения с перезагрузкой компьютера (значение по умолчанию). • Force – обновление приложения без перезагрузки. Вы можете обновлять версию приложения без перезагрузки начиная с версии 11.10.0. Для обновление более ранних версий приложения необходимо выполнять перезагрузку компьютера. Также вы можете устанавливать патчи без перезагрузки начиная с версии 11.11.0. При установке Kaspersky Endpoint Security перезагрузка не требуется. Таким образом, режим обновления приложения будет установлен в параметрах приложения. Вы можете изменить этот параметр в настройках приложения или в политике. Если приложение уже установлено, при установке обновления приоритет параметра из командной строки ниже, чем параметр, заданный в настройках приложения или в файле setup.ini. То есть, если в командной строке задан режим Force, а в параметрах приложения задан режим Seamless, инсталлятор установит обновление с перезагрузкой (Seamless).
RESTAPI	Управление приложением через REST API. Для управления приложением через REST API обязательно нужно задать имя пользователя (параметр RESTAPI_User). Возможные значения: • 1 – управление через REST API разрешено. • 0 – управление через REST API запрещено (значение по умолчанию). Для управления приложением через REST API должно быть разрешено управление с помощью систем администрирования. Для этого задайте параметр AdminKitConnector=1. Если вы управляете приложением через REST API, управлять приложением с помощью систем администрирования "Лаборатории Касперского" невозможно.
RESTAPI_User	Имя пользователя доменной учетной записи Windows для управления приложением через REST API. Управление приложением через REST API доступно только этому пользователю. Введите имя пользователя в формате <DOMAIN>\<UserName> (например, RESTAPI_User=COMPANY\Administrator). Для работы с REST API вы можете выбрать только одного пользователя. Добавление имени пользователя является необходимым условием для управления приложением через REST API.
RESTAPI_Port	Порт для управления приложением через REST API. По умолчанию используется порт 6782. Убедитесь, что порт свободен.
RESTAPI_Certificate	Сертификат для идентификации запросов (например, RESTAPI_Certificate=C:\cert.pem). Для безопасной работы Kaspersky Endpoint Security с REST-клиентом вам нужно настроить идентификацию запросов. Для этого вам нужно установить сертификат и в дальнейшем подписывать полезные данные каждого запроса.
ADMINKITCONNECTOR	Управление приложением с помощью систем администрирования. К системам администрирования относится, например, Kaspersky Security Center. Кроме систем администрирования "Лаборатории Касперского" вы можете использовать сторонние решения. Для этого Kaspersky Endpoint Security предоставляет API. Возможные значения: • 1 – управление приложением с помощью систем администрирования разрешено (значение по умолчанию). • 0 – разрешено управление приложением только через локальный интерфейс.

`EnableUniqueSensorID`	Создание уникального идентификатора компьютера (Sensor ID) при установке или обновлении приложения. Sensor ID используется в решении Kaspersky Anti Targeted Attack Platform для идентификации компьютеров, которые отправляют телеметрию на сервер. При создании Sensor ID приложение использует алгоритм, который учитывает конфигурацию компьютера, например, серийный номер материнской платы. В некоторых случаях, например, при использовании приложения в виртуальной среде, Sensor ID может повторяться. Таким образом, Kaspersky Anti Targeted Attack Platform не может идентифицировать компьютер, с которого отправлена телеметрия. Для создания уникального Sensor ID вам нужно задать параметр `EnableUniqueSensorID=1`. В результате приложение будет использовать другой алгоритм для создания Sensor ID, который учитывает другие данные о компьютере. Это обеспечивает уникальный Sensor ID. По умолчанию параметр не задан. Приложение наследует Sensor ID в следующих случаях: • обновление версии приложения; • миграция конфигурации [KES+KEA] на [KES+встроенный агент]. При восстановлении приложения установщик пытается наследовать Sensor ID. Если восстановить Sensor ID не удалось, приложение создает новый Sensor ID.
`SKIPKB5007186CHECK=1`	Выключение проверки установленного обновления операционной системы KB5007186. Перед установкой приложения установщик проверяет наличие обновлений операционной системы. Обновление KB5007186 входит в список обновлений операционной системы, которые могут привести к проблемам в работе приложения. Подробнее см. в базе знаний Службы технической поддержки. Поэтому установщик, обнаружив это обновление, останавливает установку приложения. Для продолжения установки приложения задайте параметр `SKIPKB5007186CHECK=1`.

Пример

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

После установки приложения Kaspersky Endpoint Security происходит активация по пробной лицензии, если вы не указали код активации в файле setup.ini. Пробная лицензия обычно имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Endpoint Security прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно активировать приложение по коммерческой лицензии с помощью мастера активации приложения или специальной команды.

Во время установки приложения или обновления версии приложения в тихом режиме поддерживается использование следующих файлов:

- setup.ini – общие параметры установки приложения.

  Чтобы применить параметры из файла setup.ini, разместите файл в папке с дистрибутивом Kaspersky Endpoint Security.

- install.cfg – параметры работы Kaspersky Endpoint Security.

  Чтобы применить параметры из конфигурационного файла install.cfg вам нужно указать путь к файлу в команде установки приложения: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – ключи реестра.

  Запись ключей реестра из файла setup.reg в реестр осуществляется, только если в файле setup.ini указано значение `setup.reg` для параметра `SetupReg`. Файл setup.reg формируется специалистами "Лаборатории Касперского". Не рекомендуется изменять содержимое этого файла. Чтобы применить параметры из файла setup.reg, разместите файл в папке с дистрибутивом Kaspersky Endpoint Security. Также вы можете разместить файл setup.reg в другой папке. В этом случае вам нужно указать путь к файлу в команде установки приложения: `SETUPREG=<path to the setup.reg file>`.

Setup /x. Удаление приложения

Удаление Kaspersky Endpoint Security из командной строки можно выполнить в одном из следующих режимов:

- В интерактивном режиме с помощью мастера установки приложения.
- В тихом режиме. После запуска удаления в тихом режиме ваше участие в процессе удаления не требуется (тихое удаление). Для удаления приложения в тихом режиме используйте ключи `/s` и `/qn`.

Чтобы удалить приложение в тихом режиме, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security.
3. Выполните команду:

   - Если операция удаления не защищена паролем:

     ```
     setup_kes.exe /s /x
     ```

     или

     ```
     msiexec.exe /x <GUID> /qn
     ```

     где `<GUID>` – уникальный идентификатор приложения. Вы можете узнать GUID приложения в базе знаний Службы технической поддержки или с помощью команды:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Если операция удаления защищена паролем:

     ```
     setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```

     или

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Также вы можете использовать параметр `SAVEQB` для сохранения файлов, проверенных приложением и помещенных в резервное хранилище. Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES.14.3\QB`. По умолчанию сохранение файлов в резервном хранилище выключено (`SAVEQB=0`).

Пример

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. Восстановление приложения

При восстановлении приложение проверяет и восстанавливает целостность всех поврежденных модулей приложения и ключей системного реестра, созданных при установке приложения.

Восстановление Kaspersky Endpoint Security из командной строки можно выполнить в одном из следующих режимов:

- В интерактивном режиме с помощью мастера установки приложения.
- В тихом режиме. После запуска восстановления в тихом режиме ваше участие в процессе восстановления не требуется.

Если инсталлятор Kaspersky Endpoint Security запущен в режиме восстановления, а приложение не требует восстановления, то инсталлятор не выполняет никаких изменений.

Если инсталлятор Kaspersky Endpoint Security запущен в режиме восстановления, а приложение не установлено, то инсталлятор запустит установку приложения.

Чтобы восстановить приложение в тихом режиме, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security.
3. Выполните команду:
   - Если операция восстановления не защищена паролем:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     где `<GUID>` – уникальный идентификатор приложения. Вы можете узнать GUID приложения в базе знаний Службы технической поддержки или с помощью команды:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Если операция восстановления защищена паролем:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Пример

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

Команды AVP

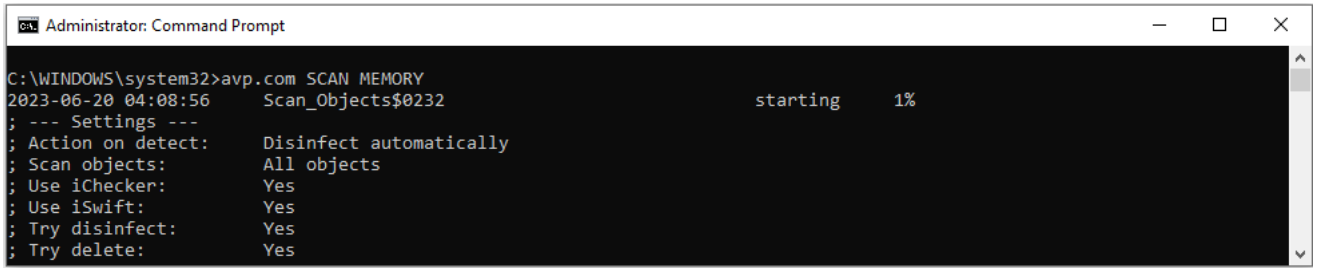
Чтобы управлять Kaspersky Endpoint Security из командной строки, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

   Вы можете добавить в системную переменную %PATH% путь к исполняемому файлу при установке приложения.
3. Используйте следующий шаблон для выполнения команды:

```
avp.com <command> [options]
```

В результате Kaspersky Endpoint Security выполнит команду (см. рис. ниже).



Управление приложением из командной строки

SCAN. Поиск вредоносного ПО

Запуск задачи *Поиск вредоносного ПО*.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

Область проверки	
`<files to scan>`	Список файлов и папок через пробел. Длинные пути должны быть заключены в кавычки. Короткие пути (формат MS-DOS) заключать в кавычки не требуется. Например: • `"C:\Program Files (x86)\Example Folder"` – длинный путь. • `C:\PROGRA~2\EXAMPL~1` – короткий путь.

`/ALL`	Запустить задачу *Поиск вредоносного ПО*. Kaspersky Endpoint Security проверяет следующие объекты: • память ядра; • объекты, загрузка которых осуществляется при запуске операционной системы; • загрузочные секторы; • резервное хранилище операционной системы; • все жесткие и съемные диски. В Kaspersky Endpoint Security для Windows версии 12.12 почта исключена из области проверки приложения. Проверку входящих и исходящих сообщений выполняет компонент Защита от почтовых угроз. Если вы используете плагин управления более ранней версии, то приложение исключает почту из области проверки, даже если эта область включена в политике.
`/MEMORY`	Проверить память ядра.
`/STARTUP`	Проверить объекты, загрузка которых осуществляется при запуске операционной системы.
`/REMDRIVES`	Проверить съемные диски.
`/FIXDRIVES`	Проверить жесткие диски.
`/NETDRIVES`	Проверить сетевые диски.
`/QUARANTINE`	Проверить файлы в резервном хранилище Kaspersky Endpoint Security.
`/@:<file list.lst>`	Проверить файлы и папки, перечисленные в списке. Каждый файл из списка нужно вводить с новой строки. Длинные пути должны быть заключены в кавычки. Короткие пути (формат MS-DOS) заключать в кавычки не требуется. Например: • `"C:\Program Files (x86)\Example Folder"` – длинный путь. • `C:\PROGRA~2\EXAMPL~1` – короткий путь.

Действие при обнаружении угрозы	
`/i0`	**Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз.
`/i1`	**Лечить. Информировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security добавляет информацию об обнаруженных зараженных файлах в список активных угроз.
`/i2`	**Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл. Этот вариант действия выбран по умолчанию.
`/i3`	**Удалять, если лечение невозможно**. Также удалять составные файлы (например, архивы), если вылечить или удалить зараженный файл невозможно.
`/i4`	**Удалять**. Также удалять составные файлы (например, архивы), если удалить зараженный файл невозможно.

Типы файлов	
`/fe`	**Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
`/fi`	**Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.
`/fa`	**Все файлы**. Если выбран этот параметр, приложение проверяет все файлы без исключения (любых форматов и расширений). Параметр выбран по умолчанию.

Исключения из проверки	
`-e:a`	Исключение из проверки архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
`-e:<file mask>`	Исключение из проверки файлов по маске. Например: • Маска `*.exe` будет включать все пути к файлам с расширением exe. • Маска `example*` будет включать все пути к файлам с именем EXAMPLE.
`-e:<seconds>`	Исключение из проверки файлов, длительность проверки которых превышает установленное значение в секундах.
`-es:<megabytes>`	Исключение из проверки файлов, размер которых превышает установленное значение в мегабайтах.

Режим сохранения событий в файл отчета (только для профилей Scan, Updater, Rollback)	
`/R:<report file>`	Сохранять только критические события в файл отчета.
`/RA:<report file>`	Сохранять все события в файл отчета.

Технологии проверки	
`/iChecker=on|off`	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
`/iSwift=on|off`	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.

Дополнительные параметры	
`/C:<file with scan settings>`	Файл с параметрами задачи *Поиск вредоносного ПО*. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Пример

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Обновление баз и модулей приложения

Запуск задачи *Обновление баз и модулей приложения*.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Параметры задачи обновления	
`local`	Запуск задачи *Обновление баз и модулей приложения*, созданной автоматически после установки приложения. Вы можете изменить параметры задачи *Обновление баз и модулей приложения* в локальном интерфейсе приложения или в консоли Kaspersky Security Center. Если этот параметр не установлен, Kaspersky Endpoint Security запускает задачу *Обновление баз и модулей приложения* с параметрами по умолчанию или с параметрами, заданными в команде. Таким образом, вы можете настроить параметры задачи *Обновление баз и модулей приложения*, следующим образом: • `UPDATE` – запуск задачи *Обновление баз и модулей приложения* с параметрами по умолчанию: источник обновлений – серверы обновлений "Лаборатории Касперского", учетная запись – System, и другие. • `UPDATE local` – запуск задачи *Обновление баз и модулей приложения*, созданной автоматически после установки (предустановленная задача). • `UPDATE <update settings>` – запуск задача *Обновление баз и модулей приложения* с параметрами, заданными вручную (см. ниже).

Источник обновлений	
`"<update source>"`	Адрес HTTP-, FTP-сервера или папки общего доступа с пакетом обновлений. Вы можете указать только один источник обновлений. Если источник обновлений не указан, Kaspersky Endpoint Security использует источник по умолчанию – серверы обновлений "Лаборатории Касперского".

Режим сохранения событий в файл отчета (только для профилей Scan, Updater, Rollback)	
`/R:<report file>`	Сохранять только критические события в файл отчета.
`/RA:<report file>`	Сохранять все события в файл отчета.

Дополнительные параметры	
`/C:<file with update settings>`	Файл с параметрами задачи *Обновление баз и модулей приложения*. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: `["<update source>"] [/R[A]: <report file>]`.

Пример

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Откат последнего обновления

Откат последнего обновления антивирусных баз. Это позволяет вернуться к использованию предыдущей версии баз и модулей приложения при необходимости, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасное приложение.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Режим сохранения событий в файл отчета (только для профилей Scan, Updater, Rollback)	
`/R:<report file>`	Сохранять только критические события в файл отчета.
`/RA:<report file>`	Сохранять все события в файл отчета.

Пример

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Трассировка

Файлы трассировки хранятся на вашем компьютере в течение всего времени использования приложения и безвозвратно удаляются при удалении приложения. Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке `%ProgramData%\Kaspersky Lab\KES.14.3\Traces`. По умолчанию трассировка выключена.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Уровень трассировки	
`<tracing level>`	Уровень детализации трассировки. Возможные значения: • `100` (критический). Только сообщения о неустранимых ошибках. • `200` (высокий). Сообщения обо всех ошибках, включая неустранимые. • `300` (диагностический). Сообщения обо всех ошибках, а также предупреждения. • `400` (важный). Сообщения обо всех ошибках, предупреждения, а также дополнительная информация. • `500` (обычный). Сообщения обо всех ошибках, предупреждениях, а также подробная информация о работе приложения в нормальном режиме (значение по умолчанию). • `600` (низкий). Все сообщения.

Дополнительные параметры	
`all`	Выполнить команду с параметрами `file` и `mem`.
`file`	Сохранить один файл трассировки (без ограничений по размеру).

`rot`	Сохранить результаты трассировки в ограниченное число комплектов файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера.
`mem`	Записывать результаты трассировки в файлы дампов.

Пример

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Запуск профиля

Запуск профиля (например, запуск обновления баз или включение компонента защиты).

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com START <profile> [/R[A]:<report file>]
```

Профиль	
`<profile>`	Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей вы можете узнать по команде `HELP START`.

Режим сохранения событий в файл отчета (только для профилей Scan, Updater, Rollback)	
`/R:<report file>`	Сохранять только критические события в файл отчета.
`/RA:<report file>`	Сохранять все события в файл отчета.

Пример

```
avp.com START Scan_Objects
```

STOP. Остановка профиля

Остановка выполнения профиля (например, остановка проверки съемных дисков или выключение компонента защиты).

> Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешения **Выключение компонентов защиты**, **Выключение компонентов контроля**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Профиль	
`<profile>`	Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей вы можете узнать по команде `HELP STOP`.

Авторизация	
`/login=<user name> /password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

STATUS. Статус профиля

Отображение информации о состоянии профилей приложения (например, `running` или `completed`). Список доступных профилей вы можете узнать по команде `HELP STATUS`.

> Также Kaspersky Endpoint Security показывает информацию о состоянии служебных профилей. Информация о состоянии служебных профилей может понадобиться при обращении в Службу технической поддержки "Лаборатории Касперского".

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com STATUS [<profile>]
```

Если вы введете команду без профиля, Kaspersky Endpoint Security покажет состояние всех профилей приложения.

STATISTICS. Статистика выполнения профиля

Отображение статистической информации о профиле приложения (например, время проверки или количество обнаруженных угроз). Список доступных профилей вы можете узнать по команде `HELP STATISTICS`.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com STATISTICS <profile>
```

RESTORE. Восстановление файлов из резервного хранилища

Восстановление файла из резервного хранилища в папку его исходного размещения. Если по указанному пути уже существует файл с таким же именем, приложение запросит подтверждение для замены файла. Восстанавливаемый файл копируется с исходным именем.

> Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение **Восстановление из резервного хранилища**.

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES.14.3\QB`.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security.

> В Kaspersky Endpoint Security отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Дополнительные параметры	
`/REPLACE`	Переписать существующий файл.
`<file name>`	Имя восстанавливаемого файла.

Авторизация	
`/login=<user name> /password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

Пример

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Экспорт параметров приложения

Экспорт параметров Kaspersky Endpoint Security в файл. Если в команде указано только имя файла, в который нужно экспортировать параметры, приложение размещает файл следующим образом:

- Если путь к avp.com добавлен в системную переменную %PATH%, приложение помещает файл в папку `C:\Windows\SysWOW64`.
- Если вы выполняете команду из папки установки приложения, экспорт завершится с ошибкой, так как самозащита приложения заблокирует создание нового файла в папке приложения. Для экспорта параметров приложения в файл введите путь к файлу.

Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение **Экспорт настроек**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Профиль	
`<profile>`	Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей вы можете узнать по команде `HELP EXPORT`.

Файл для экспорта	
`<file name>`	Имя файла, в который должны быть экспортированы параметры профиля. Также вы можете ввести путь к файлу. Вы можете экспортировать параметры профиля в конфигурационный файл в формате DAT или CFG, в текстовый файл в формате TXT или в документ в формате XML.

Авторизация	
`/login=<user name> /password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

Пример

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Импорт параметров приложения

Импорт параметров Kaspersky Endpoint Security из файла, который был создан с помощью команды `EXPORT`.

Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение **Настройка приложения**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Файл для импорта	
`<file name>`	Имя файла, из которого должны быть импортированы параметры приложения. Вы можете импортировать параметры Kaspersky Endpoint Security из конфигурационного файла в формате DAT или CFG, текстового файла в формате TXT или документа в формате XML.

Авторизация	
`/login=<user name> /password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

Пример

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Применение файла ключа

Активация Kaspersky Endpoint Security с помощью файла ключа. Если приложение уже активировано, ключ будет добавлен в качестве резервного.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Файл ключа	
`<file name>`	Имя файла ключа.

Авторизация	
`/login=<user name> /password=<password>`	Данные учетной записи пользователя. Данные учетные записи нужно вводить, только если включена Защита паролем.

Пример

```
avp.com ADDKEY file.key
```

LICENSE. Лицензирование

Управление лицензионными ключами приложения Kaspersky Endpoint Security, а также ключами решений EDR Optimum или EDR Expert (Kaspersky Endpoint Detection and Response Add-on).

Для выполнения команды удаления лицензионного ключа должна быть включена Защита паролем. Пользователь должен иметь разрешение **Удаление ключа**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Операция	
`/ADD <file name>`	Активация Kaspersky Endpoint Security с помощью файла ключа. Если приложение уже активировано, ключ будет добавлен в качестве резервного.
`/ADD <activation code>`	Активировать Kaspersky Endpoint Security с помощью кода активации. Если приложение уже активировано, ключ будет добавлен в качестве резервного.
`/REFRESH`	Обновить статус лицензии Kaspersky Endpoint Security. В результате приложение получает актуальную информацию о статусе лицензии с серверов активации "Лаборатории Касперского".

`/REFRESH <license ID>`	Обновить статус лицензий по лицензионному идентификатору. С помощью этой команды вы можете обновить статус лицензий EDR Add-on, MDR Add-on, KUMA Add-on или другой лицензии. Вы можете узнать лицензионный идентификатор в лицензионном сертификате. В результате приложение получает актуальную информацию о статусе лицензии с серверов активации "Лаборатории Касперского".
`/CHECK`	Получить информацию о лицензии. Kaspersky Endpoint Security показывает информацию обо всех добавленных лицензионных ключах, включая резервные ключи и ключи EDR Add-on, MDR Add-on, KUMA Add-on и другие ключи. Kaspersky Endpoint Security показывает следующую информацию о лицензии: • название лицензии; • идентификатор лицензии; • адрес Сервера защиты (SVM), к которому подключена виртуальная машина с приложением, установленным в режиме Легкого агента; • тип лицензии: пробная, коммерческая, beta, подписка; • дата и время активации приложения; • дата и время истечения срока действия лицензии; • количество дней до истечения срока действия лицензии.
`/CHECK <license ID>`	Получить информацию о лицензии по идентификатору. С помощью этой команды вы можете получить информацию о лицензии. Вы можете узнать лицензионный идентификатор в лицензионном сертификате.
`/DEL /login=<user name> /password= <password>`	Удалить лицензионный ключ приложения. Также будет удален резервный ключ.
`/DEL <license ID> /login=<user name> /password=<password>`	Удалить ключ по лицензионному идентификатору. С помощью этой команды вы можете удалить ключ от лицензий EDR Add-on, MDR Add-on, KUMA Add-on или другой ключ. Вы можете узнать лицензионный идентификатор в лицензионном сертификате.

Авторизация	
`/login=<user name> /password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

Пример

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Пример

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. Приобретение лицензии

Переход на веб-сайт "Лаборатории Касперского" для приобретения лицензии или продления ее срока действия.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

PBATESTRESET. Сброс результатов проверки перед шифрованием диска

Сброс результатов проверки поддержки полнодискового шифрования (FDE) по технологиям Шифрование диска Kaspersky и BitLocker.

Перед запуском полнодискового шифрования приложение выполняет ряд проверок на возможность шифрования компьютера. Если полнодисковое шифрование невозможно, Kaspersky Endpoint Security сохраняет информацию о несовместимости. При следующей попытке шифрования приложение не выполняет проверки и предупреждает о том, что шифрование невозможно. Если аппаратная конфигурация компьютера изменилась, то для проверки системного жесткого диска на совместимость с технологией Шифрования диска Kaspersky или BitLocker требуется сбросить информацию о несовместимости, полученную приложением при предыдущей проверке.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

EXIT. Завершение работы приложения

Завершение работы Kaspersky Endpoint Security. Приложение будет выгружено из оперативной памяти компьютера.

> Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение **Завершение работы приложения**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Выключение политики

Выключение политики Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком (🔒).

> Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение **Выключение политики Kaspersky Security Center**.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Включение политики

Включение политики Kaspersky Security Center на компьютере. Параметры приложения будут настроены в соответствии с политикой.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

DISABLE. Выключение защиты

Выключение Защиты от файловых угроз на компьютере с истекшей лицензией на Kaspersky Endpoint Security. Выполнить команду на компьютере с неактивированным приложением или с действующей лицензией невозможно.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

SPYWARE. Обнаружение шпионского ПО

Управление обнаружением шпионского ПО. По умолчанию обнаружение шпионского ПО включено.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com SPYWARE on|off
```

KSN. Переключение KSN / KPSN

Выбор решения "Лаборатории Касперского" для определения репутации файлов или сайтов. Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения для работы с репутационными базами "Лаборатории Касперского":

- *Kaspersky Security Network (KSN)* – это решение, которое используют большинство приложений "Лаборатории Касперского". Участники KSN получают информацию от "Лаборатории Касперского", а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.

- *Kaspersky Private Security Network (KPSN)* – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров. KPSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

  - отсутствие подключения локальных рабочих мест к сети Интернет;

  - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
avp.com KSN /global | /private <file name>
```

Конфигурационный файл Kaspersky Security Network	
`<file name>`	Имя конфигурационного файла с параметрами Kaspersky Private Security Network. Файл имеет разрешение PKCS7 или PEM.

Пример

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Пример

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Выключение защиты подключения к серверу

Запуск задачи *Защита подключения к Серверу администрирования*, которая удаляет пароль для подключения компьютера к Серверу администрирования. Таким образом, задача выключает защиту подключения к Серверу администрирования.

Для выполнения команды должна быть включена Защита паролем.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Пароль	
/password=<password>	Пароль учетной записи KLAdmin или пароль из задачи *Защита подключения к Серверу администрирования*. Если параметр не задан, Kaspersky Endpoint Security предложит ввести пароль в следующей строке.

ZTNA. Удаленный доступ

Данная функция находится на этапе бета-тестирования и доступна только участникам программы бета-тестирования решений "Лаборатории Касперского". Работа функции может быть нестабильной.

Команды управления Удаленным доступом:

- Установление или разрыв VPN-соединения.
- Отображение текущего статуса VPN-соединения.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com ZTNA CONNECT /server=<server address>:<port>
```

```
avp.com ZTNA DISCONNECT
```

```
avp.com ZTNA status
```

Операция	
`connect`	Установить VPN-соединение. Для установления VPN-соединения нужно указать адрес удаленного сервера (`/server=<server address>:<port>`).
`disconnect`	Разорвать VPN-соединение.
`status`	Показать текущий статус VPN-соединения. В результате вы получите следующий ответ: • `Connecting` • `Connected` • `Reconnecting` • `Disconnected` Для статусов `Reconnecting` и `Disconnected` приложение показывает возможную причину отсутствия VPN-соединения. Например: • `ProxyAuthError` • `ServerCertificateError` • `UserVpnSessionLimitExceededError`

Команды KESCLI

Команды KESCLI позволяют получать информацию о состоянии защиты компьютера с помощью компонента OPSWAT, а также выполнять стандартные задачи (например, *Поиск вредоносного ПО*, *Обновление баз и модулей приложения*).

Вы можете просмотреть список команд KESCLI с помощью команды `kescli --help` или сокращенной команды `kescli -h`.

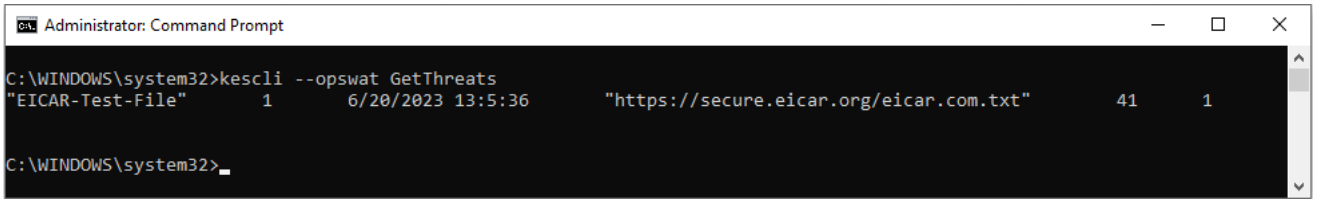
Чтобы управлять Kaspersky Endpoint Security из командной строки, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

   Вы можете добавить в системную переменную %PATH% путь к исполняемому файлу при установке приложения.
3. Используйте следующий шаблон для выполнения команды:

   ```
   kescli <command> [options]
   ```

В результате Kaspersky Endpoint Security выполнит команду (см. рис. ниже).



Управление приложения из командной строки

Scan. Поиск вредоносного ПО

Запуск задачи *Поиск вредоносного ПО* (Полная проверка).

> Для запуска задачи администратору нужно разрешить использование локальных задач в политике.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

Вы можете проверить статус выполнения задачи *Поиск вредоносного ПО* с помощью команды `GetScanState` и посмотреть дату и время последнего выполнения проверки с помощью команды `GetLastScanTime`.

Область проверки	
`<scan scope>`	Список файлов и папок через символ `;`. Например, `"C:\Program Files (x86)\Example Folder"`.

Действие при обнаружении угрозы	
`0`	**Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз.
`1`	**Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл. Этот вариант действия выбран по умолчанию.

Пример

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. Статус выполнения проверки

Отображение информации о статусе выполнения задачи *Поиск вредоносного ПО* (*Полная проверка*):

- `1` – проверка выполняется.
- `0` – проверка не запущена.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat GetScanState
```

GetLastScanTime. Определения времени выполнения проверки

Отображение информации о дате и времени последнего выполнения задачи *Поиск вредоносного ПО* (*Полная проверка*).

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat GetLastScanTime
```

GetThreats. Получение данных об обнаруженных угрозах

Отображение списка обнаруженных угроз (*Отчет об угрозах*). Отчет содержит информацию об угрозах и вирусной активности за 30 дней до момента создания отчета.

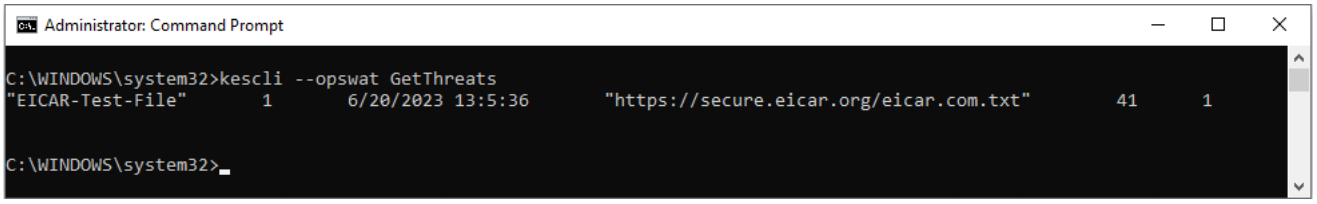
Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat GetThreats
```

В результате выполнение команды Kaspersky Endpoint Security отправит ответ в следующем формате:

```
<name of detected object> <type of object> <detection date and time> <path to file>
<action on threat detection> <threat danger level>
```



Управление приложением из командной строки

Тип объекта	
0	Неизвестно (Unknown).
1	Вирусы (Virware).
2	Троянские приложения (Trojware).
3	Вредоносные приложения (Malware).
4	Рекламные приложения (Adware).
5	Приложения автодозвона (Pornware).

6	Приложения, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя (`Riskware`).
7	Упакованные объекты, способ упаковки которых может использоваться для защиты вредоносного кода (`Packed`).
20	Неизвестные объекты (`Xfiles`).
21	Известные приложения (`Software`).
22	Скрытые файлы (`Hidden`).
23	Приложения, требующие вашего внимания (`Pupware`).
24	Аномальное поведение (`Anomaly`).
30	Не определено (`Undetect`).
40	Рекламные баннеры (`Banner`).
50	Сетевая атака (`Attack`).
51	Доступ к реестру (`Registry`).
52	Подозрительные действия (`Suspicion`).
60	Уязвимости (`Vulnerability`).
70	Фишинг (`Phishing`).
80	Нежелательные почтовые вложения (`Attachment`).
90	Вредоносное приложение, обнаруженная с помощью Kaspersky Security Network (`Urgent`).
100	Неизвестная ссылка (`Suspic URL`).
110	Другое вредоносное приложение (`Behavioral`).

Действие при обнаружении угрозы	
0	Неизвестно (`unknown`).
1	Угроза устранена (`ok`).
2	Объект заражен и не вылечен (`infected`).
5	Объект в архиве и не вылечен (`archive`).
9	Объект вылечен (`disinfected`).
10	Объект не вылечен (`not disinfected`).
11	Объект удален (`deleted`).
13	Создана резервная копия объекта (`backupped`).
15	Объект помещен в резервное хранилище (`quarantined`).
23	Объект удален при перезагрузке компьютера (`delete on reboot`).
25	Объект вылечен при перезагрузке компьютера (`disinfect on reboot`).
29	Объект помещен в резервное хранилище пользователем (`added by user`).
30	Объект добавлен в исключения (`added to exclude`).
31	Объект помещен в резервное хранилище при перезагрузке компьютера (`quarantine on reboot`).
36	Ложное срабатывание (`false alarm`).
38	Процесс завершен (`terminated`).
40	Объект не обнаружен (`not found`).
41	Невозможно устранить угрозу (`untreatable`).
42	Объект восстановлен (`rolled back`).
43	Объект создан в результате активности угрозы (`produced by threat`).

44	Объект восстановлен при перезагрузке компьютера (`roll back on reboot`).
0xffffffff	Объект не обработан (`discarded`).

Уровень опасности угрозы	
0	Неизвестно
1	Высокий
2	Средний
4	Низкий
8	Информационный (ниже уровня *Низкий*)

UpdateDefinitions. Обновление баз и модулей приложения

Запуск задачи *Обновление баз и модулей приложения*. Kaspersky Endpoint Security использует источник по умолчанию – серверы обновлений "Лаборатории Касперского".

Для запуска задачи администратору нужно разрешить использование локальных задач в политике.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Команду невозможно выполнить, если приложение установлено в режиме Легкого агента.

Синтаксис команды

```
kescli --opswat UpdateDefinitions
```

Вы можете просмотреть дату и время выпуска используемых антивирусных баз с помощью команды `GetDefinitionsetState`.

GetDefinitionState. Определение даты и времени последнего обновления баз

Отображение информации о дате и времени последнего обновления антивирусных баз.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat GetDefinitionState
```

EnableRTP. Включение защиты

Включение компонентов защиты Kaspersky Endpoint Security на компьютере: Защита от файловых угроз, Защита от веб-угроз, Защита от почтовых угроз, Защита от сетевых угроз, Предотвращение вторжений.

> Для включения компонентов защиты администратору нужно убедиться, что необходимые параметры в политике доступны для изменения (атрибуты открыты).

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat EnableRTP
```

В результате компоненты защиты будут включены, даже если вы запретили изменение параметров приложения с помощью Защиты паролем.

Вы можете проверить статус работы Защиты от файловых угроз с помощью команды `GetRealTimeProtectionState`.

GetRealTimeProtectionState. Статус Защиты от файловых угроз

Отображение информации о статусе работы компонента Защита от файловых угроз:

- `1` – компонент включен.
- `0` – компонент выключен.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Статус шифрования диска

Отображение информации о статусе шифрования диска:

- `1` – диск защищен с помощью технологии шифрования Kaspersky или BitLocker.
- `0` – диск не зашифрован.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --opswat GetEncryptionState
```

Version. Определение версии приложения

Отображение версии приложения Kaspersky Endpoint Security для Windows.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

Синтаксис команды

```
kescli --Version
```

Вы также можете использовать сокращенную команду `-v`.

Команды управления Detection and Response

Вы можете управлять встроенными функциями решений Detection and Response из командной строки (например, Kaspersky Sandbox или Kaspersky Endpoint Detection and Response Optimum). Вы можете управлять решениями Detection and Response, если управление через консоль Kaspersky Security Center невозможно. Вы можете просмотреть список команд для управления приложением с помощью команды `HELP`. Чтобы получить справку по синтаксису конкретной команды, введите `HELP <command>`.

Чтобы управлять встроенными функциями решений Detection and Response из командной строки, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Используйте следующий шаблон для выполнения команды:

   ```
   avp.com <command> [options]
   ```

   В результате Kaspersky Endpoint Security выполнит команду.

SANDBOX. Управление Sandbox

Команды управления компонентом Sandbox:

- Включение и выключение компонента Sandbox.

  Компонент Sandbox обеспечивает взаимодействие с решением Kaspersky Sandbox и компонентом KATA Sandbox, который входит в состав Kaspersky Anti Targeted Attack Platform.

- Настройка параметров работы компонента Sandbox:

  - Подключение компьютера к серверам Sandbox.

    На серверах развернуты виртуальные образы операционных систем Microsoft Windows, в которых запускаются проверяемые объекты. Вы можете ввести IP-адрес (IPv4 или IPv6) или полное доменное имя. Подробнее о развертывании виртуальных образов и конфигурации серверов Sandbox см. в справке Kaspersky Sandbox и справке Kaspersky Anti Targeted Attack Platform.

  - Настройка времени ожидания соединения с сервером.

    Время ожидания соединения с сервером Sandbox (для Kaspersky Sandbox) или Central Node (для KATA). По истечению заданного времени ожидания Kaspersky Endpoint Security отправит запрос на следующий сервер. Вы можете увеличить время ожидания соединения с сервером, если у вас низкая скорость соединения или соединение нестабильно. Рекомендованное значение времени ожидания запроса не более 0,5 сек.

  - Настройка доверенного соединения между компьютером и серверами.

    Для настройки доверенного соединения с сервером Sandbox (для Kaspersky Sandbox) или Central Node (для KATA) вам нужно подготовить TLS-сертификат. Далее вам нужно добавить сертификат на компьютер с помощью политики. Также вам нужно добавить сертификат на сервер Sandbox (для Kaspersky Sandbox) или Central Node (для KATA).

  - Настройка режима интеграции.

    Вам нужно выбрать решение, в составе которого работает Sandbox: Kaspersky Sandbox или KATA Sandbox. *Kaspersky Sandbox* – это отдельное решение Detection and Response от "Лаборатории Касперского". *KATA Sandbox* – это компонент решения Kaspersky Anti Targeted Attack Platform. При интеграции с KATA Sandbox компонент может работать в следующих режимах:

    - **Вручную**. Пользователь вручную отправляет файл на проверку из контекстного меню (**Отправить в Sandbox**).
    - **Автоматически**. Приложение автоматически обнаруживает объекты и отправляет их на проверку в Sandbox.
    - **Комбинированный**.

- Отображение текущих параметров работы компонента.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

Операция	
`stop`	Выключить компонент Sandbox.
`start`	Включить компонент Sandbox.

`set`	Настроить параметры работы компонента Sandbox. Вы можете настроить следующие параметры:
	• добавление серверов Sandbox (`--servers`);
	• добавление TLS-сертификата (`--pinned-certificate`);
	• добавление криптоконтейнера (`--client-certificate`);
	• указание пароля к криптоконтейнеру (`--client-certificate-password`);
	• установка времени ожидания соединения с сервером (`--timeout`);
	• выбор режима интеграции (`--mode`):
	  • `KSB` – интеграция с Kaspersky Sandbox;
	  • `KATAManual` – интеграция с KATA Sandbox в ручном режиме работы;
	  • `KATAAuto` – интеграция с KATA Sandbox в автоматическом режиме;
	  • `KATAFull` – интеграция с KATA Sandbox в комбинированном режиме.

`show`	Показать текущие параметры работы компонента. В результате вы получите следующий ответ:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Авторизация	
`/login=<user name> /password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

Пример

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB /login=login /password=password
```

PREVENTION. Управление Запретом запуска объектов

Выключение компонента Запрет запуска объектов или отображение текущих параметров работы компонента, включая список правил запрета запуска объектов.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com prevention disable
```

```
avp.com prevention /show
```

В результате выполнения команды `prevention /show` вы получите следующий ответ:

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

Коды возврата команды:

- `-1` – команда не поддерживается версией приложения, которое установлено на компьютере.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.
- `9` – неверная операция (например, попытка выключить компонент, если компонент уже выключен).

ISOLATION. Управление Сетевой изоляцией

Выключение Сетевой изоляции компьютера или отображение текущих параметров работы компонента. Параметры работы компонента также включают в себя список сетевых соединений, которые добавлены в исключения.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

В результате выполнения команды `stat` вы получите следующий ответ: `Network isolation on|off`.

RESTORE. Восстановление файлов из карантина

Восстановление файла из карантина в папку его исходного размещения. *Карантин* – это специальное локальное хранилище на компьютере. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства. Kaspersky Endpoint Security использует карантин только при работе с решениями Detection and Response от "Лаборатории Касперского". В остальных случаях Kaspersky Endpoint Security помещает файл в резервное хранилище. Подробнее о работе с карантином в составе решений см. в справке Kaspersky Sandbox, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Endpoint Detection and Response Expert, Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Detection and Response Expert (on-premises).

Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение **Восстановление из резервного хранилища**.

Объект помещается на карантин под системной учетной записью (SYSTEM).

Восстановление файлов из карантина имеет следующие особенности:

- Если папка назначения удалена или у пользователя нет прав доступа к этой папке, приложение помещает файл в папку `%DataRoot%\QB\Restored`. Далее вам нужно вручную переместить файл в папку назначения.
- Приложение учитывает регистр имени восстанавливаемого файла. Если вы введите имя файла в неверном регистре, приложение не восстановит файл.
- Если в папке восстановления уже есть файл с таким же именем, приложение отменит восстановление файла.
- Если вы используете решение KATA (EDR), после восстановления файла приложение сохраняет копию файла на карантине. Вы можете очистить карантин вручную. Для решений EDR Optimum и EDR Expert приложение удаляет файл из карантина после восстановления.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Дополнительные параметры	
`/REPLACE`	Переписать существующий файл.
`<file name>`	Имя восстанавливаемого файла.

Авторизация	
`/login=<user name> /password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

Пример

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

Коды возврата команды:

- `-1` – команда не поддерживается версией приложения, которое установлено на компьютере.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.

IOCSCAN. Поиск индикаторов компрометации (IOC)

Запуск задачи *Поиск IOC. Индикатор компрометации (Indicator of Compromise, IOC)* – набор данных об объекте или активности, который указывает на несанкционированный доступ к компьютеру (компрометация данных). Например, индикатором компрометации может быть большое количество неудачных попыток входа в систему. Задача *Поиск IOC* позволяет обнаруживать индикаторы компрометации на компьютере и выполнять действия по реагированию на угрозы.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Поиск IOC прерывается при обнаружении 128 совпадений с индикаторами компрометации, описанными в IOC-файлах. Это необходимо для ограничения количества записей в отчете задачи Поиск IOC для удобства его анализа и защиты отчета от переполнения из-за неточно сформулированных индикаторов компрометации, для которых совпадений может быть очень много.

Синтаксис команды

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off] [/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off] [/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

IOC-файлы	
`<full path to the IOC file>`	Полный путь к IOC-файлу, по которому требуется выполнить поиск. Вы можете указать несколько IOC-файлов через пробел. Полный путь к IOC-файлу следует ввести без аргумента `/path`. Например, `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	Путь к папке с IOC-файлами, по которым требуется выполнять поиск. *IOC-файлы* – файлы, содержащие набор индикаторов, при совпадении с которыми приложение считает событие обнаружением. IOC-файлы должны соответствовать стандарту описания OpenIOC. Например, `C:\Users\Admin\Desktop\IOC`

Тип данных для поиска IOC	
`/process=on|off`	Анализ данных о процессах при поиске IOC (термин ProcessItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет запущенные на компьютере процессы при выполнении проверки. Если в IOC-файле указаны IOC-термины IOC-документа ProcessItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security проверяет данные о процессах, только если IOC-документ ProcessItem описан в переданном на проверку IOC-файле.
`/hint=<full path to the executable file of the process|full path to the file>`	Анализ данных о файле при поиске IOC (термины ProcessItem и FileItem). Вы можете выбрать файл следующими способами: • `<full path to the executable file of the process>` – термин ProcessItem; • `<full path to the file>` – термин FileItem.

`/registry=on|off`	Анализ данных о реестре Windows при поиске IOC (термин RegistryItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет реестр Windows. Если в IOC-файле указаны термины IOC-документа RegistryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security проверяет реестр Windows, только если IOC-документ RegistryItem описан в переданном на проверку IOC-файле. Для типа данных RegistryItem Kaspersky Endpoint Security анализирует определенный набор разделов реестра.
`/dnsentry=on|off`	Анализ данных о записях в локальном кеше DNS при поиске IOC (термин DnsEntryItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет локальный кеш DNS. Если в IOC-файле указаны термины IOC-документа DnsEntryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security проверяет локальный кеш DNS, только если IOC-документ DnsEntryItem описан в переданном на проверку IOC-файле.
`/arpentry=on|off`	Анализ данных о записях в ARP-таблице при поиске IOC (термин ArpEntryItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет таблицу ARP. Если в IOC-файле указаны термины IOC-документа ArpEntryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security проверяет ARP-таблицу, только если IOC-документ ArpEntryItem описан в переданном на проверку IOC-файле.
`/ports=on|off`	Анализ данных о портах, открытых на прослушивание, при поиске IOC (термин PortItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет таблицу активных соединений на устройстве. Если в IOC-файле указаны термины IOC-документа PortItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security проверяет таблицу активных соединений, только если IOC-документ PortItem описан в переданном на проверку IOC-файле.
`/services=on|off`	Анализ данных о службах, установленных на устройстве, при поиске IOC (термин ServiceItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет данные о службах, установленных на устройстве. Если в IOC-файле указаны термины IOC-документа ServiceItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security проверяет данные о службах, только если IOC-документ ServiceItem описан в переданном на проверку IOC-файле.
`/system=on|off`	Анализ данных об окружении при поиске IOC (термин SystemInfoItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не анализирует данные об окружении. Если в IOC-файле указаны термины IOC-документа SystemInfoItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security анализирует данные об окружении, только если IOC-документ SystemInfoItem описан в переданном на проверку IOC-файле.
`/users=on|off`	Анализ данных о пользователях при поиске IOC (термин UserItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не анализирует данные о пользователях, созданных в системе. Если в IOC-файле указаны термины IOC-документа UserItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security анализирует данные о пользователях, созданных в системе, только если IOC-документ UserItem описан в переданном на проверку IOC-файле.
`/volumes=on|off`	Анализ данных о томах при поиске IOC (термин VolumeItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет данные о томах на устройстве. Если в IOC-файле указаны термины IOC-документа VolumeItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security анализирует данные о томах, только если IOC-документ VolumeItem описан в переданном на проверку IOC-файле.

`/eventlog=on|off`	Анализ данных о записях в журнале событий Windows при поиске IOC (термин EventLogItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет записи в журнале событий Windows. Если в IOC-файле указаны термины IOC-документа EventLogItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security проверяет записи в журнале событий Windows, только если IOC-документ EventLogItem описан в переданном на проверку IOC-файле. При указании значения IOC-термина EventLogItem\source вам необходимо использовать значение параметра **Provider Name** из XML-схемы события.
`/datetime=<event publication date>`	Учет даты публикации события в журнале событий Windows при определении области поиска IOC для соответствующего IOC-документа. При поиске IOC Kaspersky Endpoint Security проверяет записи в журнале событий Windows, опубликованные в период с указанного времени и даты и до момента выполнения задачи. В качестве значения параметра Kaspersky Endpoint Security позволяет задать дату публикации события. Проверка будет выполняться только для событий, опубликованных в журнале событий Windows после указанной даты и до момента выполнения проверки. Если параметр не указан, Kaspersky Endpoint Security проверяет события с любой датой публикации. Параметр `TaskSettings::BaseSettings::EventLogItem::datetime` недоступен для редактирования. Параметр используется, только если IOC-документ EventLogItem описан в переданном на проверку IOC-файле.
`/channel=<list of channels>`	Список имен каналов (журналов), для которых требуется выполнить поиск IOC. Если параметр указан, Kaspersky Endpoint Security проверяет записи, опубликованные в указанных журналах. При этом в IOC-документе должен быть описан термин EventLogItem. Имя журнала задается в формате строки, в соответствии с именем журнала (канала), указанного в свойствах этого журнала (параметр Full Name) или в свойствах события (параметр `<Channel></Channel>` в xml-схеме события). Вы можете указать несколько каналов через пробел. Если параметр не указан, Kaspersky Endpoint Security проверяет записи для каналов `Application`, `System`, `Security`.
`/files=on|off`	Анализ данных о файлах при поиске IOC (термин FileItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не анализирует данные о файлах. Если в IOC-файле указаны термины IOC-документа FileItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security анализирует данные о файлах, только если IOC-документ FileItem описан в переданном на проверку IOC-файле.
`/drives=<all|system|critical|custom>`	Область поиска IOC при анализе данных для IOC-документа FileItem. Доступны следующие значения области поиска: • `<all>` – все доступные файловые области. • `<system>` – файлы, расположенные в папках, в которых установлена ОС. • `<critical>` – временные файлы в пользовательских и системных папках. • `<custom>` – файлы в указанных пользователем областях (`/scope=<list of folders to scan>`). Если параметр не установлен, проверка выполняется в критических областях.
`/excludes=<list of exclusions>`	Область исключений при анализе данных для IOC-документа FileItem. Вы можете указать несколько путей через пробел.
`/scope=<list of folders to scan>`	Пользовательская область поиска IOC при анализе данных для IOC-документа FileItem (`/drives=custom`). Вы можете указать несколько путей через пробел.
`/retro /<number of days>`	*Ретроспективный поиск IOC* – это режим работы задачи *Поиск IOC*, при котором Kaspersky Endpoint Security выполняет поиск индикаторов компрометации по данным, полученным за определенный интервал времени. Режим предназначен для поиска индикаторов компрометации по телеметрии защищаемого компьютера, такой как сетевая активность, процессы, файлы и другие. Вы можете указать интервал времени в диапазоне 1 - 14 дней. По умолчанию приложение выполняет поиск индикаторов компрометации за один день.
`/network=on|off`	Анализ сетевых данных (термин NetworkItem).
`/url=on|off`	Анализ данных в журналах браузеров (термин UrlHistoryItem). Ретроспективный поиск IOC анализирует журналы следующих браузеров: Google Chrome, Mozilla Firefox, Microsoft Edge (версии 79 и выше).

`/email`	Анализ почтовых объектов (термин EmailItem).
`/route`	Анализ таблиц маршрутизации (термин RouteEntryItem).

Коды возврата команды:

- `-1` – команда не поддерживается версией приложения, которое установлено на компьютере.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Endpoint Security выводит в командную строку следующие данные о результатах выполнения задачи:

`Uuid`	Идентификатор IOC-файла из заголовка структуры IOC-файла (тег `<ioc id="">`)
`Name`	Описание IOC-файла из заголовка структуры IOC-файла (тег `<description></description>`)
`Matched Indicator Items`	Перечень идентификаторов всех сработавших индикаторов.
`Matched objects`	Данные по каждому документу IOC, по которому было найдено совпадение.

MDRLICENSE. Активация MDR

Добавление конфигурационного файла BLOB для активации Managed Detection and Response. BLOB-файл содержит идентификатор клиента и информацию о лицензии Kaspersky Managed Detection and Response. BLOB-файл находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробную информацию о BLOB-файле см. в справке Kaspersky Managed Detection and Response.

Для выполнения операций с BLOB-файлом требуются права администратора. Также параметры Managed Detection and Response в политике должны быть доступны для изменения ( ).

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Операция	
`/ADD <file name>`	Применить конфигурационный файл BLOB для интеграции с Kaspersky Managed Detection and Response (формат файла P7). Вы можете применить только один BLOB-файл. Если BLOB-файл уже добавлен на компьютер, файл будет заменен.
`/DEL`	Удалить конфигурационный файл BLOB.

Авторизация	
`/login=<user name> /password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

Пример

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

Пример

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. Интеграция с EDR (KATA)

Команды управления компонентом Endpoint Detection and Response (KATA):

- Включение или выключение компонента EDR (KATA).

  Компонент EDR (KATA) обеспечивает взаимодействие с решением Kaspersky Anti Targeted Attack Platform.

- Настройка параметров подключения к серверам Kaspersky Anti Targeted Attack Platform.

- Отображение текущих параметров работы компонента.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

Операция	
`stop`	Выключить компонент EDR (KATA).
`start`	Включить компонент EDR (KATA).

`set`	Настроить параметры работы компонента EDR (KATA). Вы можете настроить следующие параметры: • добавление серверов Central Node (`servers=<server address>:<port>`); • добавление TLS-сертификата (`server-certificate=<path to the TLS certificate>`); • установка времени ожидания соединения с сервером Central Node (`/timeout=<Central Node server connection timeout (s)>`); • установка периода синхронизации с сервером Central Node (`/sync-period=<Central Node server synchronization period (min)>`).
`show`	Показать текущие параметры работы компонента.

EDRExpertOnPrem. Интеграция с EDR Expert (on-premises)

Команды управления встроенным агентом для интеграции с решением Kaspersky Endpoint Detection and Response Expert (on-premises):

- Включение или выключение встроенного агента EDR Expert (on-premises).
- Настройка параметров подключения к серверам EDR Expert (on-premises).
- Отображение текущих параметров работы встроенного агента.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com START EDRExpertOnPrem
```

```
avp.com STOP EDRExpertOnPrem
```

```
avp.com EDRExpertOnPrem /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate>
[/client-certificate=<path to the PFX archive> /client-certificate-password=<password to the PFX archive>]
[/timeout=<server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
/telemetry-servers=<server address:port> /telemetry-server-certificate=<path to the TLS certificat> [telemetry-
client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>]
[/telemetry-timeout=<server connection timeout (s)>] [/events-send-period=<seconds>] [/events-limit=<0|1>]
[/events-per-hour=<number of events>] [/max-packet-length=<number of packets>] [/telemetry-only-tagged-events=
<0|1>] login=<user name> password=<password>
```

```
avp.com EDRExpertOnPrem /show
```

Операция	Описание
`stop`	Выключить встроенный агент EDR Expert (on-premises).
`start`	Включить встроенный агент EDR Expert (on-premises).

`set`	Настроить параметры работы встроенного агента EDR Expert (on-premises).
	Вы можете настроить следующие параметры подключения к *серверам реагирования*:
	• `servers=<server address>:<port>`. Адрес сервера реагирования (FQDN, IPv4, IPv6).
	• `server-certificate=<path to the TLS certificate>`. TLS-сертификат для установки доверенного соединения с сервером. Вы можете получить TLS-сертификат в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `client-certificate=<path to the PFX archive> client-certificate-password=<password to the PFX archive>`. Использование криптоконтейнара для двусторонней аутентификации. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом в формате PKCS#12. Для включения такой проверки вам нужно сформировать криптоконтейнер во внешнем центре сертификации.
	• `timeout=<server connection timeout (s)>`. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу.
	• `sync-period=<server synchronization period (min)>`. Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Endpoint Security получает задачи по реагированию на угрозы и отправляет результаты выполнения задач.
	Вы можете настроить следующие параметры подключения к *серверам сбора телеметрии*:
	• `telemetry-servers=<server address:port>`. Адрес сервера сбора телеметрии (FQDN, IPv4, IPv6).
	• `telemetry-server-certificate=<path to the TLS certificat>`. TLS-сертификат для установки доверенного соединения с сервером. Вы можете получить TLS-сертификат в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `telemetry-client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>`. Использование криптоконтейнара для двусторонней аутентификации. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом в формате PKCS#12. Для включения такой проверки вам нужно сформировать криптоконтейнер во внешнем центре сертификации.
	• `telemetry-timeout=<server connection timeout (s)>`. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу.
	• `events-send-period=<seconds>`. Максимальная задержка отправки событий. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд.
	• `events-limit=<0|1>`. Регулирование количества запросов. Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события.
	• `events-per-hour=<number of events>`. Максимальное количество событий в час. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.
	• `max-packet-length=<number of packets>`. Максимальная длина пакета. Приложение выполняет синхронизацию с сервером при заполнении буфера событиями. По умолчанию установлено значение 1024 события.
	• `telemetry-only-tagged-events=<0|1>`. Отправка телеметрии только с IOA. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию *потоковой проверки*, которая позволяет отслеживать такие события в режиме реального времени.
	Вы можете настроить следующие общие параметры:
	• `mode=EDRKATA | EDRExpertOnPrem`. Переключение между решениями:
	  • `EDRKATA`. Endpoint Detection and Response Expert (версия 7.1 и ниже).
	  • `EDRExpertOnPrem`. Endpoint Detection and Response Expert (версия 8.0 и выше). Значение по умолчанию.
	• `login=<user name> password=<password>`. Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

`show`	Показать текущие параметры работы компонента.

KUMA. Интеграция с KUMA

Команды управления встроенным агентом KUMA:

- Включение или выключение интеграции с KUMA.

  Встроенный агент KUMA обеспечивает взаимодействие с решением Kaspersky Unified Monitoring and Analysis Platform.

- Настройка параметров подключения к серверам Kaspersky Unified Monitoring and Analysis Platform.

- Отображение текущих параметров работы компонента.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

Операция	
`stop`	Выключить интеграцию с KUMA.
`start`	Включить интеграцию с KUMA.
`set`	Настроить параметры работы встроенного агента KUMA. Вы можете настроить следующие параметры: • Добавление серверов KUMA (`/servers=<protocol>://<server address>:<port>`). Приложение поддерживает следующие протоколы для подключения к серверу: `tcp`, `udp`, `http`, `https`. • добавление TLS-сертификата (`/server-certificate=<path to the TLS certificate>`). • установка времени ожидания соединения с сервером (`/timeout=<KUMA server connection timeout (s)>`). • добавление криптоконтейнера (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`). • настройка задержки отправки событий (`/maximum-data-transfer-time=<maximum events transmission delay (sec)`).
`show`	Показать текущие параметры работы компонента.

Авторизация	
`/login=<user name> /password=<password>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

Пример

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15 /login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer /login=login /password=password
```

YARA. Запуск YARA-проверки

Запуск задачи *Запустить YARA-проверку*. Приложение выполняет проверку файлов и объектов на наличие признаков целевых атак на IT-инфраструктуру организации с помощью баз YARA-правил. *YARA-правила* представляют собой описание сигнатур целевых атак и вторжений в IT-инфраструктуру организации, по которым Kaspersky Endpoint Security производит проверку объектов.

Для запуска YARA-проверки вам нужно подготовить YARA-файлы, которые описывают правила. При создании YARA-файлов учитывайте следующие требования:

- Kaspersky Endpoint Security поддерживает YARA-файлы с расширением .YARA и .YAR открытого стандарта описания индикаторов компрометации YARA версии 4.2.3.
- В задаче можно указывать только файлы с YARA-правилами. Задача *Запустить YARA-проверку* не поддерживает другие типы правил.
- Если вы добавили YARA-файлы, которые Kaspersky Endpoint Security не поддерживает, или правила содержат синтаксические ошибки, запуск задачи будет прерван с соответствующим уведомлением об ошибке.
- Идентификаторы всех YARA-файлов, которые используются в одной задаче, должны быть уникальными. Наличие YARA-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.
- YARA-проверка прерывается при обнаружении 128 совпадений с маркерами, описанными в YARA-правилах. Это необходимо для ограничения количества записей в отчете YARA-проверки для удобства его анализа и защиты отчета от переполнения из-за неточно сформулированных YARA-правил, для которых совпадений может быть очень много.

Специалисты "Лаборатории Касперского" рекомендуют создавать по одному правилу в одном YARA-файле. Такой подход облегчает чтение результатов проверки.

YARA-проверка может занять продолжительное время. В зависимости от размера диска, параметров задачи, количества объектов на диске YARA-проверка может длиться от нескольких минут до нескольких часов. При этом приложение не показывает индикатор выполнения. Прервать или отменить YARA-проверку невозможно. Рекомендуем дождаться результатов YARA-проверки.

Синтаксис команды

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

YARA-файлы	
`<full path to the YARA file>`	Полный путь к YARA-файлу, по которому требуется выполнить поиск. Вы можете указать пути к нескольким YARA-файлам через пробел. Обязательный параметр, если параметр `/path=<path to the folder with YARA files>` не задан. Пример: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`

`/path=<path to the folder with YARA files>`	Полный путь к папке с YARA-файлами, по которым требуется выполнить поиск. Обязательный параметр, если параметр `<full path to the YARA file>` не задан. Пример: `/path=C:\Users\Admin\Desktop\YARA`

Дополнительные параметры	
`/fastScan=<on|off>`	Быстрая YARA-проверка. Для каждого объекта приложение фиксирует в журнале одно вхождение обнаруженного маркера. При этом приложение скрывает дубликаты обнаруженных маркеров в журнале. Быстрая YARA-проверка позволяет сократить время проверки больших файлов. Если параметр не задан, приложение выполняет стандартную YARA-проверку. В этом режиме приложение записывает дубликаты обнаруженных маркеров в журнал.
`/maxRules=<maximum number of scan rules>`	Ограничение количества уникальных сработавших правил, при превышении которого приложение прекращает YARA-проверку. Если значение параметра не задано или равно `0`, приложение выполняет YARA-проверку без ограничений.
`/timeOut=<stop scan after the specified time in seconds>`	Ограничение длительности YARA-проверки в секундах. По истечении указанного времени приложение останавливает YARA-проверку. Если значение параметра не задано или равно `0`, приложение выполняет YARA-проверку без ограничений.
`/recursive=<on|off>`	Параметр запускает рекурсивную проверку вложенных папок в рамках выборочной проверки (`/scanFolders`).
`/scanFolders=<list of folders to be scanned>`	Параметр запускает YARA-проверку файлов по указанному списку папок. Вы можете указать несколько значений через пробел. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски пути к папке. Если значение параметра не задано, приложение выполняет YARA-проверку на всех локальных дисках, кроме сетевых, облачных и подключаемых дисков.
`/scanMemory=<on|off>`	Проверка памяти всех запущенных процессов.
`/scanProcess=<process name>`	Проверка памяти только для указанных процессов. Необходимо через пробел указать пути к исполняемым файлам процессов вместе с названиями файлов. Вы можете также использовать символы `*` и `?` для ввода маски.
`/maxSize=<file size in bytes>`	Ограничение размера файлов для YARA-проверки. Приложение пропускает файлы большего размера.
`/includes=<list of objects to be scanned>>`	Формирование области проверки. Вы можете указать несколько значений через пробел. Доступны следующие значения: • имя файла; • маска имени файла. Область проверки необходимо задавать с параметром `/scanFolders`. Пример: `/scanFolders C:\*.* /includes=*.exe *.dll` – приложение проверит все файлы с расширением .EXE и .DLL на диске C.
`/excludes=<list of objects to be scanned>`	Исключение файлов из YARA-проверки. Вы можете указать несколько значений через пробел. Доступны следующие значения: • путь к файлу; • маска пути к файлу. Исключения необходимо задавать с параметром `/scanFolders`. Пример: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – приложение пропускает файл readme.txt, все файлы из папки C:\trusted, а также все файлы с расширением .XML в корневой папке на диске C.
`/scanAutoruns=<on|off>`	YARA-проверка объектов точек автозапуска.
`/excludeAutoruns=<list of autorun point areas to skip>`	Исключение объектов точек автозапуска из области проверки. Необходимо через пробел указать пути к исполняемым файлам процессов вместе с названиями файлов. Вы можете также использовать символы `*` и `?` для ввода маски.

`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Если указан путь к папке, приложение сохраняет результаты сканирования по указанному пути в файле yara_<имя компьютера>_<время завершения сканирования>.txt. Если указан путь к конкретному TXT-файлу, приложение сохраняет результаты сканирования в нем. Например: `/logFolder=C:\test` или `/logFolder=C:\test\abc.txt`. Результаты проверки будут выведены в командной строке независимо от того, указано ли значение параметра `/logFolder`.

Коды возврата команды:

- `-1` – команда не поддерживается версией приложения, которое установлено на компьютере.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.
- `5` – не найден один или несколько файлов с YARA-правилами из указанных в значении параметра.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Endpoint Security выводит в командную строку следующие данные о результатах выполнения задачи:

`Started at <time>` `Finished at <time>`	Время начала и завершения сканирования.
`Host name: <computer name>`	Имя компьютера, на котором обнаружен объект.
`Result: <error>`	Код ошибки, которая возникла при выполнении задачи. Если ошибки нет, приложение выводит `0x00000000`.
`Comment: <comment text>`	Описание ошибки, которая возникла при выполнении задачи. Например, `Operation timeout`.
`Object Name:` или `Process:` (при проверке памяти процессов)	Имя объекта/процесса, на котором сработало YARA-правило.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Хеши объекта, на котором сработало YARA-правило.
`Rule Name`	Имя сработавшего YARA-правила.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Метаданные, которые указаны в YARA-правиле.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Найденные совпадения внутри объекта, которые соответствуют условиям YARA-правила:
	• Смещение в памяти процесса / в файле, где обнаружено совпадение (`Offset`).
	• Имя строки в YARA-правиле, с которой произошло совпадение (`String name`).
	• Совпавшая строка в памяти процесса / в файле (`String data`).

TELEMETRYFILTERS. Фильтрация событий для отправки в KUMA

По умолчанию отправка событий на Сервер KUMA выключена. Для работы KUMA вам нужно включить отправку телеметрии. Для выбора источника событий доступны стандартные журналы: *Application*, *Security* или *System*. Для повышения производительности и оптимизации отправки данных на Сервер KUMA вы можете вручную добавить или исключить отдельные события из телеметрии. Например, вы можете отменить отправку событий Sysmon.

Из командной строки вы можете экспортировать список исключений в файл в формате JSON.

Если в команде указано только имя файла, в который нужно экспортировать параметры, приложение размещает файл следующим образом:

- Если путь к avp.com добавлен в системную переменную %PATH%, приложение помещает файл в папку `C:\Windows\SysWOW64`.
- Если вы выполняете команду из папки установки приложения, экспорт завершится с ошибкой, так как самозащита приложения заблокирует создание нового файла в папке приложения. Для экспорта параметров приложения в файл введите путь к файлу.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Операция	
`export`	Экспорт фильтров событий для отправки в KUMA.
`import`	Импорт фильтров событий для отправки в KUMA. Если на компьютере уже есть правила фильтрации событий, Kaspersky Endpoint Security заменит их при импорте.

Файл для экспорта / импорта	
`<file name>`	Имя файла с фильтрами событий для отправки в KUMA. Также вы можете ввести путь к файлу. Вы можете экспортировать фильтры для отправки в KUMA в файл в формате JSON.

Команды управления Легким агентом

Вы можете управлять приложением в режиме Легкого агента для защиты виртуальных сред из командной строки. Вы можете управлять приложением в режиме Легкого агента, если управление через консоль Kaspersky Security Center невозможно. Вы можете просмотреть список команд для управления приложением с помощью команды `HELP`. Чтобы получить справку по синтаксису конкретной команды, введите `HELP <command>`.

Чтобы управлять приложением в режиме Легкого агента из командной строки, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Используйте следующий шаблон для выполнения команды:

   ```
   avp.com <command> [options]
   ```

   В результате Kaspersky Endpoint Security выполнит команду.

Приложение, установленное в режиме Легкого агента, поддерживает почти все команды AVP для приложения, установленного в стандартном режиме. Из-за особенностей работы приложения в режиме Легкого агента существуют ограничения при выполнении команд обновления антивирусных баз и управления лицензионными ключами.

KSVLAINFO. Определение режима работы Легкого агента

Определение режима работы Легкого агента.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com KSVLAINFO
```

В результате выполнения команды в консоль выводится следующая информация:

- Режим Легкого агента для защиты виртуальных сред: включен или выключен.

  Если режим Легкого агента включен, приложение используется в составе решения Kaspersky Security для виртуальных сред Легкий агент.

- Режим защиты инфраструктуры VDI: включен или выключен.

  Режим защиты инфраструктуры VDI позволяет оптимизировать работу приложения Kaspersky Endpoint Security на временных виртуальных машинах. Если режим защиты инфраструктуры VDI включен, то обновления, требующие перезагрузки защищенной виртуальной машины, не устанавливаются на временных виртуальных машинах. При получении обновлений, требующих перезагрузки, Легкий агент, установленный на временной виртуальной машине, отправляет в Kaspersky Security Center сообщение о необходимости обновления шаблона защищенных виртуальных машин.

- Тип защищенной виртуальной машины: временная или постоянная.

- Роль защищенной виртуальной машины в виртуальной инфраструктуре: сервер или рабочая станция.

- Идентификатор – UUID.

VIISINFO. Статус подключения Легкого агента к Серверу интеграции

Просмотр информации о подключении Легкого агента к Серверу интеграции.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com VIISINFO
```

В результате выполнения команды в консоль выводится следующая информация:

- Адрес и порт Сервера интеграции, к которому подключается Легкий агент.

- Статус подключения к Серверу интеграции.

- Дата и время последнего соединения Легкого агента с Сервером интеграции.

SVMINFO. Статус подключения Легкого агента к Серверу защиты

Просмотр информации о подключении Легкого агента к Серверу защиты.

Для выполнения команды перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security. Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% и выполнять команду без перехода в папку приложения.

Синтаксис команды

```
avp.com SVMINFO
```

В результате выполнения команды в консоль выводится следующая информация:

- Адрес SVM, к которой подключен Легкий агент, и расположение SVM в виртуальной инфраструктуре относительно Легкого агента: локальная или не локальная.
- Способ обнаружения SVM Легким агентом: с помощью Сервера интеграции или с использованием списка адресов SVM, заданных вручную.
- Список адресов SVM, если в качестве способа обнаружения SVM выбрано использование списка адресов SVM.
- Тег для подключения Легкого агента к SVM.
- Алгоритм выбора SVM: стандартный или расширенный. Если применяется расширенный алгоритм выбора SVM, также выводится тип расположения SVM в виртуальной инфраструктуре.
- Наличие защиты соединения между Легким агентом и Сервером защиты.

Коды ошибок

При работе с приложением через командную строку возможно появление ошибок. При появлении ошибки Kaspersky Endpoint Security показывает сообщение об ошибке, например, `Error: Cannot start task 'EntAppControl'`. Также Kaspersky Endpoint Security может показать дополнительные сведения в виде кода, например, `error=8947906D` (см. таблицу ниже).

Коды ошибок

Код ошибки	Описание
09479001	Этот ключ уже используется
0947901D	Истек срок действия лицензии. Обновление баз недоступно
89479002	Ключ не найден
89479003	Цифровая подпись повреждена или не найдена
89479004	Данные повреждены
89479005	Файл ключа поврежден
89479006	Истек срок действия лицензии
89479007	Файл ключа не указан
89479008	Неверный файл ключа
89479009	Не удалось сохранить данные
8947900A	Не удалось прочитать данные
8947900B	Ошибка ввода / вывода
8947900C	Базы не найдены
8947900E	Библиотека лицензирования не загружена
8947900F	Базы повреждены или обновлены вручную
89479010	Базы повреждены
89479011	Невозможно применить недействительный файл ключа для добавления резервного ключа
89479012	Системная ошибка
89479013	Список запрещенных ключей поврежден

Код ошибки	Описание
89479014	Подпись файла не соответствует цифровой подписи "Лаборатории Касперского"
89479015	Невозможно использовать ключ для пробной лицензии в качестве ключа для коммерческой лицензии
89479016	Чтобы использовать бета-версию приложения, требуется лицензия для бета-тестирования
89479017	Файл ключа не подходит для данного приложения. Невозможно активировать Kaspersky Endpoint Security для Windows с помощью файла ключа для другого приложения. Пожалуйста, проверьте установленное приложение
89479018	Лицензионный ключ заблокирован "Лабораторией Касперского"
89479019	Приложение уже использовалось по пробной лицензии. Невозможно снова добавить ключ для пробной лицензии
8947901A	Файл ключа поврежден
8947901B	Цифровая подпись не найдена, повреждена или не соответствует подписи "Лаборатории Касперского"
8947901C	Невозможно добавить ключ, если срок действия соответствующей ему некоммерческой лицензии истек
8947901E	Дата создания файла ключа или его применения некорректна. Проверьте системную дату
8947901F	Невозможно добавить ключ для пробной лицензии, пока действует другая аналогичная лицензия
89479020	Список запрещенных ключей поврежден или не найден
89479021	Описание обновлений повреждено или не найдено
89479022	Ключ не подходит для этого приложения
89479023	Невозможно применить недействительный файл ключа для добавления резервного ключа
89479025	Возникла ошибка при отправке запроса на сервер активации. Возможные причины: ошибка соединения с интернетом или временные проблемы на сервере активации. Попробуйте активировать приложение с помощью кода активации позже (через 1-2 часа). В случае повторения ошибки обратитесь к вашему интернет-провайдеру
89479026	В запросе указан неверный код активации
89479027	Невозможно получить статус ответа
89479028	Ошибка при сохранении временного файла
89479029	Введен неверный код активации или на компьютере установлена некорректная системная дата. Проверьте системную дату на компьютере
8947902A	Ключ не подходит для данного приложения или истек срок действия лицензии
8947902B	Не удалось получить файл ключа. Введен неверный код активации
8947902C	Сервер активации возвратил ошибку 400
8947902D	Сервер активации возвратил ошибку 401
8947902E	Сервер активации возвратил ошибку 403
8947902F	Недоступен необходимый ресурс на сервере активации. Сервер активации возвратил ошибку 404. Пожалуйста, проверьте настройки подключения к интернету
89479030	Сервер активации возвратил ошибку 405
89479031	Сервер активации возвратил ошибку 406
89479032	Требуется аутентификация на прокси-сервере. Пожалуйста, проверьте настройки сети
89479033	Истек тайм-аут ожидания запроса
89479034	Сервер активации возвратил ошибку 409
89479035	Недоступен необходимый ресурс на сервере активации. Сервер активации возвратил ошибку 410. Пожалуйста, проверьте настройки подключения к интернету
89479036	Сервер активации возвратил ошибку 411
89479037	Сервер активации возвратил ошибку 412
89479038	Сервер активации возвратил ошибку 413
89479039	Сервер активации возвратил ошибку 414

Код ошибки	Описание
8947903A	Сервер активации возвратил ошибку 415
8947903C	Внутренняя ошибка сервера
8947903D	Функциональность не поддерживается
8947903E	Некорректный ответ от шлюза. Пожалуйста, проверьте настройки сети
8947903F	Ресурс временно недоступен
89479040	Истек тайм-аут ожидания ответа от шлюза. Пожалуйста, проверьте настройки сети
89479041	Протокол не поддерживается сервером
89479043	Неизвестная ошибка HTTP
89479044	Некорректный идентификатор ресурса
89479046	Некорректный адрес (URL)
89479047	Некорректная целевая папка
89479048	Ошибка выделения памяти
89479049	Ошибка конвертации параметров в ANSI-строку (url, folder, agent)
8947904A	Ошибка создания рабочего потока
8947904B	Рабочий поток уже запущен
8947904C	Рабочий поток не запущен
8947904D	Файл ключа не найден на сервере активации
8947904E	Ключ заблокирован
8947904F	Внутренняя ошибка сервера активации
89479050	Недостаточно данных в запросе на активацию
89479053	Срок действия лицензии, соответствующей добавляемому ключу, уже истек
89479054	На компьютере установлена некорректная системная дата. Пожалуйста, проверьте системную дату на компьютере
89479055	Срок действия пробной лицензии истек
89479056	Период активации приложения истек
89479057	Превышено допустимое количество активаций приложения с помощью указанного кода
89479058	Процедура активации завершилась с системной ошибкой
89479059	Невозможно использовать ключ для пробной лицензии в качестве ключа для коммерческой лицензии
8947905C	Требуется код активации
89479062	Невозможно подключиться к серверу активации
89479064	Сервер активации недоступен. Пожалуйста, проверьте настройки подключения к интернету и попробуйте активировать приложение снова
89479065	Срок действия лицензии истек
89479066	Невозможно заменить активный ключ на ключ с истекшим сроком годности
89479067	Невозможно добавить резервный ключ, если срок действия соответствующей лицензии истекает раньше по сравнению с действующей лицензией
89479068	Отсутствует обновленный ключ по подписке
8947906A	Неподходящий код активации
8947906B	Ключ уже активен
8947906C	Типы лицензий, которые соответствуют активному и резервному ключам, не совпадают
8947906D	Лицензия не допускает работу компонента

Код ошибки	Описание
8947906E	Невозможно добавить ключ по подписке в качестве резервного
89479213	Общая ошибка транспортного уровня
89479214	Не удалось связаться с сервером активации
89479215	Неверный формат веб-адреса
89479216	Не удалось преобразовать адрес прокси-сервера
89479217	Не удалось преобразовать адрес сервера. Пожалуйста, проверьте настройки подключения к интернету
89479218	Попытка соединения с сервером завершилась с ошибкой
89479219	Удаленный отказ в доступе
8947921A	Тайм-аут операции истек
8947921B	Ошибка отправки HTTP-запроса
8947921C	Ошибка SSL-соединения
8947921D	Операция прервана в результате обратного вызова
8947921E	Слишком много перенаправлений
8947921F	Проверка адресата завершилась с ошибкой
89479220	Пустой ответ от сервера
89479221	Ошибка отправки данных
89479222	Ошибка приема данных
89479223	Проблема, связанная с SSL-сертификатом
89479224	Проблема, связанная с шифрованием SSL
89479225	Проблема, связанная с центром SSL-сертификации
89479226	Некорректное содержимое сетевого пакета
89479227	Учетной записи отказано в доступе
89479228	Некорректный файл SSL-сертификата
89479229	Не удалось завершить SSL-соединение
8947922A	Повторная ошибка
8947922B	Некорректный файл с отозванными сертификатами
8947922C	Ошибка запроса SSL-сертификата
89479401	Неизвестная ошибка сервера
89479402	Внутренняя ошибка сервера
89479403	Ключ для введенного кода активации отсутствует
89479404	Активный ключ заблокирован
89479405	Отсутствуют обязательные параметры запроса для активации
89479406	Неверный номер или пароль клиента
89479407	Неверный код активации
89479408	Код активации не подходит для данного приложения. Невозможно активировать Kaspersky Endpoint Security для Windows с помощью кода активации для другого приложения. Пожалуйста, проверьте установленное приложение
89479409	Требуется код активации
8947940B	Истек период активации
8947940C	Превышено число активаций приложения с помощью этого кода активации
8947940D	Неверный формат идентификатора запроса

Код ошибки	Описание
8947940E	Код активации уже используется
8947940F	Невозможно обновить код активации
89479410	Код активации не подходит для этого региона
89479411	Данный код активации не предназначен для используемой языковой версии приложения
89479412	Код активации предназначен для новой версии данного приложения. Для активации установленной версии приложения необходимо получить другой код активации
89479413	Сервер активации вернул ошибку 643
89479414	Сервер активации вернул ошибку 644
89479415	Сервер активации вернул ошибку 645
89479416	Сервер активации вернул ошибку 646
89479417	Требуется сервер активации версии 1.0
89479418	Неверный формат кода активации
89479419	Время на компьютере не синхронизировано со временем на сервере активации
8947941A	Неверная версия приложения
8947941B	Срок действия подписки истек
8947941C	Превышено допустимое количество активаций
8947941D	Неверная подпись тикета
8947941E	Требуются дополнительные данные пользователя
8947941F	Проверка данных пользователя завершилась с ошибкой
89479420	Подписка неактивна
89479421	В данный момент производятся технические работы с сервером активации
89479501	Непредвиденная ошибка
89479502	Передан недопустимый параметр. Например, пустой список адресов серверов активации
89479503	Код активации недействителен (неправильная контрольная сумма)
89479504	Неверный идентификатор пользователя
89479505	Неверный пароль пользователя
89479506	Сервер активации вернул неверный ответ
89479507	Исполнение запроса на активацию было прервано
89479509	Сервер активации вернул пустой список переадресации

Приложение. Профили приложения

Профиль – компонент, задача или функция Kaspersky Endpoint Security. Профили предназначены для управления приложением из командной строки. Вы можете использовать профили для выполнения команд `START`, `STOP`, `STATUS`, `STATISTICS` и `EXPORT`. С помощью профилей вы можете настроить параметры приложения (например, `STOP DeviceControl`) или запустить задачу (например, `START Scan_My_Computer`).

Доступны следующие профили:

- `AdaptiveAnomaliesControl` – Адаптивный контроль аномалий.
- `AMSI` – AMSI-защита.
- `AntiCryptor` – Защита от шифрования.
- `BehaviorDetection` – Анализ поведения.
- `DeviceControl` – Контроль устройств.
- `EntAppControl` – Контроль приложений.
- `File_Monitoring` или `FM` – Защита от файловых угроз.
- `Firewall` или `FW` – Сетевой экран.
- `HIPS` – Предотвращение вторжений.
- `IDS` – Защита от сетевых угроз.
- `IntegrityCheck` – Проверка целостности.
- `LogInspector` – Анализ журналов.
- `Mail_Monitoring` или `EM` – Защита от почтовых угроз.
- `Rollback` – Откат обновления (профиль невозможно применить, если приложение установлено в режиме Легкого агента).
- `Scan_ContextScan` – Проверка из контекстного меню.
- `Scan_IdleScan` – Фоновая проверка.
- `Scan_Memory` – Проверка памяти ядра.
- `Scan_My_Computer` – Полная проверка.
- `Scan_Objects` – Выборочная проверка.
- `Scan_Qscan` – Проверка объектов, загрузка которых осуществляется при запуске операционной системы.
- `Scan_Removable_Drive` – Проверка съемных дисков.
- `Scan_Startup` или `STARTUP` – Проверка важных областей.
- `Updater` – Обновление (профиль невозможно применить, если приложение установлено в режиме Легкого агента).

- `Web_Monitoring` или `WM` – Защита от веб-угроз.
- `WebControl` – Веб-Контроль.

Также Kaspersky Endpoint Security поддерживает работу служебных профилей. Служебные профили могут понадобиться при обращении в Службу технической поддержки "Лаборатории Касперского".

Управление приложением через REST API

Kaspersky Endpoint Security позволяет настраивать параметры приложения, запускать проверку и обновление антивирусных баз, а также выполнять другие задачи с помощью сторонних решений. Для этого Kaspersky Endpoint Security предоставляет API. Kaspersky Endpoint Security REST API работает по протоколу HTTP и представляет собой набор методов "запрос / ответ". То есть вы можете управлять Kaspersky Endpoint Security через стороннее решение, а не локальный интерфейс приложения или Консоль администрирования Kaspersky Security Center.

Для начала работы с REST API нужно установить Kaspersky Endpoint Security с поддержкой REST API. REST-клиент и Kaspersky Endpoint Security должны быть установлены на одном компьютере.

Для безопасной работы Kaspersky Endpoint Security с REST-клиентом выполните следующие требования:

- Настройте защиту REST-клиента от несанкционированного доступа в соответствии с рекомендациями производителя REST-клиента. Также настройте защиту папки с REST-клиентом от записи с помощью списка управления избирательным доступом (англ. Discretionary Access Control List, DACL).
- Для запуска REST-клиента используйте отдельную учетную запись с правами администратора. Запретите интерактивный вход в систему для этой учетной записи.

Управление приложением через REST API осуществляется по адресу http://127.0.0.1 или http://localhost. Удаленно управлять Kaspersky Endpoint Security через REST API невозможно.

ОТКРЫТЬ ДОКУМЕНТАЦИЮ REST API

Установка приложения с REST API

Для управления приложением через REST API нужно установить Kaspersky Endpoint Security с поддержкой REST API. Если вы управляете Kaspersky Endpoint Security через REST API, управлять приложением с помощью Kaspersky Security Center невозможно.

Подготовка к установке приложения с поддержкой REST API

Для безопасной работы Kaspersky Endpoint Security с REST-клиентом вам нужно настроить идентификацию запросов. Для этого вам нужно установить сертификат и в дальнейшем подписывать полезные данные каждого запроса.

Для создания сертификата вы можете использовать, например, OpenSSL.

Пример:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Используйте алгоритм шифрования RSA и размер ключа 2048 бит и более.

В результате вы получите сертификат `cert.pem` и закрытый ключ `key.pem`.

Установка приложения с поддержкой REST API

Чтобы установить Kaspersky Endpoint Security с поддержкой REST API, выполните следующие действия:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security версии 11.2.0 или выше.
3. Установите Kaspersky Endpoint Security со следующими параметрами:

   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     Имя пользователя для управления приложением через REST API. Введите имя пользователя в формате `<DOMAIN>\<UserName>` (например, `RESTAPI_User=COMPANY\Administrator`). Вы можете управлять приложением через REST API только под этой учетной записью. Для работы с REST API вы можете выбрать только одного пользователя.
   - `RESTAPI_Port=<port>`

     Порт для управления приложением через REST API. По умолчанию используется порт 6782. Убедитесь, что порт свободен. Необязательный параметр.
   - `RESTAPI_Certificate=<path to certificate>`

     Сертификат для идентификации запросов (например, `RESTAPI_Certificate=C:\cert.pem`).

     Вы можете установить сертификат после установки приложения или обновить сертификат после истечения срока действия.

     Как установить сертификат для идентификации запросов REST API

     1. Выключите самозащиту Kaspersky Endpoint Security.

        Механизм самозащиты предотвращает изменение и удаление файлов приложения на жестком диске, процессов в памяти, записей в системном реестре.
     2. Перейдите в раздел с параметрами REST API в реестре:
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. Введите путь к сертификату, например, `Certificate = C:\Folder\cert.pem`.
     4. Включите самозащиту Kaspersky Endpoint Security.
     5. Перезапустите приложение.
   - `AdminKitConnector=1`

     Управление приложением с помощью систем администрирования. По умолчанию управление разрешено.

Также вы можете задать параметры работы с REST API с помощью файла setup.ini.

Пример:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
/pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
```

В результате вы сможете управлять приложением через REST API. Для проверки работы откройте документацию REST API с помощью GET-запроса.

Пример:
```
GET http://localhost:6782/kes/v1/api-docs
```

Если вы установили приложение с поддержкой REST API, Kaspersky Endpoint Security автоматически создает в параметрах Веб-Контроля разрешающее правило доступа к веб-ресурсам *Служебное правило для REST API*. Это правило нужно для обеспечения постоянного доступа REST-клиента к Kaspersky Endpoint Security. Например, если вы ограничили доступ пользователя к веб-ресурсам, это не повлияет на управление приложением через REST API. Мы рекомендуем не удалять правило и не изменять параметры правила *Служебное правило для REST API*. Если вы удалили правило, Kaspersky Endpoint Security восстановит правило после перезапуска приложения.

Работа с API

Ограничить доступ к приложению через REST API с помощью Защиты паролем невозможно. Например, запретить выключать защиту через REST API невозможно. Вы можете настроить Защиту паролем через REST API и ограничить доступ пользователей к приложению через локальный интерфейс.

Для управления приложением через REST API нужно запустить REST-клиент под учетной записью, которую вы задали при установке приложения с поддержкой REST API. Для работы с REST API вы можете выбрать только одного пользователя.

ОТКРЫТЬ ДОКУМЕНТАЦИЮ REST API

Управление приложением через REST API состоит из следующих этапов:

1. Получите текущие значения параметров приложения. Для этого отправьте GET-запрос.

   Пример:
   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. Приложение отправит ответ со структурой и значениями параметров. Kaspersky Endpoint Security поддерживает XML- и JSON-форматы.

   Пример:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. Измените параметры приложения. Используйте структуру параметров, полученную в ответ от GET-запроса.

   Пример:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. Сохраните параметры приложения (полезные данные) в JSON (payload.json).

5. Подпишите JSON в формате PKCS7.

   Пример:
   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out signed_payload.pem
   ```

   В результате вы получите подписанный файл с полезными данными запроса (`signed_payload.pem`).

6. Измените параметры приложения. Для этого отправьте POST-запрос с прикрепленным подписанным файлом с полезными данными запроса (`signed_payload.pem`).

Приложение применит изменения в параметрах и отправит ответ с результатами настройки приложения (ответ может быть пустым). Вы можете убедиться в том, что параметры изменены, с помощью GET-запроса.

Источники информации о приложении

Этот раздел содержит описание источников информации о приложении.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

Страница Kaspersky Endpoint Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Security вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница Kaspersky Endpoint Security содержит ссылку на интернет-магазин. В нем вы можете приобрести приложение или продлить право пользования приложением.

Страница Kaspersky Endpoint Security в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Endpoint Security в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Endpoint Security, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение приложений "Лаборатории Касперского" на Форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме.

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Обращение в Службу технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Endpoint Security, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Endpoint Security.

Kaspersky предоставляет поддержку Kaspersky Endpoint Security в течение жизненного цикла (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас создать *файл трассировки*. Файл трассировки позволяет отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка.

Кроме того, специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на компьютере, подробные отчеты работы компонентов приложения.

Во время работ по диагностике специалисты Службы технической поддержки могут попросить вас изменить параметры приложения:

- Активировать функциональность получения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов приложения, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения полученной диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся необходимая для выполнения перечисленных действий информация (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав полученных в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы приложения способами, не описанными в справке или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

О составе и хранении файлов трассировки

Вы сами несете ответственность за обеспечение безопасности полученной информации и, в частности, за контроль и ограничение доступа к полученной информации, хранимой на компьютере, до ее передачи в "Лабораторию Касперского".

Файлы трассировки хранятся на вашем компьютере в течение всего времени использования приложения и безвозвратно удаляются при удалении приложения.

Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке `%ProgramData%\Kaspersky Lab\KES.14.3\Traces`.

Файлы трассировки называются следующим образом: `KES<14.3_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

Вы можете просмотреть данные, записанные в файлы трассировки.

Все файлы трассировки содержат следующие общие данные:

- Время события.
- Номер потока выполнения.

  Эту информацию не содержит файл трассировки Агента аутентификации.

- Компонент приложения, в результате работы которого произошло событие.
- Степень важности события (информационное, предупреждение, критическое, ошибка).
- Описание события выполнения команды компонента приложения и результата выполнения этой команды.

Содержание файлов трассировки SRV.log, GUI.log и ALL.log

В файлы трассировки `SRV.log`, `GUI.log` и `ALL.log`, помимо общих данных, может записываться следующая информация:

- Персональные данные, в том числе фамилия, имя и отчество, если эти данные являются частью пути к файлам на локальном компьютере.
- Данные об установленном на компьютере аппаратном обеспечении (например, данные о прошивке BIOS / UEFI). Эти данные записываются в файлы трассировки при выполнении полнодискового шифрования по технологии Шифрование диска Kaspersky.
- Имя пользователя и пароль, если они передавались в открытом виде. Эти данные могут записываться в файлы трассировки при проверке интернет-трафика.
- Имя пользователя и пароль, если они содержатся в заголовках протокола HTTP.
- Имя учетной записи для входа в Microsoft Windows, если имя учетной записи является частью имени файла.
- Адрес вашей электронной почты или веб-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта.
- Веб-сайты, которые вы посещаете, а также ссылки с этих веб-сайтов. Эти данные записываются в файлы трассировки, когда приложение проверяет веб-сайты.
- Адрес прокси-сервера, имя компьютера, порт, IP-адрес, имя пользователя, используемое при авторизации на прокси-сервере. Эти данные записываются в файлы трассировки, если приложение использует прокси-сервер.
- Внешние IP-адреса, с которыми было установлено соединение с вашего компьютера.
- Тема сообщения, идентификатор, имя отправителя и адрес веб-страницы отправителя сообщения в социальной сети. Эти данные записываются в файлы трассировки, если включен компонент Веб-Контроль.
- Данные о сетевом трафике. Эти данные записываются в файлы трассировки, если включены компоненты мониторинга трафика (например, Веб-Контроль).
- Данные, полученные с серверов "Лаборатории Касперского" (например, версия антивирусных баз).
- Статусы компонентов Kaspersky Endpoint Security и сведения об их работе.
- Данные о действиях пользователя в приложении.
- События операционной системы.

Содержание файлов трассировки HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Файл трассировки `HST.log`, помимо общих данных, содержит информацию о выполнении задачи обновления баз и модулей приложения.

Файл трассировки `BL.log`, помимо общих данных, содержит информацию о событиях, возникающих во время работы приложения, а также данные, необходимые для устранения неполадок в работе приложения. Этот файл создается, если приложение запускается с параметром avp.exe –bl.

Файл трассировки `Dumpwriter.log`, помимо общих данных, содержит служебную информацию, необходимую для устранения неполадок, возникающих при записи файла дампа приложения.

Файл трассировки `WD.log`, помимо общих данных, содержит информацию о событиях, возникающих в процессе работы службы avpsus, в том числе события обновления модулей приложения.

Файл трассировки `AVPCon.dll.log`, помимо общих данных, содержит информацию о событиях, возникающих при работе модуля связи с Kaspersky Security Center.

Содержание файлов трассировки производительности

Файлы трассировки производительности называются следующим образом: `KES<14.3_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Файлы трассировки производительности, помимо общих данных, содержат информацию о нагрузке на процессор, о времени загрузки операционной системы и приложений, о запущенных процессах.

Содержание файла трассировки компонента AMSI-защита

Файл трассировки `AMSI.log`, помимо общих данных, содержит информацию о результатах проверок, запрошенных сторонними приложениями.

Содержание файла трассировки компонента Защита от почтовых угроз

Файл трассировки `mcou.OUTLOOK.EXE.log`, помимо общих данных, может содержать части сообщений электронной почты, в том числе адреса электронной почты.

Содержание файла трассировки компонента Проверка из контекстного меню

Файл трассировки `shellex.dll.log`, помимо общих данных, содержит информацию о выполнении задачи проверки и данные, необходимые для устранения неполадок в работе приложения.

Содержание файлов трассировки веб-плагина приложения

Файлы трассировки веб-плагина приложения хранятся на компьютере, на котором развернута Kaspersky Security Center Web Console, в папке `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs`.

Файлы трассировки веб-плагина приложения называются следующим образом: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`. Web Console начинает записывать данные после установки и удаляет файлы трассировки после удаления Web Console.

Файлы трассировки веб-плагина приложения, помимо общих данных, содержат следующую информацию:

- Пароль пользователя KLAdmin для разблокировки интерфейса Kaspersky Endpoint Security (Защита паролем).
- Временный пароль для разблокировки интерфейса Kaspersky Endpoint Security (Защита паролем).
- Имя пользователя и пароль для почтового SMTP-сервера (Уведомления по электронной почте).
- Имя пользователя и пароль для прокси-сервера сети интернет (Прокси-сервер).
- Имя пользователя и пароль для задачи *Изменение состава компонентов приложения*.
- Учетные данные и пути, указанные в свойствах политики и в задачах Kaspersky Endpoint Security.

Содержание файла трассировки Агента аутентификации

Файл трассировки Агента аутентификации хранится в папке System Volume Information и называется следующим образом: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Файл трассировки Агента аутентификации, помимо общих данных, содержит информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации.

Трассировка работы приложения

Трассировка приложения – это подробная запись действий, выполняемых приложением, и сообщений о событиях, происходящих во время работы приложения. В процессе трассировки приложение создает комплект файлов с данными о работе разных компонентов приложения (например, SRV.log, WD.log и другие).

Выполняйте трассировку приложения под руководством Службы технической поддержки "Лаборатории Касперского".

Чтобы создать файл трассировки приложения, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.
3. Используйте переключатель **Включить трассировку приложения**, чтобы включить или выключить трассировку работы приложения.

4. В раскрывающемся списке **Трассировка** выберите режим трассировки работы приложения:

   - **С ограничением места**. Сохранить результаты трассировки в ограниченное число комплектов файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера. Если выбран этот режим, вы можете указать максимальное количество комплектов файлов для ротации и максимальный размер каждого комплекта файлов.

     По умолчанию приложение сохраняет пять комплектов файлов с трассировками. Размер каждого комплекта файлов составляет 3072 МБ. Таким образом, вам необходимо 15 ГБ свободного пространства на диске для сохранения файлов трассировки.

   - **Без ограничений**. Сохранить один файл трассировки (без ограничений по размеру).

5. В раскрывающемся списке **Уровень** выберите уровень трассировки:

   - **Обычный** – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждениях, а также информация о работе приложения в нормальном режиме (значение по умолчанию).

   - **Детальный** – в файле трассировки сохраняется вся информация о работе приложения.

   Дополнительные уровни трассировки доступны при настройке трассировки приложения из командной строки. Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки. Если указания Службы технической поддержки отсутствуют, рекомендуется устанавливать уровень трассировки **Обычный**.

   > Если трассировка приложения была включена из командной строки с уровнем, отличным от **Обычный** или **Детальный**, то в раскрывающемся списке **Уровень** будет отображаться значение **Обычный**.

6. Чтобы остановить процесс трассировки, вернитесь в окно **Мониторинг проблем** и выключите трассировку.

> Вы также можете создать файлы трассировки во время установки приложения из командной строки, в том числе с помощью файла setup.ini.

В результате в папке `%ProgramData%\Kaspersky Lab\KES.14.3\Traces` будут созданы файлы трассировки работы приложения. После создания файлов трассировки отправьте файлы в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Endpoint Security автоматически удаляет файлы трассировки при удалении приложения. Вы также можете вручную удалить файлы. Для этого трассировка должна быть выключена и приложение остановлено.

Трассировка производительности приложения

Kaspersky Endpoint Security позволяет получить информацию о проблемах в работе компьютера при использовании приложения. Например, вы можете получить информацию о задержках при загрузке операционной системы после установки приложения. Для этого Kaspersky Endpoint Security создает файлы трассировки производительности. *Трассировка производительности* – это запись действий, выполняемых приложением, для диагностики проблем производительности Kaspersky Endpoint Security. Для получения информации Kaspersky Endpoint Security использует сервис трассировки событий Windows (англ. Event Tracing for Windows, ETW). Диагностику работы Kaspersky Endpoint Security и установление причин возникновения проблем выполняет Служба технической поддержки "Лаборатории Касперского".

Выполняйте трассировку приложения под руководством Службы технической поддержки "Лаборатории Касперского".

Чтобы создать файл трассировки производительности, выполните следующие действия:

1. В главном окне приложения нажмите на кнопку .
2. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.
3. Используйте переключатель **Включить трассировку производительности**, чтобы включить или выключить трассировку производительности приложения.
4. В раскрывающемся списке **Трассировка** выберите режим трассировки работы приложения:
   - **С ограничением места**. Сохранить результаты трассировки в ограниченное число файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера. Если выбран этот режим, вы можете указать максимальный размер каждого файла.
   - **Без ограничений**. Сохранить один файл трассировки (без ограничений по размеру).
5. В раскрывающемся списке **Уровень** выберите уровень трассировки:
   - **Поверхностный**. Kaspersky Endpoint Security анализирует основные процессы операционной системы, связанные с производительностью.
   - **Детальный**. Kaspersky Endpoint Security анализирует все процессы операционной системы, связанные с производительностью.
6. В раскрывающемся списке **Тип трассировки** выберите тип трассировки:
   - **Базовая информация**. Kaspersky Endpoint Security анализирует процессы во время работы операционной системы. Используйте этот тип трассировки, если проблема воспроизводится после загрузки операционной системы, например, проблема доступа в интернет в браузере.
   - **При перезагрузке**. Kaspersky Endpoint Security анализирует процессы только на этапе загрузки операционной системы. После загрузки операционной системы Kaspersky Endpoint Security останавливает трассировку. Используйте этот тип трассировки, если проблема связана с задержкой загрузки операционной системы.

7. Перезагрузите компьютер и воспроизведите проблему.

8. Чтобы остановить процесс трассировки, вернитесь в окно Мониторинга проблем и выключите трассировку.

В результате в папке `%ProgramData%\Kaspersky Lab\KES.14.3\Traces` будет создан файл трассировки производительности. После создания файла трассировки отправьте файл в Службу технической поддержки "Лаборатории Касперского".

Запись дампов

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Security на момент создания этого файла дампа.

> Сохраненные дампы могут содержать конфиденциальные данные. Для контроля доступа к данным вам нужно самостоятельно обеспечить защиту файлов дампов.

Файлы дампов хранятся на вашем компьютере в течение всего времени использования приложения и безвозвратно удаляются при удалении приложения. Файлы дампов хранятся в папке `%ProgramData%\Kaspersky Lab\KES.14.3\Traces`.

Как включить запись дампов в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Общие настройки** → **Настройки приложения**.

4. В блоке **Отладочная информация** нажмите на кнопку **Настройка**.

5. В открывшемся окне используйте флажок **Включить запись дампов**, чтобы включить или выключить запись дампов приложения.

6. Сохраните внесенные изменения.

Как включить запись дампов в Web Console и Cloud Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки** → **Служба технической поддержки**.

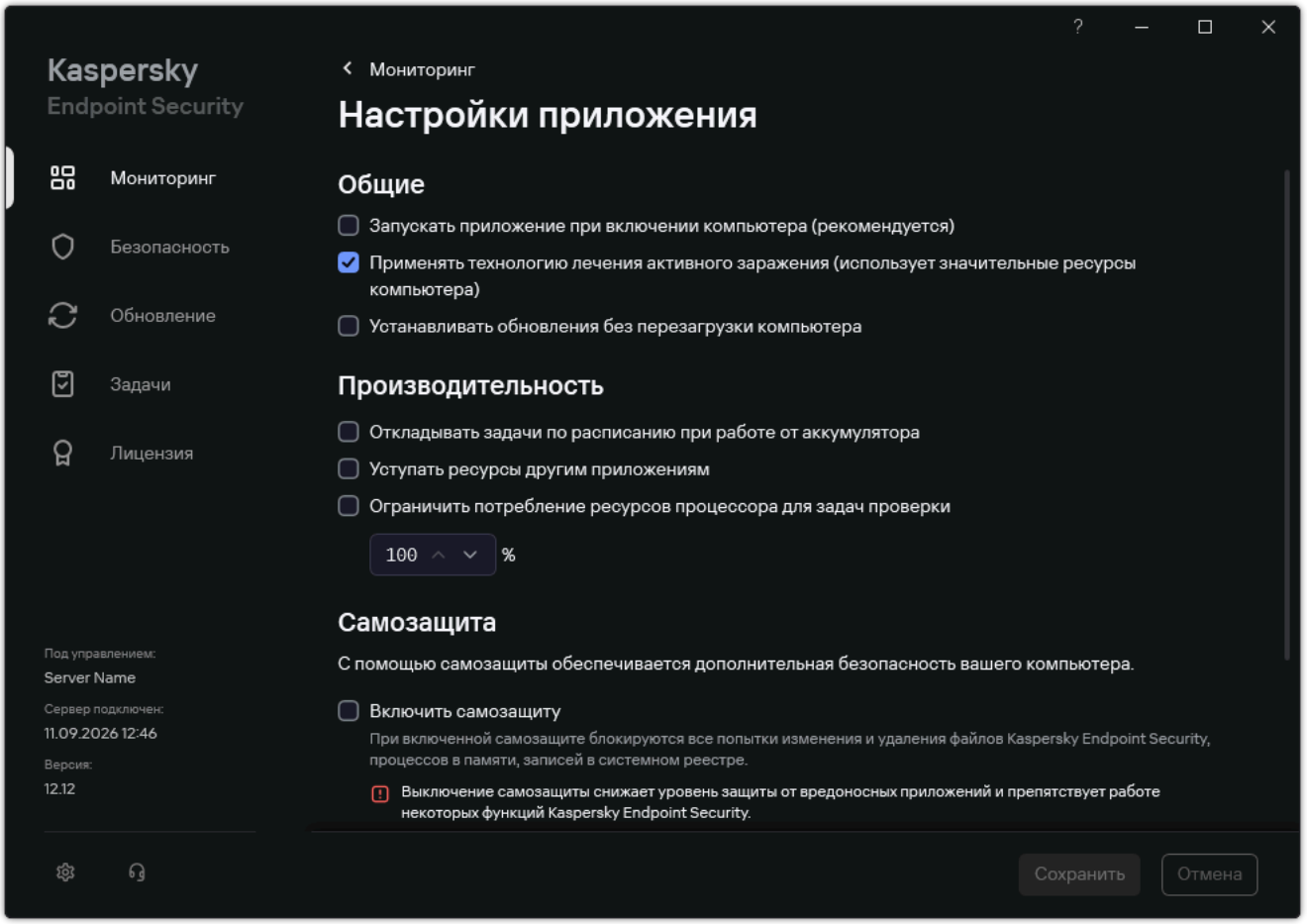
5. В блоке **Отладочная информация** используйте флажок **Запись дампов ВКЛЮЧЕНА**, чтобы включить или выключить запись дампов приложения.

6. Сохраните внесенные изменения.

Как включить запись дампов в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.



Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Отладочная информация** используйте флажок **Включить запись дампов**, чтобы включить или выключить запись дампов приложения.

4. Сохраните внесенные изменения.

Защита файлов дампов и трассировок

Файлы дампов и файлы трассировки содержат информацию об операционной системе, а также могут содержать данные пользователя. Чтобы предотвратить несанкционированный доступ к этим данным, вы можете включить защиту файлов дампов и файлов трассировки.

Если защита файлов дампов и файлов трассировки включена, доступ к файлам имеют следующие пользователи:

- К файлам дампов имеют доступ системный и локальный администраторы, а также пользователь, включивший запись файлов дампов и файлов трассировки.

- К файлам трассировки имеют доступ только системный и локальный администраторы.

Как включить защиту файлов дампов и файлов трассировки в Консоли администрирования (MMC)

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Общие настройки → Настройки приложения**.
4. В блоке **Отладочная информация** нажмите на кнопку **Настройка**.
5. В открывшемся окне используйте флажок **Включить защиту файлов дампов и файлов трассировки**, чтобы включить или выключить защиту файлов.
6. Сохраните внесенные изменения.

Как включить защиту файлов дампов и файлов трассировки в Web Console и Cloud Console

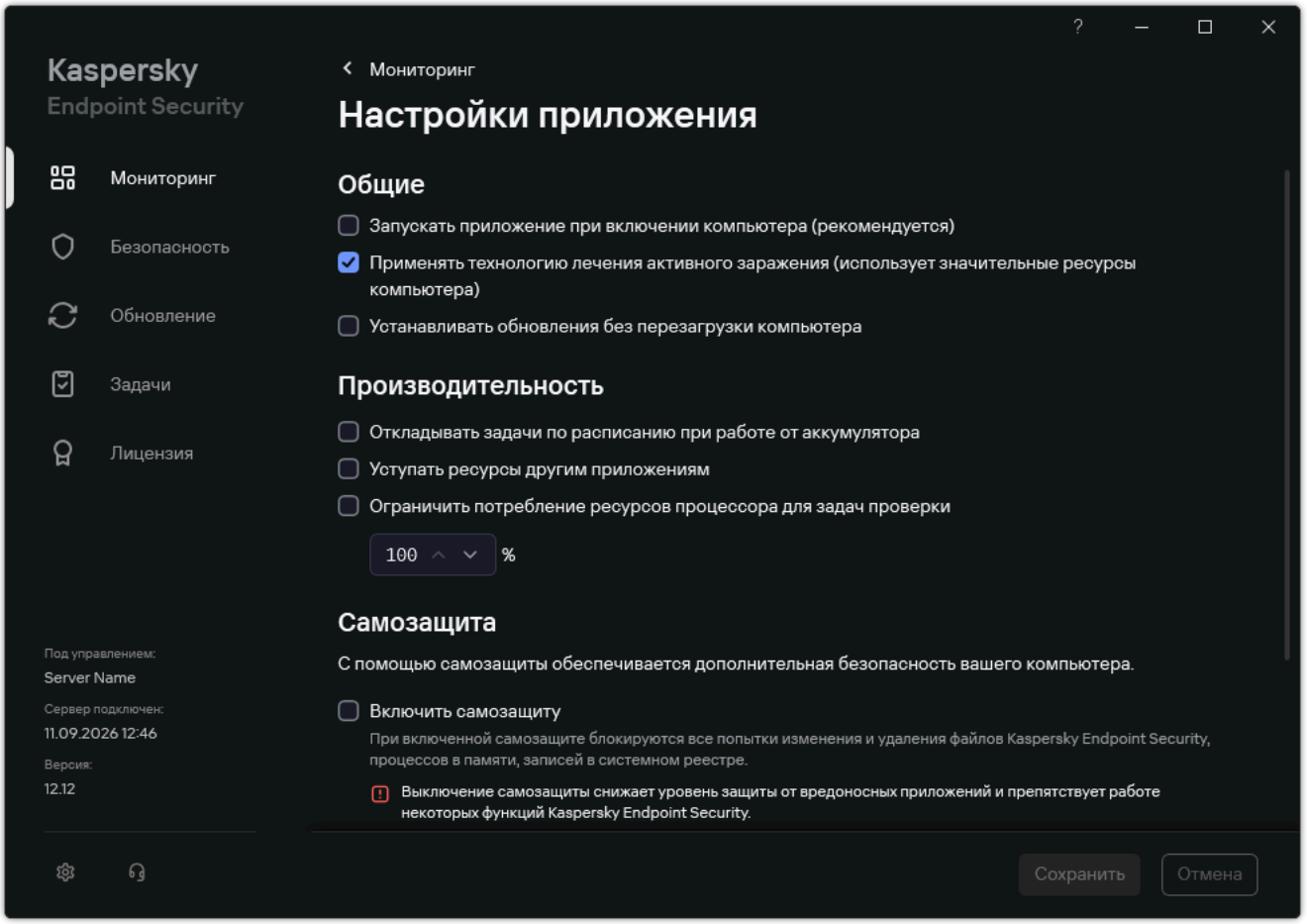
1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки → Служба технической поддержки**.
5. В блоке **Отладочная информация** используйте флажок **Защита файлов дампов и файлов трассировки ВКЛЮЧЕНА**, чтобы включить или выключить защиту файлов.
6. Сохраните внесенные изменения.

Как включить защиту файлов дампов и файлов трассировки в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.

2. В окне параметров приложения в блоке **Общие настройки** и нажмите на плитку **Настройки приложения**.



Параметры приложения Kaspersky Endpoint Security для Windows

3. В блоке **Отладочная информация** используйте флажок **Включить защиту файлов дампов и файлов трассировки**, чтобы включить или выключить защиту файлов.

4. Сохраните внесенные изменения.

Файлы дампов и файлы трассировки, записанные при включенной защите, остаются защищенными после отключения этой функции.

Получение данных об ОС (Kaspersky Get System Info)

После установки приложения Kaspersky Endpoint Security могут возникнуть ситуации, при которых операционная система или приложение работают некорректно. Происходит конфликт приложения с программным обеспечением или с драйверами комплектующих компьютера.

Чтобы выяснить причину проблемы, технической поддержке "Лаборатории Касперского" требуется отчет утилиты Kaspersky Get System Info (далее GSI). Подробную информацию о работе с утилитой см. в Базе знаний "Лаборатории Касперского".

Ограничения и предупреждения

Kaspersky Endpoint Security имеет ряд некритичных для работы приложения ограничений.

Установка приложения

- Особенности поддержки операционной системы Microsoft Windows 10, Microsoft Windows Server 2016 и Microsoft Windows Server 2019 вы можете узнать в базе знаний Службы технической поддержки.
- Особенности поддержки операционной системы Microsoft Windows 11 и Microsoft Windows Server 2022 вы можете узнать в базе знаний Службы технической поддержки.
- После установки на зараженный компьютер приложение не предупреждает пользователя о необходимости запустить проверку компьютера. Могут возникнуть проблемы с активацией приложения. Для решения этих проблем запустите проверку важных областей.
- Если в файле setup.ini и setup.reg используются не ASCII-символы (например, русские буквы), мы рекомендуем редактировать файл с помощью notepad.exe и сохранять файл в кодировке UTF-16LE. Другие кодировки не поддерживаются.
- Использование не ASCII-символов при указании пути установки приложения в параметрах инсталляционного пакета не поддерживается.
- При импорте настроек приложения из CFG-файла не применяется значение параметра, который определяет участие в Kaspersky Security Network. После импорта параметров ознакомьтесь с текстом Положения о Kaspersky Security Network и подтвердите согласие на участие в Kaspersky Security Network. Ознакомиться с текстом Положения вы можете в интерфейсе приложения или в текстовом файле ksn_*.txt, который расположен в папке с дистрибутивом приложения.
- При удалении и повторной установке шифрования (FLE или FDE) или компонента Контроль устройств требуется выполнить перезагрузку системы перед повторной установкой.
- На операционной системе Microsoft Windows 10 после удаления компонента файлового шифрования (FLE) необходимо выполнить перезагрузку системы.
- При удалении отдельных компонентов приложения (например, с помощью задачи *Изменение состава компонентов приложения*) может потребоваться перезагрузка компьютера.
- В свойствах задачи *Изменение состава компонентов приложения* при переключении режима установки (**Раздельный режим** / **Совмещенный режим**) не поддерживается синхронизация набора компонентов между режимами. Приложение синхронизирует набор компонентов между режимами после повторного открытия свойств задачи.
- Установка приложения может завершиться с ошибкой *На вашем компьютере установлена программа, в которой имя программы отсутствует или нечитаемое*. Это означает, что на вашем компьютере остались несовместимые приложения или их фрагменты. Для удаления артефактов несовместимых приложений отправьте запрос с подробным описанием ситуации в техническую поддержку "Лаборатории Касперского" через Kaspersky CompanyAccount.
- Если вы отменили удаление Kaspersky Endpoint Security, запустите восстановление приложения после перезагрузки компьютера.

- Для работы приложения на компьютере должна быть установлена платформа Microsoft .NET Framework 4.0 или выше. Microsoft .NET Framework версии 4.6.1 имеет уязвимости. Если вы используете Microsoft .NET Framework 4.6.1, вам нужно установить обновления безопасности. Подробнее об обновлениях безопасности Microsoft .NET Framework см. на сайте технической поддержки Microsoft.

- Если установка приложения с выбранным компонентом Kaspersky Endpoint Agent на серверной операционной системе завершилась неудачно и появилось окно *Windows Installer Coordinator Error*, смотрите инструкцию на сайте поддержки Microsoft.

- Если приложение было установлено локально в тихом режиме, для смены установленных компонентов используйте подложенный файл setup.ini.

- После установки приложения Kaspersky Endpoint Security для Windows на некоторых конфигурациях Windows 7 продолжает работать Windows Defender. Мы рекомендуем отключить Windows Defender вручную, чтобы избежать медленной работы системы.

- При установке приложения Kaspersky Endpoint Security для Windows на сервер с установленными приложениями Kaspersky Security для Windows Server (KSWS) и Windows Defender необходимо выполнить перезагрузку системы. Перезагрузка системы нужна, даже если вы включили установку приложения без перезагрузки системы. Windows Defender для Windows Server включен в список несовместимого ПО для Kaspersky Endpoint Security для Windows. Перед установкой приложения инсталлятор удаляет Windows Defender для Windows Server. После удаления несовместимого ПО перезагрузка системы обязательна.

- Перед установкой приложения Kaspersky Endpoint Security для Windows (KES) на сервер с установленным приложением Kaspersky Security для Windows Server (KSWS) необходимо выключить Защиту паролем KSWS. После миграции с KSWS на KES включите Защиту паролем в параметрах приложения.

- На компьютерах под управлением Windows 7 или Windows Server 2008 R2 с развернутым программным обеспечением Veeam Backup & Replication для установки приложения может потребоваться перезагрузить компьютер и повторить попытку установки приложения.

- Миграция с Kaspersky Small Office Security (KSOS) на Kaspersky Endpoint Security (KES) с включенной Защитой паролем доступна начиная с версии сборки KSOS 21.16.*.*. Для миграции более ранних версий KSOS нужно выключить Защиту паролем или удалить KSOS вручную. Миграция KSOS на KES с выключенной Защитой паролем выполняется корректно.

- Установить Kaspersky Endpoint Security на загрузочный съемный диск невозможно. При установке Kaspersky Endpoint Security покажет сообщение об ошибке *Вы выбрали неверную папку или диск. Приложение должно быть установлено на локальный жесткий диск*. Если вам удалось установить приложение на съемный диск с помощью сторонних инструментов, это может привести к сбою при загрузке операционной системы (BSOD). Таким образом, Kaspersky Endpoint Security не поддерживает Windows To Go и аналогичные решения. Для проверки компьютера со съемного диска вы можете использовать бесплатное приложение Kaspersky Rescue Disk.

- Установка Kaspersky Endpoint Security с сетевыми компонентами на терминальный сервер с многопользовательскими сессиями по RDP-протоколу имеет особенности. Операционная система принудительно завершает все пользовательские сессии после завершения сессии Администратора. Для подключения к терминальному серверу нужно перезагрузить сервер или войти в систему локально. Такое поведение связано с особенностями работы операционной системы Windows.

- Если в Kaspersky Security Center 16.0 или Kaspersky Security Center 16.1 установлены веб-плагины Kaspersky Endpoint Security для Windows (сборка 12.11.0.2004) и Kaspersky Endpoint Security для Linux (сборка 12.4.0.1354), то обновление версии веб-плагина Kaspersky Endpoint Security для Windows до версии 12.11.0.6004 может привести к сбоям в работе политик Kaspersky Endpoint Security для Linux.

  Возможное решение: перейдите в окно **Параметры** → **Веб-плагины** и удалите из списка веб-плагины Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux и Unified Protection and Management Plug-in. Далее установите сначала веб-плагин Kaspersky Endpoint Security для Linux, затем – веб-плагин Kaspersky Endpoint Security для Windows.

- В свойствах инсталляционного пакета Kaspersky Endpoint Security для Windows 12.11 в Web Console некорректно отображается список компонентов. Отдельный компонент Защита от шифрования недоступен в этой версии приложения. Функция защиты папок общего доступа от внешнего шифрования входит в состав компонента Анализ поведения. Функция выделена в отдельный компонент в Kaspersky Endpoint Security для Windows 12.12. При этом в Консоли администрирования (MMC) список компонентов отображается корректно.

- При использовании веб-плагина версии 7.0 и выше в свойствах инсталляционного пакета Kaspersky Endpoint Security версии 14.1 и ниже некорректно отображается список компонентов, выбранных для установки по умолчанию. Если при создании инсталляционного пакета этот список не изменять, приложение будет установлено с набором компонентов, заданным по умолчанию для соответствующей версии приложения.

Обновление приложения

- Начиная с версии приложения 11.0.0 вы можете установить MMC-плагин Kaspersky Endpoint Security для Windows поверх предыдущей версии плагина. Чтобы вернуть плагин предыдущей версии, удалите плагин текущей версии и установите плагин предыдущей версии.

- При обновлении версии Kaspersky Endpoint Security 11.0.0 и 11.0.1 для Windows не сохраняются настройки расписания локальных задач *Обновление баз и модулей приложения*, *Проверка важных областей*, *Выборочная проверка* и *Проверка целостности приложения*.

- На компьютерах с Windows 10 версии 1903 и 1909 обновление с версий Kaspersky Endpoint Security 10 для Windows Service Pack 2 Maintenance Release 3 (сборка 10.3.3.275), Service Pack 2 Maintenance Release 4 (сборка 10.3.3.304), 11.0.0 и 11.0.1 с установленным компонентом файлового шифрования (FLE) может завершиться ошибкой. Это вызвано тем, что на Windows 10 версии 1903 и 1909 для этих версий Kaspersky Endpoint Security для Windows не поддерживается файловое шифрование. Перед установкой обновления мы рекомендуем удалить компонент файлового шифрования.

- Для работы приложения на компьютере должна быть установлена платформа Microsoft .NET Framework 4.0 или выше. Microsoft .NET Framework версии 4.6.1 имеет уязвимости. Если вы используете Microsoft .NET Framework 4.6.1, вам нужно установить обновления безопасности. Подробнее об обновлениях безопасности Microsoft .NET Framework см. на сайте технической поддержки Microsoft.

- При обновлении Kaspersky Endpoint Security приложение выключает использование KSN пока не будет принято Положение о Kaspersky Security Network. При этом в Kaspersky Security Center статус компьютера может быть изменен на *Критический*, получено событие *Серверы KSN недоступны*. Также, если вы используете Kaspersky Managed Detection and Response, вы получите события о нарушениях в работе решения. Использование KSN является обязательным условием для работы Kaspersky Managed Detection and Response. Kaspersky Endpoint Security включит использование KSN после применения политики, в которой администратор принял условия использования KSN. После того, как Положение о Kaspersky Security Network принято, Kaspersky Endpoint Security восстановит свою работу.

- После обновления Kaspersky Endpoint Security до версии 11.10.0 и выше без перезагрузки на компьютере будет установлено два приложения Kaspersky Endpoint Security. Не удаляйте предыдущую версию приложения вручную. Предыдущая версия приложения будет удалена автоматически после перезагрузки компьютера.

- После обновления Kaspersky Endpoint Security на компьютере под управлением Microsoft Windows 11 в контекстном меню файлов могут отображаться пункты для предыдущей и новой версии приложений. Для корректной работы контекстного меню файлов перезагрузите компьютер дважды.

- В период между завершением обновления приложения и перезагрузкой компьютера не работают сетевые компоненты приложения, если выключена самозащита приложения и остановлены все сетевые адаптеры. К сетевым компонентам приложения относятся Защита от веб-угроз, Защита от почтовых угроз, Защита от сетевых угроз, Сетевой экран, Предотвращение вторжений и Веб-Контроль. Для корректной работы приложения перезагрузите компьютер.

- В период между завершением обновления приложения и перезагрузкой компьютера не работает компонент Защита от атак BadUSB. Для корректной работы приложения перезагрузите компьютер.

- Невозможно обновить приложение, если процесс предыдущего обновления не завершен. Для корректной работы приложения перезагрузите компьютер.

- После обновления приложения с версий ниже Kaspersky Endpoint Security 11 для Windows обязательно перезагружайте компьютер.

- Если для управления Kaspersky Endpoint Security вы используете решение Kaspersky Security Center Cloud Console, запрещено обновлять приложение локально. При локальном обновлении приложения невозможно принять условия Соглашения об обработке данных для Kaspersky Security Center Cloud Console.

Поддержка архитектуры Arm

- Установка Kaspersky Endpoint Security в режиме Легкого агента на виртуальные машины с Arm-архитектурой не поддерживается.

- Шифрование диска Kaspersky не поддерживается на компьютерах с Arm-архитектурой.

- Шифрование файлов не поддерживается на компьютерах с Arm-архитектурой.

- Шифрование съемных дисков не поддерживается на компьютерах с Arm-архитектурой.

- На компьютерах под управлением Windows 11 для Arm64 EDR-агент не совместим с Bitdefender Endpoint Security Tools.

- Функциональность защиты аудиосигнала и защиты доступа приложений к веб-камерам не поддерживается на компьютерах с Arm-архитектурой.

- На компьютерах с архитектурой Arm расширение компонента Защита от почтовых угроз поддерживает работу с 32- и 64-разрядной версией Outlook 2016 и Outlook 2021, 2024, 365 для Arm64.

- Kaspersky Endpoint Security не отправляет в Kaspersky Sandbox объекты, предназначенные для Arm-архитектуры.

- Контроль печати не поддерживается на компьютерах с Arm-архитектурой.

- На компьютерах с архитектурой Arm задача *Поиск IOC* поддерживает работу с почтовыми файлами только следующих почтовых клиентов: 32- и 64-разрядная версии Outlook 2016 и Outlook 2021, 2024, 365 для Arm64.

- На компьютерах под управлением Windows 11 для Arm64 может быть недоступна аутентификации по токену: операционная система не может обнаружить действующий сертификат на токене. Такое поведение обусловлено особенностями взаимодействия операционной системы и программного обеспечения токена. Например, в операционной системе могут отсутствовать необходимые драйверы для работы токена. В этом случае Kaspersky Endpoint Security также не поддерживает аутентификацию по токену (Защита паролем). Вы можете использовать другие способы аутентификации, например, учетные данные пользователя.

Поддержка серверных платформ

- На серверах с включенной *функцией дедупликации данных* необходимо добавить файл fsdmhost.exe в список доверенных приложений. Это позволит оптимизировать работу приложения и избежать повышенной нагрузки на центральный процессор.

- Файловая система ReFS поддерживается с ограничениями:

  - Kaspersky Endpoint Security может некорректно обрабатывать события устранения угроз. То есть приложение, например, удалило вредоносный файл, но в отчетах может быть запись о том, что объект не обработан. При этом Kaspersky Endpoint Security устраняет угрозы в соответствии с настроенными параметрами приложения. Также Kaspersky Endpoint Security может создавать копию события *Объект будет вылечен при перезагрузке* для одного объекта.

  - Защита от файловых угроз может пропускать некоторые угрозы. При этом поиск вредоносного ПО работает корректно.

  - После запуска задачи *Поиск вредоносного ПО* исключения, добавленные с помощью технологии iChecker, сбрасываются после перезагрузки сервера.

  - Технология iSwift не поддерживается. Kaspersky Endpoint Security не учитывает исключения из проверки, добавленные с помощью технологии iSwift.

  - Kaspersky Endpoint Security не обнаруживает файлы eicar.com и susp-eicar.com, если файл meicar.exe находился на компьютере до установки Kaspersky Endpoint Security.

  - Kaspersky Endpoint Security может некорректно показывать уведомления об устранении угроз. То есть, приложение, например, может показать уведомление об угрозе, которая уже устранена.

- Шифрование файлов (FLE) и технология Шифрование диска Kaspersky (FDE) на серверных платформах не поддерживаются. При этом Kaspersky Endpoint Security может некорректно обрабатывать события шифрования данных.

- В серверных операционных системах не выводится предупреждение о необходимости лечения активного заражения.

- Операционная система Microsoft Windows Server 2008 исключена из поддержки. Установка приложения на компьютер под управлением операционной системы Microsoft Windows Server 2008 не поддерживается.

- Приложение Kaspersky Endpoint Security, установленное на сервер с развернутым решением Microsoft Data Protection Manager (DPM), может вызывать сбои в работе DPM. Это связано с ограничениями в работе DPM. Для устранения сбоев вам следует добавить локальные диски сервера в исключения для компонента Защита от файловых угроз и задач *Поиск вредоносного ПО*.

- Режим основных серверных компонентов (англ. Server Core Mode) поддерживается с ограничениями:
  - Недоступен локальный графический интерфейс приложения, включая уведомления, всплывающие подсказки и другие элементы интерфейса. У приложения нет возможности показать окна запросов, включая следующие окна:
    - запрос подтверждения обновления версии и модулей приложения;
    - запрос для перезагрузки компьютера;
    - запрос учетных данных для аутентификации на прокси-сервере;
    - запрос для получения доступа к устройству (Контроль устройств).
  - Недоступны следующие компоненты: Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль, Защита от атак BadUSB.
  - Недоступна функция Анти-Бриджинг.
  - Вы можете принять Положение о Kaspersky Security Network только в политике приложения в консоли Kaspersky Security Center.
  - Шифрование диска BitLocker доступно только с помощью доверенного платформенного модуля (TPM). Использовать PIN / пароль при шифровании невозможно, так как у приложения нет возможности показать окно запроса пароля для предзагрузочной аутентификации. Если в операционной системе включен режим совместимости с Федеральным стандартом обработки информации (FIPS), вам нужно подключить съемный диск для сохранения ключа шифрования до начала шифрования диска.

Поддержка виртуальных платформ

- Не поддерживается полнодисковое шифрование (FDE) на виртуальных машинах Hyper-V.
- Не поддерживается полнодисковое шифрование (FDE) на виртуальных платформах Citrix.
- Операционные системы Windows 10 Enterprise multi-session и Windows 11 Enterprise multi-session поддерживаются с ограничениями:
  - Kaspersky Endpoint Security выполняет лечение активных угроз без уведомления пользователя, как при лечении активного заражения на серверах. Из-за того, что операционная система позволяет работать в многосеансовом режиме, другие активные пользователи могут потерять свои данные, если не устранить угрозу немедленно.
  - Не поддерживается полнодисковое шифрование (FDE).
  - Не поддерживается управление BitLocker.
  - Не поддерживается работа Kaspersky Endpoint Security со съемными дисками. Инфраструктура Microsoft Azure определяет съемные диски как сетевые диски.
- Не поддерживается установка и использование шифрования файлов и папок (FLE) на виртуальных платформах Citrix.

- Для поддержки совместимости Kaspersky Endpoint Security для Windows с Citrix PVS выполняйте установку с включенной опцией **Обеспечить совместимость с Citrix PVS**. Опцию можно включить в мастере установки или через параметр командной строки `/pCITRIXCOMPATIBILITY=1`. При удаленной установке необходимо отредактировать файл с расширением kud, добавив в него параметр `/pCITRIXCOMPATIBILITY=1`.

- Citrix XenDesktop. Перед началом клонирования необходимо отключить самозащиту для клонирования виртуальных машин, которые используют vDisk.

- При подготовке эталонной машины для мастер-образа Citrix XenDesktop с предустановленным Kaspersky Endpoint Security для Windows и Агентом администрирования Kaspersky Security Center добавьте в конфигурационный файл исключения вида:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Подробнее о Citrix XenDesktop смотрите на сайте поддержки Citrix.

- В некоторых случаях на виртуальной машине, развернутой на гипервизоре VMware ESXi, попытка безопасного извлечения съемного диска может завершиться неудачно. Выполните безопасное извлечение устройства еще раз.

- Совместимость приложения Kaspersky Endpoint Security и гипервизора VMware ESXi имеет следующие ограничения:

  - Приложение Kaspersky Endpoint Security может быть несовместимо с драйверами Guest Introspection (vnetWFP.sys, vnetFLT.sys и другие). Для устранения несовместимости обновите драйверы до последней версии или удалите драйверы.

  - В некоторых случаях на виртуальной машине попытка безопасного извлечения съемного диска может завершиться неудачно. Выполните безопасное извлечение устройства еще раз.

- Установка Kaspersky Endpoint Security на виртуальные машины с VDA-агентом Citrix может завершиться с ошибкой совместимости. Это связано с ограничениями в работе Citrix Provisioning Services с антивирусными решениями. Лучшие практики по работе антивирусных решений с Citrix Provisioning Services см. на сайте поддержки Citrix.

- Kaspersky Endpoint Security пропускает проверку съемного диска при подключении диска к виртуальным машинам на гипервизоре Citrix (задача *Проверка съемных дисков*). На таких устройствах операционная система определяет подключенный съемный диск как сетевой диск. В этом случае вы можете использовать задачу *Выборочная проверка*. Поведение приложения не отличается в стандартном режиме и в режиме Легкого агента.

- Если Kaspersky Endpoint Security установлен на виртуальной машине в инфраструктуре, использующей технологию Citrix App Layering, обнаруженные приложением зараженные файлы со статусом *Объект будет удален при перезагрузке* не будут удалены автоматически при перезагрузке виртуальной машины.

  Для удаления таких файлов вам необходимо смонтировать VHDX-файл, содержащий пользовательский слой (User Layer), на компьютере администратора Citrix App Layering и выполнить поиск вредоносного ПО на смонтированном диске.

- Перед созданием снапшота "Золотого образа" виртуальной машины с установленным приложением Kaspersky Endpoint Security рекомендуется выключить виртуальную машину (сделать "холодный" снапшот). При создании снапшота включенной виртуальной машиной ("горячего" снапшота) корректная работа приложения не гарантируется.

Совместимость с Kaspersky Security Center

- В Kaspersky Security Center Web Console версии 14.1 и ниже в свойствах Сервера администрирования в разделе настройки прав доступа пользователей некорректно отображаются названия функциональных областей Анализ журналов и Мониторинг файловых операций.

- После восстановления приложения защита подключения компьютера к Серверу администрирования будет выключена. После восстановления приложения запустите задачу *Защита подключения к Серверу администрирования* повторно.

- В Консоли администрирования Kaspersky Security Center в окне **Выбор пользователя или группы пользователей** отображаются только первые 50 000 пользователей из списка пользователей Kaspersky Security Center. Подробнее см. в справке Kaspersky Security Center.

- При поиске управляемых устройств в Консоли администрирования Kaspersky Security Center на вкладке **Компоненты приложения** могут одновременно отображаться несколько вариантов названия одного и того же компонента приложения, в том числе названия, соответствующие предыдущим версиям Kaspersky Endpoint Security. Также названия некоторых компонентов могут дублироваться.

  Для поиска по компоненту вам достаточно выбрать один из отображаемых вариантов. Подробнее о поиске устройств см. в справке Kaspersky Security Center.

- В Kaspersky Security Center Web Console версии 15.1 Update 2 с установленными веб-плагином Kaspersky Endpoint Security для Windows 12.11 и выше и Unified Protection and Management Plug-in не срабатывают условия активации профиля для политики. Kaspersky Security Center не добавляет новые устройства в консоль, которые удовлетворяют условиям активации профиля.

Лицензирование

- При появлении системного сообщения с текстом *Ошибка приема данных* проверьте доступ к сети компьютера, на котором выполняется активация, или настройте параметры активации через Kaspersky Security Center Activation Proxy.

- В интерфейсе приложения дата истечения лицензии отображается в локальном времени компьютера.

- Установка приложения с подложенным файлом ключа на компьютере с нестабильным доступом в интернет может вызвать временное появление событий о том, что приложение не активировано или лицензия не допускает работу компонента. Это вызвано тем, что в процессе установки приложение сначала активирует встроенную пробную лицензию. Для этого требуется доступ в интернет.

- Во время пробного периода установка любого обновления приложения или патча на компьютере с нестабильным доступом в интернет может вызвать временное появление событий о том, что приложение не активировано. Это вызвано тем, что в процессе установки обновления приложение сначала активирует встроенную пробную лицензию. Для этого требуется, доступ в интернет.

- Если при установке приложение было автоматически активировано пробной лицензией, а затем удалено без сохранения информации о лицензии, при повторной установке оно не активируется пробной лицензией автоматически. В этом случае активируйте приложение вручную.

- Если вы используете Kaspersky Security Center версии 11 и Kaspersky Endpoint Security для Windows 14.3, отчеты о работе компонентов могут работать некорректно. Если вы установили компоненты Kaspersky Endpoint Security, которые не входят в вашу лицензию, Агент администрирования может отправлять в журнал событий Windows ошибки статусов компонентов. Чтобы избежать ошибок, удалите компоненты, которые не входят в лицензию.

Защита от почтовых угроз

- При проверке почты с помощью расширения Защиты от почтовых угроз для Microsoft Outlook мы рекомендуем использовать режим кеширования сервера Exchange (Use Cached Exchange Mode).

- Kaspersky Endpoint Security не поддерживает работу с 64-битной версией почтового клиента Microsoft Outlook. То есть, Kaspersky Endpoint Security не проверяет файлы, связанные с работой 64-битной версии почтового клиента Microsoft Outlook (PST- и OST-файлы), даже если почта включена в область проверки.

- Kaspersky Endpoint Security не поддерживает работу с почтовым клиентом Microsoft Outlook New.

- Если вы выключили лечение обнаруженных угроз для Защиты от почтовых угроз и получили зараженное письмо в почтовый ящик Outlook, Защита от веб-угроз может заблокировать обмен данными с сервером Exchange по протоколу MAPI. При этом Защита от веб-угроз формирует событие об обнаружении угрозы и отправляет его в Kaspersky Security Center. Для восстановления соединения между компьютером и сервером Exchange, необходимо вручную удалить зараженное письмо из почтового ящика Outlook.

  При обновлении версии приложения без перезагрузки уровень защиты Защиты от почтовых угроз временно снижается (до одной минуты). Если во время обновления приложения вы получите зараженное письмо в почтовый ящик Outlook, Защита от веб-угроз также заблокирует соединение с сервером Exchange по протоколу MAPI. Для восстановления соединения удалите зараженное письмо из почтового ящика Outlook.

Откат вредоносных действий

- Приложение восстанавливает файлы только на устройствах с файловой системой NTFS и FAT32.

- Приложение восстанавливает файлы размером не более 100 МБ.

- Приложение восстанавливает файлы следующих расширений: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.

- Невозможно восстановить файлы, размещенные на сетевых дисках, а также на перезаписываемых CD/DVD-дисках.

- Невозможно восстановить файлы, зашифрованные с помощью Encryption File System (EFS). Подробнее о работе EFS см. на сайте Microsoft.

- Приложение не контролирует изменения файлов, выполненные процессами на уровне ядра операционной системы.

Сетевой экран

- Если в сетевом пакетном правиле или сетевом правиле приложения указаны DNS-имена, то Kaspersky Endpoint Security может отправлять запросы на DNS-сервер для определения IP-адресов этих ресурсов. Для контроля сетевой активности Сетевой экран использует IP-адреса. Поэтому приложение преобразует DNS-имена в IP-адреса. Рекомендуется использовать DNS-имена в правилах только для компьютеров локальной сети или внутренних сервисов.

- Чтобы задать правило для всех адресов IPv6, вам нужно добавить диапазон адресов ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Сетевой экран не поддерживает маску ::/0.

- Фильтрация пакетов или соединений по локальным адресам, физическому интерфейсу и времени жизни (TTL) пакета поддерживается в следующих случаях:
  - По локальному адресу для исходящих пакетов или соединений в правилах приложений для TCP и UDP и пакетных правилах.
  - По локальному адресу для входящих пакетов или соединений (кроме UDP) в запрещающих правилах приложений и пакетных правилах.
  - По времени жизни (TTL) пакета в запрещающих пакетных правилах для входящих или исходящих пакетов.
  - По сетевому интерфейсу для входящих и исходящих пакетов или соединений в пакетных правилах.
- Если для разрешающего пакетного правила вы настроили сетевой адаптер или время жизни пакета (TTL), приоритет такого правила ниже запрещающего правила приложений. То есть, если приложению запрещена сетевая активность (например, приложение находится в группе доверия *Сильные ограничения*), то разрешить сетевую активность с помощью пакетного правила с такими настройками невозможно. В остальных случаях приоритет пакетного правила выше сетевого правила приложений.
- При импорте списка пакетных правил Сетевого экрана Kaspersky Endpoint Security может изменять названия правил. Приложение определяет правила с одинаковым набором основных параметров: протокол, направление, удаленные и локальные порты, время жизни пакета (TTL). Если этот набор основных параметров совпадает для нескольких правил, приложение присваивает этим правилам одно название или добавляет к названию тег с параметром. Таким образом, Kaspersky Endpoint Security импортирует все пакетные правила, но название правил, которые имеют одинаковые основные параметры, может быть изменено.
- Если вы включили запись событий в отчет для приложения в сетевом правиле, при перемещении приложения в другую группу доверия не будут применены ограничения этой группы доверия. Таким образом, если приложение находится в группе доверия "Доверенные", такое приложение не имеет сетевых ограничений. Затем вы включили запись событий в отчет для этого приложения и переместили приложение в группу доверия *Недоверенные*. Сетевой экран не будет применять сетевые ограничения для этого приложения. Мы рекомендуем сначала переместить приложение в нужную группу доверия, а затем включить запись событий в отчет. Если этот способ не подходит, настройте ограничения для этого приложения вручную в параметрах сетевого правила. Ограничение касается только локального интерфейса приложения. Перемещение приложения между группами доверия в политике работает корректно.
- Компоненты Сетевое экран и Предотвращение вторжений имеют общие параметры: права приложений и защищаемые ресурсы. Если вы измените эти параметры для Сетевого экрана, Kaspersky Endpoint Security автоматически применит новые параметры для Предотвращения вторжений. Таким образом, если вы, например, разрешили изменение общих параметров в политике для Сетевого экрана ("замок" открыт), параметры Предотвращения вторжений тоже будут доступны для изменения.
- В Kaspersky Endpoint Security версии 11.6.0 и ниже при срабатывании сетевого пакетного правила в отчете Сетевого экрана в графе **Имя приложения** всегда отображается значение *Kaspersky Endpoint Security*. При этом Сетевой экран блокирует соединение на пакетном уровне для всех приложений. В Kaspersky Endpoint Security версии 11.7.0 и выше поведение изменено. В отчет Сетевого экрана добавлена графа **Тип правила**. При срабатывании сетевого пакетного правила значение в графе **Имя приложения** остается пустым.
- Если вы запретили любую сетевую активность с помощью Сетевого экрана, компонент Защита от сетевых угроз может обнаружить атаку типа Сканирование портов. Это связано с тем, что приложение запускает Защиту от сетевых угроз раньше, чем Сетевой экран, чтобы обнаруживать подозрительную активность в сети.

Защита от атак BadUSB

- Kaspersky Endpoint Security сбрасывает таймаут блокировки USB-устройства при блокировании компьютера (например, истекло время ожидания до блокировки экрана). То есть, если вы несколько раз неверно ввели код авторизации USB-устройства и приложение заблокировало USB-устройство, Kaspersky Endpoint Security позволит повторить попытку авторизации после разблокирования компьютера. Kaspersky Endpoint Security в этом случае не блокирует USB-устройство на время, заданное в параметрах компонента Защита от атак BadUSB.

- Kaspersky Endpoint Security сбрасывает таймаут блокировки USB-устройства при приостановке защиты компьютера. То есть, если вы несколько раз неверно ввели код авторизации USB-устройства и приложение заблокировало USB-устройство, Kaspersky Endpoint Security позволит повторить попытку авторизации после возобновления защиты компьютера. Kaspersky Endpoint Security в этом случае не блокирует USB-устройство на время, заданное в параметрах компонента Защита от атак BadUSB.

Kaspersky Security Network

- Kaspersky Endpoint Security не поддерживает KSN Proxy с использованием HTTPS (в параметрах подключения к KSN Proxy установлен флажок **Использовать HTTPS**), если адрес сервера содержит нелатинские буквы (не ASCII символы).

- При переключении в Kaspersky Security Center приложения с использования глобального Kaspersky Security Network на использование локального Kaspersky Security Network (KPSN) или, наоборот, с локального Kaspersky Security Network на глобальный Kaspersky Security Network, в продуктовой политике отключается опция участия в Kaspersky Security Network. После выполнения переключения ознакомьтесь с текстом Положения о Kaspersky Security Network и подтвердите согласие на участие. Ознакомиться с текстом Положения вы можете в интерфейсе приложения или при редактировании продуктовой политики.

- Начиная с версии Kaspersky Endpoint Security для Windows 12.9 при переключении с KPSN на глобальный KSN необходимо повторно подтвердить согласие с Положением о Kaspersky Security Network. Для этого вам нужно в свойствах политики или в интерфейсе приложения включить использование Kaspersky Security Network и подтвердить согласие с Положением о Kaspersky Security Network. Если ранее вы уже использовали глобальный KSN, вам нужно сначала выключить использование KSN, далее повторно включить использование KSN и подтвердить согласие с Положением о Kaspersky Security Network. Если вы не подтвердите согласие с Положением о Kaspersky Security Network, приложение не получит доступ к данным Kaspersky Security Network.

- Kaspersky Endpoint Security не отправляет файлы текстовых форматов на проверку в Kaspersky Security Network (например, TXT, CSV, LOG, DOCX без макросов). Приложение отправляет на проверку в KSN файлы, которые могут представлять угрозу. К таким файлам относятся исполняемые файлы или файлы, которые могут содержать исполняемый код (например, макросы в DOCX-файлах). Проверку файлов текстовых форматов выполняют другие компоненты приложения. При этом вы можете проверить репутацию текстового файла вручную из контекстного меню файла. Если текстовый файл имеет репутацию *Недоверенная (Kaspersky Security Network)*, приложение игнорирует действие, заданное для обнаруженных угроз.

Контроль приложений

- При работе с правилами Контроля приложений не рекомендуется добавлять суммарно в рамках различных категорий более 100 000 условий включения и исключения приложений, при условии работы Kaspersky Endpoint Security на компьютере с аппаратной конфигурацией, соответствующей минимальным требованиям, под управлением Microsoft Windows 10.

- При работе с правилами Контроля приложений в Kaspersky Security Center Web Console поддерживается архивы только в формате ZIP. Архивы других форматов, например, RAR или 7z, не поддерживаются. Если вы работаете с правилами Контроля приложений в Консоли администрирования (MMC), такого ограничения нет.

- При работе с правилами Контроля приложений в Kaspersky Security Center Web Console поддерживается загрузка файлов размером не более 104 МБ. Если вы работаете с правилами Контроля приложений в Консоли администрирования (MMC), такого ограничения нет.

- При работе на операционный системе Microsoft Windows 10 в режиме списка запрещенных приложений возможно некорректное применение правил блокировки, в результате которого будет заблокирован запуск приложений, которые не указаны в правилах.

- Если при обновлении версии Kaspersky Endpoint Security добавлены новые *предустановленные правила Контроля приложения*, то применить эти правила к предыдущим версиям приложения невозможно.

- При блокировании компонентом Контроль приложений PWA-приложений (Progressive Web App) в отчете в качестве заблокированного приложения указывается appManifest.xml.

- Для добавления стандартного приложения Блокнот в правило Контроля приложений для Windows 11 не рекомендуется указывать путь к приложению. На компьютерах под управлением Windows 11 операционная система использует метро-приложение Блокнот, расположенное в папке `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe`. В предыдущих версиях операционной системы приложение Блокнот расположено в следующих папках:

  - `C:\Windows\notepad.exe`;
  - `C:\Windows\System32\notepad.exe`;
  - `C:\Windows\SysWOW64\notepad.exe`.

  При добавлении приложения Блокнот в правило Контроля приложений вы можете указать, например, название приложения и хеш файла из свойств запущенного приложения.

- При миграции политики KSWS в профиль политики KES мастер массовой конвертации политики и задач (мастер миграции) переименовывает категории приложений, если имена категорий содержат недопустимые символы: `'` `*` `<` `>` `?` `\` `:` `|`. Мастер миграции заменит эти символы на символ `_`. Например, категория приложений `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` будет переименована в категорию `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Контроль устройств

- Kaspersky Endpoint Security может регистрировать события подключения и отключения внешних устройств. Службы Windows выполняют подключение или отключение устройств под системной учетной записью. Таким образом, определить пользователя, который выполняет подключение или отключение устройства невозможно. Kaspersky Endpoint Security указывает учетную запись SYSTEM в событии.

- Доступ к устройствам типа Принтер, которые добавлены в список доверенных, запрещается правилами блокировки устройств и шин.

- Для MTP-устройств поддерживается контроль операций Read, Write, Connect, если используются драйверы Microsoft, встроенные в операционную систему. Если для работы с устройством пользователь устанавливает кастомный драйвер (например, в составе iTunes или Android Debug Bridge), контроль Read и Write операций может не работать.

- При работе с MTP-устройствами изменение правил доступа выполняется после переподключения устройства.

- Компонент Контроль устройств регистрирует события, связанные с контролируемыми устройствами, такие как подключение и отключение устройства, чтение файла с устройства, запись файла на устройство и другие события. При этом Kaspersky Endpoint Security регистрирует события отключения только для следующих типов устройств: Портативные устройства (MTP), Съемные диски, Дискеты, CD/DVD-приводы. Для остальных типов устройств приложение не регистрирует события отключения. Операцию подключения устройства к компьютеру приложение регистрирует для всех типов устройств.

- Если вы добавляете устройство в доверенные по маске модели и используете символы, которые входят в идентификатор, но не входят в название модели, устройства не добавятся. На рабочей станции эти устройства будут добавлены в доверенные по маске идентификатора.

- При обновлении приложения без перезагрузки Контроль устройств не применяет правила доступа к устройствам, которые подключены повторно. При этом, если устройство было подключено до обновления, Контроль устройств применяет правила корректно. Для корректной работы приложения с устройствами, которые подключены повторно, перезагрузите компьютер.

- На компьютерах с установленным приложением Kaspersky Endpoint Security версии 12.0 для типа устройств **Сетевые принтеры** режим доступа **Разрешать и не записывать в отчет** имеет название **Зависит от шины подключения**, если на компьютере применена политика Kaspersky Endpoint Security версии 12.1. В этих режимах приложение выполнят одни и те же действия. В Kaspersky Endpoint Security версии 12.1 режим доступа к сетевым принтерам называется корректно – **Разрешать и не записывать в отчет**.

- Начиная с версии Kaspersky Endpoint Security для Windows 12.0 в приложении добавлена возможность настраивать правила печати для принтеров (контроль печати). При установке приложения с функцией контроля печати или при обновлении приложения на версию с функцией контроля печати необходимо перезагрузить компьютер. До перезагрузки компьютера Kaspersky Endpoint Security не применяет правила печати, а может управлять только доступом к принтерам. Если перезагрузка компьютера влияет на рабочие процессы в вашей организации, вы можете перезапустить только сервис spoolsv (Print Spooler). Контроль печати не поддерживается на компьютерах с Arm-архитектурой.

- Начиная с версии Kaspersky Endpoint Security для Windows 12.0 в приложении для типа устройств **Wi-Fi** добавлена поддержка протокола WPA3. Если на компьютере применена политика Kaspersky Endpoint Security версии 12.2, на компьютерах с установленным приложением Kaspersky Endpoint Security версии 11.11.0 и более ранних версий будет выбран протокол WPA2, для версий 12.0 – 12.1 будет выбран протокол WPA2 / WPA3, для версии 12.2 и выше – WPA3.

- Устройства Apple относятся к типу портативных устройств (MTP) и iTunes-устройств. Операционная система может некорректно распознать подключение устройства Apple и не определить устройство Apple как портативное устройств (MTP). Из-за этого устройство Apple будет недоступно в файловом менеджере, но доступно в приложении iTunes. В результате Kaspersky Endpoint Security контролирует доступ к устройству Apple только в приложении iTunes. Для доступа к устройству Apple как к портативному устройству (MTP) вам нужно перейти в Диспетчер устройств и удалить Apple Mobile Device USB Driver из списка Контроллеров USB. После перезагрузки компьютера операционная система определит устройство Apple как портативное устройство (MTP) и iTunes-устройство. Kaspersky Endpoint Security будет контролировать доступ к устройству как в приложении iTunes, так и в файловом менеджере.

- В Kaspersky Endpoint Security для Windows версии 12.3 для типа устройств **Bluetooth** изменились настройки доступа. Если в предыдущей версии приложения для этого типа устройств вы установили значение **Зависит от шины подключения**, то после обновления приложения до версии 12.3 будет установлено значение **Разрешать и не записывать в отчет**. Поведение приложения при этом не изменится.

- Контроль устройств поддерживает Bluetooth-устройства только через стек Microsoft Windows Bluetooth. Контроль устройств может работать некорректно со сторонними стеками Bluetooth.

- Если Bluetooth-устройство скрывает или подменяет свой класс (англ. Class of Device, COD), Контроль устройств может работать некорректно.

- На компьютерах под управлением Windows 7 или Windows 8 с некоторыми драйверами Realtek для Bluetooth-адаптера невозможно разрешить подключение Bluetooth-устройств только как устройств ввода (класс HID-устройств). То есть, если вы в параметрах приложения запретили доступ к Bluetooth-устройствам и добавили устройства ввода в исключения, Контроль устройств может запретить доступ к устройствам полностью.

Веб-Контроль

- Не поддерживаются форматы OGV и WEBM.

- Не поддерживается протокол RTMP.

- Веб-Контроль поддерживает работу только с WSL1. Приложение не контролирует трафик для WSL2.

Адаптивный контроль аномалий

- Мы рекомендуем при необходимости создавать исключения автоматически на основе события. При ручном добавлении исключения при указании Целевого объекта добавляйте символ `*` в начало пути.

- Не поддерживается формирование отчета **Отчет о срабатываниях правил Адаптивного контроля аномалий**, если в данные попадает хотя бы одно событие, которое содержит более 260 символов.

- Не поддерживается добавление исключений из хранилища срабатывания правил Адаптивного контроля аномалий, если свойства объекта или процесса имеют значение, которое содержит более 256 символов (например, путь к целевому объекту). Вы можете добавить исключение вручную в параметрах политики. Также вы можете добавить исключение в отчете о срабатывании правил Адаптивного контроля аномалий.

- В Kaspersky Security Center 15.1 невозможно сформировать подробный отчет **Отчет о состоянии правил Адаптивного контроля аномалий** для конкретного правила.

- Правила Адаптивного контроля аномалий доступны только на том языке, соответствующем языку установки веб-плагина. При смене языка интерфейса Web Console отображает пустой список правил. Для доступа к правилам необходимо вернуть язык интерфейса, соответствующий языку установки веб-плагина.

Шифрование диска (FDE)

- Шифрование диска Kaspersky не поддерживается на компьютерах с Arm-архитектурой.

- Шифрование диска BitLocker не поддерживается на компьютерах под управлением операционных систем Windows Home.

- При шифровании диска BitLocker пользователь может вручную сменить пароль для аутентификации с помощью Windows API. При этом BitLocker игнорирует требования к паролю, заданные в политике Kaspersky Endpoint Security. То есть пользователь может задать любой пароль.

- Для работы шифрования жестких дисков перезагрузите операционную систему после установки приложения.

- В Агенте аутентификации не поддерживаются иероглифы и специальные символы `|` и `\`.

- Для оптимальной работы компьютера после шифрования необходим процессор с поддержкой набора команд шифрования AES-NI (Intel Advanced Encryption Standard New Instructions). Если процессор не поддерживает AES-NI, производительность компьютера может снизиться.

- При наличии процессов, обратившихся к зашифрованным устройствам до того, как приложение предоставило к этим устройствам доступ, оно выводит предупреждение о необходимости завершить такие процессы. Если завершить процессы невозможно, подключите зашифрованные устройства повторно.

- Уникальные идентификаторы жестких дисков в статистике шифрования устройств отображаются в инвертированном виде.

- Мы не рекомендуем выполнять форматирование устройств во время их шифрования.

- При одновременном подключении к компьютеру нескольких съемных дисков политика шифрования может применяться только к одному съемному диску. При повторном подключении съемных дисков политика шифрования применяется корректно.

- Шифрование может не запуститься на сильно фрагментированном жестком диске. Выполните дефрагментацию жесткого диска.

- При шифровании жестких дисков гибернация блокируется с момента старта задачи шифрования до первой перезагрузки компьютера в операционных системах Microsoft Windows 7 / 8 / 8.1 / 10 и после установки шифрования жестких дисков до первой перезагрузки операционных систем Microsoft Windows 8 / 8.1 / 10. При расшифровке жестких дисков гибернация блокируется с момента полной расшифровки загрузочного жесткого диска до первой перезагрузки операционной системы. В операционных системах Microsoft Windows 8 / 8.1 / 10 при включенной функции быстрого запуска системы блокировка гибернации не позволяет выключить операционную систему.

- При шифровании диска BitLocker невозможно сменить пароль при выполнении процедуры восстановления на компьютерах под управлением Windows 7. После ввода ключа восстановления и загрузки операционной системы Kaspersky Endpoint Security не предложит пользователю сменить пароль или PIN-код. Таким образом, установить новый пароль или PIN-код невозможно. Проблема связана с особенностями операционной системы. Для продолжения работы вам нужно перешифровать жесткий диск.

- Мы не рекомендуем использовать инструмент xbootmgr.exe с включением дополнительных провайдеров. Например, Dispatcher, Network, Drivers.

- Не поддерживается форматирование зашифрованного съемного диска на компьютере с установленным приложением Kaspersky Endpoint Security для Windows.

- Не поддерживается форматирование зашифрованного съемного диска с файловой системой FAT32 (диск отображается как зашифрованный). Для форматирования диска переформатируйте его файловую систему в NTFS.

- Не поддерживается совместное существование нескольких загрузочных агентов на одном зашифрованном компьютере.

- При попытке восстановления образа загрузочного GPT-диска с незашифрованным состоянием может быть нарушена работа операционной системы. Чтобы избежать этого, воспользуйтесь рекомендациями:

  - Полностью расшифруйте диск перед восстановлением резервной копии образа.

  - Используйте посекторное копирование при создании образа.

  - Удалите данные из первых секторов зашифрованного диска перед восстановлением образа и заново инициализируйте диск.

- Невозможно получить доступ к съемному диску, который был зашифрован ранее на другом компьютере, при одновременном выполнении следующих условий:

  - Отсутствие связи с сервером Kaspersky Security Center.

  - Авторизация пользователя с новым токеном или паролем.

  При возникновении подобной ситуации перезагрузите компьютер. После перезагрузки компьютера доступ к зашифрованному съемному диску будет предоставлен.

- Может не поддерживаться распознавание USB-устройств Агентом аутентификации, если в параметрах BIOS включен режим xHCI для USB.

- Для SSHD-устройств не поддерживается технология Шифрование диска Kaspersky (FDE) для SSD-части устройства, предназначенной для кеширования часто используемых данных.

- Не поддерживается шифрование жестких дисков в 32-битных операционных системах Microsoft Windows 8 / 8.1 / 10, которые работают в режиме UEFI.

- Перед повторным шифрованием расшифрованного жесткого диска выполните перезагрузку компьютера.

- Шифрование жестких дисков несовместимо с Антивирусом Касперского для UEFI. Мы не рекомендуем использовать шифрование жестких дисков на компьютерах с установленным Антивирусом Касперского для UEFI.

- Создание учетных записей Агента аутентификации на основе учетных записей Microsoft поддерживается со следующими ограничениями:

  - Не поддерживается технология единого входа.

  - Не поддерживается автоматическое создание учетных записей Агента аутентификации, если выбрана опция создания учетных записей для пользователей, которые выполняют вход в систему в последние N дней.

- Если имя учетной записи Агента аутентификации сформировано в виде `<domain>/<Windows account name>`, после изменения имени компьютера измените имена учетных записей, которые созданы для локальных пользователей этого компьютера. Например, на компьютере `Ivanov` существует локальный пользователь `Ivanov`, для которого была создана учетная запись Агента аутентификации с именем `Ivanov/Ivanov`. Если имя компьютера `Ivanov` было изменено, например, на `Ivanov-PC`, измените имя учетной записи Агента аутентификации для пользователя `Ivanov` с `Ivanov/Ivanov` на `Ivanov-PC/Ivanov`. Для изменения имени учетной записи вы можете воспользоваться локальной задачей управления учетными записями Агента аутентификации. До изменения имени учетной записи аутентификация в предзагрузочной среде возможна по старому имени (например, `Ivanov/Ivanov`).

- Если на компьютере, который зашифрован с помощью технологии Шифрование диска Kaspersky, пользователю разрешен вход только по токену и требуется пройти процедуру восстановления доступа, убедитесь, что после восстановления доступа к зашифрованному компьютеру для этого пользователя разрешен вход по паролю. Пароль, который задал пользователь при восстановлении доступа, может не сохраниться. В этом случае пользователю придется снова проходить процедуру восстановления доступа к зашифрованному компьютеру при следующей перезагрузке.

- Если при расшифровке жесткого диска с помощью утилиты восстановления FDE Recovery Tool данные на исходном устройстве перезаписываются расшифрованными данными, процесс расшифровки может завершиться ошибкой. Часть данных на жестком диске останется зашифрованной. Мы рекомендуем в параметрах расшифровки устройства с помощью FDE Recovery Tool выбирать вариант сохранения расшифрованных данных в файл.

- Если при изменении пароля в Агенте аутентификации после появления сообщения с текстом *Ваш пароль успешно изменен. Нажмите OK* пользователь перезагружает компьютер, новый пароль не сохраняется. Для последующей аутентификации в предзагрузочной среде необходимо использовать старый пароль.

- Шифрование дисков несовместимо с технологией Intel Rapid Start.

- Шифрование дисков несовместимо с технологией ExpressCache.

- В некоторых случаях при попытке расшифровать зашифрованный диск с помощью утилиты FDE Recovery Tool после прохождения процедуры "Запрос-Ответ" утилита ошибочно детектирует состояние устройства как незашифрованное. В логе работы утилиты появляется событие, что устройство успешно расшифровано. В этом случае для расшифровки устройства необходимо повторно запустить процесс восстановления данных.

- После обновления плагина Kaspersky Endpoint Security для Windows в Web Console в свойствах клиентского компьютера не показывается ключ восстановления Bitlocker до перезапуска службы Web Console.

- Остальные ограничения поддержки полнодискового шифрования и список устройств, для которых шифрование жестких дисков поддерживается с ограничениями, см. в базе знаний Службы технической поддержки.

Шифрование файлов (FLE)

- Шифрование файлов не поддерживается на компьютерах с Arm-архитектурой.

- Шифрование файлов и папок не поддерживается в операционных системах семейства Microsoft Windows Embedded.

- Для шифрования файлов и папок требуется перезагрузка операционной системы после установки приложения.

- Приложение поддерживает шифрование файлов только на устройствах с файловой системой NTFS и FAT32. Если зашифрованный файл перенести на устройство с неподдерживаемой файловой системой (например, exFAT), файл на этом устройстве не будет зашифрован и будет доступен для изменения.

- Если зашифрованный файл хранится на компьютере с доступной функцией шифрования и вы обращаетесь к нему с компьютера, где шифрование недоступно, к этому файлу будет предоставлен прямой доступ. Зашифрованный файл, который хранится в сетевой папке на компьютере с доступной функцией шифрования, копируется на компьютер с недоступной функцией шифрования в незашифрованном виде.

- Мы рекомендуем расшифровать файлы, которые зашифрованы с помощью Encrypting File System, перед шифрованием файлов с помощью Kaspersky Endpoint Security для Windows.

- После шифрования файла его размер увеличивается на 4 КБ.

- После шифрования в свойствах файла устанавливается атрибут *Архивный*.

- При копировании расшифрованного файла, например, на съемный диск файл может остаться зашифрованными. Это связано с тем, что при попытке получить доступ к зашифрованному файлу файловый менеджер (например, explorer.exe) сохраняет хеш файла в специальный список процесса. После расшифровки файла при попытке файлового менеджера получить доступ к файлу, процесс выполняет поиск хеша файла в списке. Если хеш найден, Kaspersky Endpoint Security оставляет файл в зашифрованном виде. Чтобы избежать этого, вам нужно очистить список процесса. Операционная система автоматически очищает список процесса по мере заполнения. Также вы можете очистить список процесса вручную. Для этого вы можете перезагрузить компьютер, перезапустить процесс, с помощью которого вы пытаетесь получить доступ к файлу (например, explorer.exe), или вы можете воспользоваться другим файловым менеджером, который вы не использовали для доступа к зашифрованному файлу.

- При распаковке зашифрованного архива файлы, которые хранятся в распакованной папке, перезаписываются файлами, которые входят в состав зашифрованного архива, если их имена совпадают. Пользователь не уведомляется об операции перезаписи.

- При распаковке зашифрованного архива убедитесь, что на диске достаточно свободного пространства для распакованных файлов. Если на диске недостаточно пространства, распаковка архива может быть завершена, но файлы будут повреждены. При этом Kaspersky Endpoint Security может не показать сообщений об ошибках.

- В интерфейсе портативного файлового менеджера не отображаются сообщения об ошибках, которые возникают в процессе его работы.

- На компьютере с установленным компонентом шифрования файлов Kaspersky Endpoint Security для Windows не выполняется запуск портативного файлового менеджера.

- Получить доступ к съемному диску с помощью портативного файлового менеджера невозможно при одновременном выполнении следующих условий:

  - отсутствует связь с Kaspersky Security Center;

  - на компьютере установлено приложение Kaspersky Endpoint Security для Windows;

  - на компьютере не выполнялось шифрование данных (FDE или FLE).

  Получить доступ невозможно, даже если вы знаете пароль для портативного файлового менеджера.

- При использовании шифрования файлов приложение несовместимо с почтовым клиентом Sylpheed.

- Kaspersky Endpoint Security для Windows не поддерживает правила запрета доступа к зашифрованным файлам для некоторых приложений. Это связано с тем, что некоторые операции с файлами выполняет стороннее приложение. Например, копирование файла выполняет файловый менеджер, а не само приложение. Таким образом, если для почтового клиента Outlook запрещен доступ к зашифрованным файлам, Kaspersky Endpoint Security может разрешить доступ почтовому клиенту к зашифрованному файлу, если пользователь скопировал файлы в электронное сообщение через буфер обмена или перетащил файлы. Операцию копирования выполнил файловый менеджер, для которого правила запрета доступ к зашифрованным файлам не заданы, то есть доступ разрешен.

- При шифровании съемных дисков с поддержкой портативного режима не поддерживается отмена срока действия пароля.

- Не поддерживается изменение параметров файла подкачки. Вместо заданных значений параметров операционная система использует значения по умолчанию.

- При работе с зашифрованными съемными дисками используйте безопасное извлечение. При небезопасном извлечении съемного диска мы не гарантируем сохранность данных.

- После шифрования файлов выполняется безопасное удаление их незашифрованных оригиналов.
- Не поддерживается синхронизация автономных файлов с помощью Client-Side Caching (CSC). Также не поддерживается шифрование автономных файлов и технология Branch Caching для серверов по протоколу SMB. Мы рекомендуем запрещать автономную работу с общими ресурсами на уровне групповых политик. Файлы, которые находятся в автономном режиме, доступны для изменения. В результате синхронизации могут быть утрачены изменения, которые внесены в автономный файл.
- Не поддерживается создание зашифрованного архива в корне системного жесткого диска.
- Возможны проблемы с доступом к зашифрованным файлам по сети. Мы рекомендуем разместить файлы на другом источнике или убедиться, что компьютер, который используется как файловый сервер, находится под управлением того же Сервера администрирования Kaspersky Security Center.
- При смене раскладки клавиатуры может зависать окно ввода пароля для самораспаковывающегося зашифрованного архива. Для решения проблемы закройте окно ввода пароля, смените в операционной системе язык ввода по умолчанию и повторно введите пароль для зашифрованного архива.
- При использовании шифрования файлов на системах с несколькими разделами на одном диске мы рекомендуем использовать настройку автоматического определения размера файла pagefile.sys. После перезагрузки компьютера файл pagefile.sys может перемещаться между разделами диска.
- После применения правил шифрования файлов, включая файлы в папке *Мои документы*, убедитесь, что пользователи, для которых было применено шифрование, успешно получают доступ к зашифрованным файлам. Для этого каждый из пользователей должен войти в систему при наличии связи с Kaspersky Security Center. Если пользователь попытается получить доступ к зашифрованным файлам без связи с Kaspersky Security Center, система может зависнуть.
- При попадании системных файлов в область шифрования FLE в отчетах могут появиться события об ошибках шифрования этих файлов. Сами файлы, указанные в этих событиях, не шифруются.
- Pico-процессы не поддерживаются.
- Пути, которые зависят от регистра, не поддерживаются. При применении правил шифрования или расшифровки пути в продуктовых событиях отображаются в нижнем регистре.
- Мы не рекомендуем шифровать файлы, которые используются системой во время загрузки. Если эти файлы зашифрованы, при попытке доступа к зашифрованным файлам без связи с Kaspersky Security Center возможно зависание системы или появление запросов на получение доступа к незашифрованным файлам.
- При совместной работе по сети под правилами шифрования FLE через приложения, использующие метод отображения файла в память, например WordPad или FAR, и приложения, предназначенные для работы с файлами большого объема, например Notepad++, файл в незашифрованном виде может блокироваться на неопределенный срок без возможности получить к нему доступ с компьютера, на котором он находится.
- Kaspersky Endpoint Security не шифрует файлы, содержимое которых расположено в облачном хранилище OneDrive и других папках с именем OneDrive. Также Kaspersky Endpoint Security блокирует копирование зашифрованных файлов в папки OneDrive, если эти файлы не добавлены в правило расшифровки.
- При установленном компоненте файлового шифрования не работает управление пользователями и группами в режиме WSL (Windows Subsystem for Linux).

- При установленном компоненте файлового шифрования отсутствует поддержка режима POSIX (Portable Operating System Interface) для переименования или удаления файлов.

- Рекомендуется не шифровать временные файлы, так как это может привести к потере данных. Например, Microsoft Word создает временные файлы при работе с документом. Если временные файлы зашифрованы, а исходный файл нет, то при попытке сохранить документ пользователь может получить ошибку *Доступ запрещен*. Также Microsoft Word может сохранить файл, но открыть документ в следующий раз будет невозможно, то есть данные будут утеряны. Чтобы не допустить потери данных, вам нужно исключить папку с временными файлами из правил шифрования.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- Невозможно выполнить проверку объекта, помещенного на карантине в результате выполнения задачи *Помещение файла на карантин*.

- Невозможно поместить на карантин альтернативный поток данных (англ. Alternate Data Stream, ADS), размер которого превышает 4 МБ. Kaspersky Endpoint Security пропускает такой ADS без уведомления пользователя.

- Kaspersky Endpoint Security не выполняет задачу *Поиск IOC* на сетевых дисках, если в свойствах задачи указан путь к папке начиная с буквы диска. Kaspersky Endpoint Security поддерживает только UNC-формат пути для работы задачи *Поиск IOC* на сетевых дисках. Например, `\\server\shared_folder`.

- Для корректной работы задачи *Поиск IOC* с терминами EmailItem необходимо обновить веб-плагин Kaspersky Endpoint Security до актуальной версии.

- На компьютерах с архитектурой Arm задача *Поиск IOC* поддерживает работу с почтовыми файлами только следующих почтовых клиентов: 32- и 64-разрядная версии Outlook 2016 и Outlook 2021, 2024, 365 для Arm64.

- Импорт конфигурационного файла приложения завершится с ошибкой, если в конфигурационном файле включен параметр интеграции с Kaspersky Sandbox. Перед экспортом параметров приложения выключите Kaspersky Sandbox. Затем выполните процедуру экспорта / импорта. После импорта конфигурационного файла включите Kaspersky Sandbox.

- При импорте политики из KLP-файла не применяется значение параметра, который определяет принятие условий Соглашения для Kaspersky Detection and Response Expert. В результате после импорта политики Kaspersky Endpoint Security не выполняет функции EDR-агента. Для работы EDR-агента откройте политику, измените любой параметр и сохраните параметры политики.

- При обнаружении индикатора компрометации при выполнении задачи *Поиск IOC* приложение помещает файл на карантин только для термина FileItem. Помещение файла на карантин для других терминов не поддерживается.

- Для работы с деталями алерта требуется веб-плагин Kaspersky Endpoint Security для Windows версии 11.7.0 или выше. Детали алерта нужны при работе с решениями Endpoint Detection and Response (EDR Optimum и EDR Expert). Детали алерта доступны только в Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console.

- Миграция конфигурации [KES+KEA] на [KES+встроенный агент] может завершиться с ошибкой удаления приложения Kaspersky Endpoint Agent. Ошибка удаления приложения исправлена в последней версии Kaspersky Endpoint Agent. Для удаления Kaspersky Endpoint Agent перезагрузите компьютер и создайте задачу удаления приложения.

- Конфигурация [KES+KEA+встроенный агент] не поддерживается. Такая конфигурация нарушает взаимодействие между приложениями и решением Detection and Response, которое развернуто в вашей организации. Также использование Kaspersky Endpoint Agent и встроенного агента на одном компьютере может привести к дублированию телеметрии и повышенной нагрузке на компьютер и сеть. После миграции на конфигурацию [KES+встроенный агент] убедитесь, что приложение Kaspersky Endpoint Agent удалено с компьютера. Если Kaspersky Endpoint Agent продолжает работу после миграции, удалите приложение вручную (например, с помощью задачи *Удаленная деинсталляция приложения*).

  Установщик позволяет развернуть Kaspersky Endpoint Agent на компьютере с Kaspersky Endpoint Security и встроенным агентом. Также Kaspersky Endpoint Agent и встроенный агент могут быть установлены на одном компьютере в результате выполнения задачи *Изменение состава компонентов приложения*. Поведение зависит от версий Kaspersky Endpoint Security и Kaspersky Endpoint Agent.

- При формировании деталей алерта приложение предоставляет данные об обнаруженной угрозе, включая хеши файлов, которые были изменены. Kaspersky Endpoint Security вычисляет хеш файла при формировании деталей алерта. При этом исходный хеш файла при формировании события об изменении файла может отличаться от хеша, вычисленного при формировании деталей алерта.

- Встроенный агент EDR (KATA) возобновляет сетевую изоляцию компьютера после перезагрузки компьютера, даже если период изоляции истек. Для предотвращения повторной изоляции компьютера вам нужно выключить сетевую изоляцию в консоли Kaspersky Anti Targeted Attack Platform.

- Рекомендуется обновлять версию приложения после завершения Сетевой изоляции компьютера. После обновления версии Kaspersky Endpoint Security Сетевая изоляция может быть прекращена.

- Встроенные агенты EDR (KATA), EDR Optimum и EDR Expert несовместимы между собой. Таким образом, активация встроенного агента EDR отдельной лицензией Kaspersky Endpoint Detection and Response Add-on может быть пропущена, если вы активировали Kaspersky Endpoint Security с другой функциональностью EDR. Например, активация встроенного агента EDR (KATA) отдельной лицензией будет пропущена, если вы активировали Kaspersky Endpoint Security с помощью лицензии [KES+EDR Optimum].

- В Kaspersky Endpoint Security версии 12.1 встроенный агент EDR (KATA) для задачи *Получить метафайлы NTFS* не поддерживает следующие метафайлы: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. Поддержка этих метафайлов добавлена в Kaspersky Endpoint Security версии 12.2.

- При миграции с Kaspersky Endpoint Agent на Kaspersky Endpoint Security для решения Kaspersky Anti Targeted Attack Platform (EDR) могут возникнуть ошибки подключения компьютера к серверам Central Node. Это связано с тем, что мастер миграции в Web Console пропускает и не переносит следующие параметры политики:

  - Запрет на изменение параметров **Настройки подключения** ("замок").

    По умолчанию изменение параметров разрешено ("замок" открыт). Поэтому параметры не будут применены на компьютере. Вам нужно запретить изменение параметров и закрыть "замок".

  - Криптоконтейнер.

    Если вы используете двустороннюю аутентификацию для подключения к серверам Central Node, нужно добавить криптоконтейнер повторно. TLS-сертификат сервера мастер миграции переносит корректно.

  Мастер миграции политики и задач в Консоли администрирования (MMC) переносит все параметры для решения Kaspersky Anti Targeted Attack Platform (EDR).

- При установке приложения в режиме Endpoint Detection and Response-агента для работы решения Kaspersky Managed Detection and Response без подключения к Kaspersky Security Center некорректно отображается статус активации приложения. После загрузки BLOB-файла в области уведомлений панели задач Windows отображается некорректный статус *Приложение не активировано*. При этом в интерфейсе приложения статус активации отображается верно. Для корректной работы приложения перезагрузите компьютер.

- Kaspersky Endpoint Security позволяет интегрироваться с решением Kaspersky Anti Targeted Attack Platform с помощью компонентов EDR (KATA) или Endpoint Sensor (не поддерживается). При этом вы можете использовать только один компонент для взаимодействия с Kaspersky Anti Targeted Attack Platform. Для просмотра статуса компонента вы можете открыть свойства компьютера в Консоли администрирования (MMC), в разделе **Приложения** открыть свойства приложения Kaspersky Endpoint Security для Windows и перейти в раздел **Компоненты**. Отображение статуса компонента для взаимодействия с Kaspersky Anti Targeted Attack Platform имеет следующие особенности:

  - Для плагина управления версии 12.0 и ниже приложение показывает текущий статус **Endpoint Sensor**. В Kaspersky Endpoint Security версии 12.0 и ниже компонент EDR (KATA) недоступен. Компонент EDR (KATA) добавлен в версии 12.1.

  - Для плагина управления версии 12.1 и выше приложение показывает общий статус **Endpoint Detection and Response (KATA)**, который может означать как статус Endpoint Sensor, так и статус компонента EDR (KATA). Это зависит от версии приложения, установленного на компьютере пользователя, и доступных компонентов, которые вы можете использовать для взаимодействия с Kaspersky Anti Targeted Attack Platform.

- Начиная с Kaspersky Endpoint Security версии 12.6 и выше в Kaspersky Security Center Web Console версии 14.2 и ниже приложение некорректно показывает название компонента **Endpoint Detection and Response (KATA)** в свойствах компьютера. Вместо компонента **Endpoint Detection and Response (KATA)** приложение показывает название **Endpoint Detection and Response Expert (KATA EDR)**. Для просмотра списка компонентов вы можете открыть свойства компьютера в Web Console, в разделе **Приложения** открыть свойства приложения Kaspersky Endpoint Security для Windows и перейти в раздел **Компоненты**. Начиная с Kaspersky Security Center Web Console версии 15.1 и выше приложение показывает название компонента корректно.

- При обновлении плагина управления Kaspersky Endpoint Detection and Response до версии 15.3, установленного в Web Console версии 14.0-14.2, некорректно отображаются детали алерта. Для корректной работы деталей алерта перезагрузите Сервер администрирования Kaspersky Security Center.

- Плагин управления Kaspersky Endpoint Detection and Response версии 15.4 и выше не поддерживает работу с Kaspersky Security Center версии 14.0. После обновления плагина управления некорректно отображаются детали алерта.

- Решения класса Extended Detection and Response (XDR) от "Лаборатории Касперского" версии 1.4 не поддерживают веб-плагин Kaspersky Endpoint Security для Windows версии 12.12 и выше. Вы можете или оставить текущую версию веб-плагина, или обновить XDR-решение до версии 2.0 или выше.

- Kaspersky Endpoint Security не отправляет в Kaspersky Sandbox объекты, предназначенные для Arm-архитектуры.

- Kaspersky Endpoint Security поддерживает суммарно не более 10 000 включающих и исключающих правил фильтрации событий EDR Expert (on-premises).

- Правила фильтрации событий EDR Expert (on-premises) не будут переданы из политики на управляемые устройства с Kaspersky Endpoint Security версии 14.0 и ниже в случае превышения поддерживаемого объема хранимых правил фильтрации. Приложение отобразит соответствующее предупреждение.

- Kaspersky Endpoint Security для Windows версии 12.11 – 14.1 не поддерживает следующие события телеметрии EDR Expert (on-premises):
  - LDAP Attribute Change;
  - GPO Change;
  - SCCM Local Config Mismatch;
  - SCCM Config Change;
  - SCCM Deployment Task;
  - Smb Connection Open.

  Начиная с версии Kaspersky Endpoint Security для Windows 14.2, приложение поддерживает все эти события телеметрии EDR Expert (on-premises), кроме LDAP Attribute Change.

Другие ограничения

- Операционные системы Windows, начиная с версии 11 24H2, поддерживают технологию UDP Receive Segment Coalescing Offload (URO). Технология включена по умолчанию, если на компьютере установлены совместимая сетевая карта и драйверы. Отключение URO на компьютере пользователя может значительно снизить производительность приложения.
- Kaspersky Endpoint Security поддерживает подсистему WSL (Windows Subsystem for Linux) с ограничениями:
  - WSL 1. Приложение контролирует сетевой трафик и обнаруживает угрозы по протоколам HTTP / HTTPS. Из-за того, что Kaspersky Endpoint Security использует собственный сертификат для проверки защищенных соединений HTTPS, работа некоторых сторонних приложений может быть нарушена.
  - WSL 2. Приложение не поддерживает работу с WSL 2.
- Если во время работы приложения возникают ошибки или зависания, приложение может быть автоматически перезапущено. Если в работе приложения возникают повторяющиеся ошибки, которые приводят к прекращению работы, приложение выполняет следующие действия:
  1. Выключает функции контроля и защиты (функция шифрования продолжает работать).
  2. Уведомляет пользователя о выключении функций.
  3. После обновления антивирусных баз или применения обновлений модулей приложения пытается восстановить работоспособность.
- Возможна некорректная обработка веб-адресов, которые добавлены в доверенный список.
- В консоли Kaspersky Security Center невозможно сохранить файл на диск из папки **Дополнительно** → **Хранилища** → **Активные угрозы**. Для сохранения файла вам нужно вылечить зараженный файл. При лечении приложение сохраняет копию файла в резервное хранилище. Теперь вы можете сохранить файл на диск из папки **Дополнительно** → **Хранилища** → **Резервное хранилище**.

- Наследование параметров передачи данных на Сервер администрирования (**Общие настройки** → **Отчеты и хранилище** → **Передача данных на Сервер администрирования**) отличается от наследования других параметров. Если вы в политике разрешили изменение параметров передачи данных ("замок" открыт), в локальных свойствах компьютера в консоли эти параметры будут сброшены к значениям по умолчанию, если параметры ранее не были заданы. Если параметры ранее уже были заданы, то значения будут восстановлены. Такое же наследование параметров при удалении политики. Другие параметры в локальных свойствах компьютера в этих случаях наследуются из политики.

- Kaspersky Endpoint Security контролирует HTTP-трафик, соответствующий стандартам RFC 2616, RFC 7540, RFC 7541, RFC 7301. Если Kaspersky Endpoint Security обнаруживает другой формат обмена данными в HTTP-трафике, приложение блокирует это соединение для предотвращения загрузки вредоносных файлов из интернета.

- Приложение Kaspersky Endpoint Security препятствует обмену данными по протоколу QUIC. Браузеры используют стандартный транспортный протокол (TLS или SSL) независимо от того, включена в браузере поддержка протокола QUIC или нет.

- При работе стороннего ПО с библиотекой Libcurl могут возникать ошибки TLS-соединения. Это может быть связано с сертификатом "Лаборатории Касперского", который Kaspersky Endpoint Security использует для проверки защищенных соединений. Для продолжения работы вы можете выключить проверку сертификата для стороннего ПО (не рекомендуется) или добавить тело сертификата "Лаборатории Касперского" в хранилище сертификатов cURL. Подробнее см. в Базе знаний "Лаборатории Касперского".

- При первом запуске Kaspersky Endpoint Security для Windows возможно временное попадание в некорректную группу приложения, которое подписано цифровой подписью. В дальнейшем группа для приложения, которое подписано цифровой подписью, будет автоматически изменена на корректную.

- При повторном сканировании вредоносного объекта, который заблокирован сторонним программным обеспечением, пользователь не информируется о повторном обнаружении угрозы. Событие о повторном обнаружении угрозы отображается в отчете приложения и отчете в Kaspersky Security Center.

- В отчет Kaspersky Security Center о шифровании устройств не будет представлена информация об устройствах, которые зашифрованы с помощью Microsoft BitLocker на серверных платформах или на рабочих станциях, на которых не установлен компонент Контроль устройств.

- Невозможно включить отображение всех записей в отчетах в Kaspersky Security Center Web Console. В Web Console вы можете только изменить количество отображаемых в отчете записей. По умолчанию Kaspersky Security Center Web Console показывает 1000 записей в отчете. Вы можете включить отображение всех записей в отчете в Консоли администрирования (MMC).

- Невозможно установить отображение более 1000 записей в отчетах в консоли Kaspersky Security Center. Если вы установили максимальное число отображаемых записей больше 1000, консоль Kaspersky Security Center будет показывать только 1000 записей в отчете.

- При использовании иерархии политик настройки раздела Шифрования съемных дисков в дочерней политике отображаются доступными для редактирования, если в родительской политике их изменение запрещено.

- Для работы исключений при защите папок общего доступа от внешнего шифрования в параметрах операционной системы необходимо включить аудит входа в систему.

- Если включена защита папок общего доступа, Kaspersky Endpoint Security для Windows отслеживает попытки шифрования папок общего доступа для каждой сессии удаленного доступа, которая была запущена до момента запуска Kaspersky Endpoint Security для Windows, в том числе если компьютер, с которого была запущена сессия удаленного доступа, добавлен в исключения. Чтобы Kaspersky Endpoint Security для Windows не отслеживал попытки шифрования папок общего доступа для сессий удаленного доступа, которые запущены с добавленного в исключения компьютера и были запущены до момента запуска Kaspersky Endpoint Security для Windows, прервите и повторно установите эту сессию удаленного доступа или перезагрузить компьютер, на котором установлен Kaspersky Endpoint Security для Windows.

- Если задача обновления запускается с правами конкретной учетной записи при обновлении с источника, который требует авторизацию, продуктовые патчи не будут скачаны.

- Приложение может не запуститься из-за недостаточной производительности системы. Для решения этой проблемы используйте опцию Ready Boot или увеличьте таймаут операционной системы на запуск служб.

- Не поддерживается работа приложения в Безопасном режиме Windows (Safe Mode).

- Мы не гарантируем работу контроля аудио до первой перезагрузки после установки приложения.

- В Консоли администрирования (MMC) в параметрах Предотвращения вторжений в окне настройки прав приложений недоступна кнопка **Удалить**. Вы можете удалить приложение из группы доверия через контекстное меню приложения.

- В локальном интерфейсе приложения в параметрах Предотвращения вторжений недоступны для просмотра права приложений и защищаемыми ресурсами, если компьютер находится под управлением политики. Недоступны прокрутка, поиск, фильтр и другие элементы управления в окнах. Вы можете просмотреть права приложений в свойствах политики в консоли Kaspersky Security Center.

- При включении записи файлов трассировок с ротацией не создаются трассировки для компонента AMSI и Outlook-плагина.

- Не поддерживается ручной сбор трассировок производительности на операционной системе Window Server 2008.

- Не поддерживается запись трассировок производительности для типа трассировок При перезагрузке.

- Не поддерживается запись дампов для pico-процессов.

- Отключение опции **Выключить возможность внешнего управления системными службами** не будет позволять остановить службу приложения, установленной с параметром `AMPPL=1` (по умолчанию значение параметра выставлено `1` начиная с версии операционной системы Windows 10RS2). Параметр `AMPPL` со значением `1` включает использование технологии Protection Processes для продуктовой службы.

- Для запуска выборочной проверки каталога необходимо, чтобы у пользователя, который выполняет выборочное сканирование, были права на чтение атрибутов этого каталога, иначе сканирование выбранной папки невозможно и будет завершено с ошибкой.

- При задании в политике правила сканирования с указанием пути без символа `\` в конце, например, `C:\folder1\folder2`, сканирование будет выполнено для `C:\folder1\`.

- Если вы используете политики ограниченного использования приложений (англ. Software Restriction Policies, SRP), возможен сбой при загрузке компьютера (черный экран). Чтобы не допустить сбоев, вам нужно разрешить использование библиотек приложения в параметрах SRP. В параметрах SRP добавьте правило с уровнем безопасности **Неограниченный** для файла khkum.dll (пункт **Создать правило для хеша**). Файл расположен в папке `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.3\klhk\klhk_x64\`. Если вы выбрали этот способ, дополнительно в параметрах задачи *Обновление* для Kaspersky Endpoint Security вам нужно снять флажки **Загружать обновления модулей приложения**. Подробнее об использовании SRP см. в документации Microsoft.

  Также вы можете выключить SRP и использовать для контроля использования приложений Kaspersky Endpoint Security – компонент Контроль приложений.

- Если компьютер находится в домене под управлением групповой политики Windows (англ. Group Policy Object, GPO), в параметрах которой для параметра DriverLoadPolicy установлено значение 8 (Good only), перезагрузка компьютера с установленным Kaspersky Endpoint Security вызывает сбой (BSOD). Для предотвращения сбоя в групповой политике в параметрах раннего запуска защиты от вредоносного ПО (англ. Early Launch Antimalware, ELAM) должно быть установлено значение 1 (Good and unknown). Параметры ELAM расположены в политике в папке: **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.

- Не поддерживается управление настройками Outlook-плагина через Rest API.

- Не поддерживается перенос настроек запуска задачи под указанным пользователем между устройствами через файл конфигурации. После применения настроек из файла конфигурации вручную задайте имя пользователя и пароль.

- После установки обновления и до перезагрузки для его применения не поддерживается работа задачи проверки целостности.

- При изменении уровня трассировки с ротацией через утилиту удаленной диагностики в Kaspersky Endpoint Security для Windows некорректно отображается уровень трассировки: будет отображаться пустое значение. При этом файлы трассировки записываются с корректным уровнем. При изменении уровня трассировки с ротацией через локальный интерфейс приложения уровень трассировок корректно изменяется, но в утилите удаленной диагностики некорректно отображается уровень трассировки: отображается последний заданный утилитой уровень трассировки. Это может привести к тому, что администратор не будет владеть актуальной информацией о текущем уровне трассировки и необходимая информация может быть не записана, если пользователь вручную изменит уровень трассировки в локальном интерфейсе приложения.

- В локальном интерфейсе приложения в настройках Защиты паролем невозможно изменить имя учетной записи администратора (по умолчанию, KLAdmin). Для изменения имени учетной записи администратора вам нужно выключить Защиту паролем, далее включить Защиту паролем и задать новое имя учетной записи администратора.

- Приложение Kaspersky Endpoint Security, установленное на сервер под управлением Windows Server 2019, несовместимо с программным обеспечением Docker. Развертывание контейнеров Docker на компьютере с Kaspersky Endpoint Security вызывает сбой (BSOD).

- Если приложение Kaspersky Endpoint Security установлено на сервер СУБД SQL Server, приложение отправляет запросы к экземпляру сервера. Это нужно для проверки заданий Агента SQL Server и предотвращения выполнения вредоносных заданий. Kaspersky Endpoint Security проверяет задания под учетной записью SQL Server. Приложение отправляет запросы к серверу при проверке системной памяти, а также после обновления антивирусных баз.

- Совместимость приложения Kaspersky Endpoint Security и программного обеспечения Secret Net Studio имеет следующие ограничения:

  - Приложение Kaspersky Endpoint Security несовместимо с компонентом Антивирус программного обеспечения Secret Net Studio.

    Невозможно установить приложение на компьютер, на котором развернуто программное обеспечение Secret Net Studio с компонентом Антивирус. Для совместной работы приложений вам нужно удалить компонент Антивирус из состава Secret Net Studio.

  - Приложение Kaspersky Endpoint Security несовместимо с компонентом Защита дисков и шифрование данных программного обеспечения Secret Net Studio.

    Невозможно установить приложение на компьютер, на котором развернуто программное обеспечение Secret Net Studio с компонентом Защита дисков и шифрование данных. Для совместной работы приложений вам нужно удалить компонент Защита дисков и шифрование данных из состава Secret Net Studio.

  - Программное обеспечение Secret Net Studio несовместимо с компонентом Шифрование файлов (FLE) приложения Kaspersky Endpoint Security.

    При установке Kaspersky Endpoint Security с компонентом Шифрование файлов (FLE) возможны сбои в работе Secret Net Studio. Для совместной работы приложений вам нужно удалить компонент Шифрование файлов (FLE) из состава Kaspersky Endpoint Security.

- При импорте правил Контроля целостности системы приложение проверяет идентификатор и название правила. Если идентификаторы правил совпадают, Kaspersky Endpoint Security заменяет существующие правило новым. Приложение присваивает идентификатор при экспорте правил автоматически. Идентификаторы правил могут совпадать, если вы, например, вручную редактировали экспортируемые XML-файлы правил. Если идентификаторы правил уникальны, но названия правил совпадают, Kaspersky Endpoint Security добавит к названию правила `(1)` и так далее.

- Начиная с версии Kaspersky Endpoint Security для Windows 12.11 в Web Console невозможно просмотреть параметры родительской политики, открытой в дочерней группе. Также Web Console показывает предупреждение *Эта политика унаследована. Вы можете изменить параметры политики только в группе администрирования, в которой она была создана*.

- В Консоли администрирования (MMC) не отображаются всплывающие подсказки длиной более 256 символов.

- Названия компонентов в политике и инсталляционном пакете могут отличаться. Например, компонент Endpoint Detection and Response Expert (on-premises) может иметь названия Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises), Интеграция с Kaspersky Anti Targeted Attack Platform. Также названия компонентов могут отличаться в зависимости от версии приложения.

Глоссарий

Cloud discovery

Cloud Discovery управляет доступом пользователей к облачным сервисам. К облачным сервисам относятся, например, Microsoft Teams, Salesforce, Microsoft Office 365. Облачные сервисы сгруппированы в категории, например, категории *Файловые обменники*, *Мессенджеры*, *Электронная почта*.

IOC

Indicator of Compromise (индикатор компрометации). Набор данных о вредоносном объекте или действии.

IOC-файл

Файл, содержащий набор индикаторов IOC, при совпадении с которыми приложение считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

Kerberos-аутентификация

Механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, позволяющий передавать данные через незащищенные сети. Механизм основан на использовании билета (ticket), который выдается пользователю доверенным центром аутентификации.

OLE-объект

Файл, присоединенный или встроенный в другой файл. Приложения "Лаборатории Касперского" позволяют проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel® в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

OpenIOC

Открытый стандарт описания индикаторов компрометации (Indicator of Compromise, IOC), созданный на базе XML и содержащий свыше 500 различных индикаторов компрометации.

SVM

Secure virtual machine – специальная виртуальная машина, на которой установлена служба scanserver (Сервер защиты, компонент Kaspersky Endpoint Security для виртуальных сред Легкий агент).

Агент администрирования

Компонент приложения Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и приложениями "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех приложений "Лаборатории Касперского", работающих в операционной системе Windows. Для приложений, работающих в других операционных системах, предназначены отдельные версии Агента администрирования.

Агент аутентификации

Интерфейс, позволяющий после шифрования загрузочного жесткого диска пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы.

Активный ключ

Ключ, используемый в текущий момент для работы приложения.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

Архив

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

База вредоносных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как опасное. Список сформирован специалистами "Лаборатории Касперского", регулярно обновляется и входит в поставку приложения "Лаборатории Касперского".

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами "Лаборатории Касперского" как фишинговые. База регулярно обновляется и входит в поставку приложения "Лаборатории Касперского".

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором приложений "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждого из установленных в группе приложений могут быть созданы групповые политики и сформированы групповые задачи.

Доверенный платформенный модуль

Микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины.

Задача

Функции, выполняемые приложением "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Зараженный файл

Файл, внутри которого содержится вредоносный код (при проверке файла был обнаружен код известной программы, представляющей угрозу). Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими файлами, поскольку это может привести к заражению вашего компьютера.

Издатель сертификата

Центр сертификации, выдавший сертификат.

Легкий агент

Компонент Kaspersky Endpoint Security для виртуальных сред Легкий агент. Устанавливается на каждую виртуальную машину, которую требуется защищать.

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации "Лаборатория Касперского". Документ содержит информацию о предоставляемой лицензии.

Ложное срабатывание

Ситуация, когда незараженный файл определяется приложением "Лаборатории Касперского" как зараженный ввиду того, что его код напоминает код вируса.

Маска

Представление названия и расширения файла общими символами.

Для формирования маски файла можно использовать любые символы, допустимые в названиях файлов, в том числе специальные:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает. Маска ** доступна только для создания исключений из проверки.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Нормализованная форма адреса веб-ресурса

Нормализованной формой адреса веб-ресурса называется текстовое представление адреса веб-ресурса, полученное в результате применения нормализации. *Нормализация* – процесс, в результате которого текстовое представление адреса веб-ресурса изменяется в соответствии с определенными правилами (например, исключение из текстового представления адреса веб-ресурса имени пользователя, пароля и порта соединения, понижение верхнего регистра символов адреса веб-ресурса до нижнего регистра).

В контексте работы компонентов защиты цель нормализации адресов веб-ресурсов заключается в том, чтобы проверять синтаксически различные, но физически эквивалентные адреса веб-ресурсов один раз.

Пример:

Ненормализованная форма адреса: www.Example.com\.

Нормализованная форма адреса: www.example.com.

Область защиты

Объекты, которые компонент базовой защиты постоянно проверяет во время своей работы. Область защиты разных компонентов имеет разные свойства.

Область проверки

Объекты, которые Kaspersky Endpoint Security проверяет во время выполнения задачи проверки.

Портативный файловый менеджер

Приложение, предоставляющая интерфейс для работы с зашифрованными файлами на съемных дисках при недоступности функциональности шифрования на компьютере.

Потенциально заражаемый файл

Файл, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например, с расширением com, exe, dll и др. Риск внедрения в такие файлы вредоносного кода достаточно высок.

Сервер интеграции

Компонент Kaspersky Endpoint Security для виртуальных сред Легкий агент. Осуществляет взаимодействие между компонентами Kaspersky Endpoint Security и виртуальной инфраструктурой.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Приложение 1. Параметры приложения

Вы можете настроить параметры Kaspersky Endpoint Security с помощью политики, задач или интерфейса приложения. Подробная информация о компонентах приложения приведена в соответствующих подразделах.

Защита от файловых угроз

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. По умолчанию компонент Защита от файловых угроз постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы в режиме реального времени. Компонент проверяет файлы на всех дисках компьютера, а также на подключенных дисках. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Компонент проверяет файлы, к которым обращается пользователь или приложение. При обнаружении вредоносного файла Kaspersky Endpoint Security блокирует операцию с файлом. Далее приложение лечит или удаляет вредоносный файл, в зависимости от настройки компонента Защита от файловых угроз.

При обращении к файлу, содержимое которого расположено в облачном хранилище OneDrive, Kaspersky Endpoint Security загружает и проверяет содержимое этого файла.

Параметры компонента Защита от файловых угроз

Параметр	Описание
Уровень безопасности *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Для работы Защиты от файловых угроз приложение Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Высокий**. Уровень безопасности файлов, при котором компонент Защита от файловых угроз максимально контролирует все открываемые, сохраняемые и запускаемые файлы. Компонент Защита от файловых угроз проверяет все типы файлов на всех жестких, сменных и сетевых дисках компьютера, а также архивы, установочные пакеты и вложенные OLE-объекты. • **Рекомендуемый**. Уровень безопасности файлов, который рекомендован для использования специалистами "Лаборатории Касперского". Компонент Защита от файловых угроз проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты, компонент Защита от файловых угроз не проверяет архивы и установочные пакеты. • **Низкий**. Уровень безопасности файлов, параметры которого обеспечивают максимальную скорость проверки. Компонент Защита от файловых угроз проверяет только файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера, компонент Защита от файловых угроз не проверяет составные файлы.
Типы файлов *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	**Все файлы**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений). **Файлы, проверяемые по формату**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла. **Файлы, проверяемые по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.

Параметр	Описание
Область проверки	Содержит объекты, которые проверяет компонент Защита от файловых угроз. Объектом проверки может быть жесткий, съемный или сетевой диск, папка, файл или несколько файлов, определенных по маске. По умолчанию компонент Защита от файловых угроз проверяет файлы, запускаемые со всех жестких, съемных и сетевых дисков. Область защиты этих объектов невозможно изменить или удалить. Вы можете только исключить объект (например, съемные диски) из проверки.
Машинное обучение и сигнатурный анализ *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	При методе проверки Машинное обучение и сигнатурный анализ используются базы Kaspersky Endpoint Security, содержащие описания известных угроз и методы их устранения. Защиту с использованием этого метода проверки обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.
Эвристический анализ *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл. **Лечить. Блокировать, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение блокирует этот файл. **Блокировать**. Если выбран этот вариант действия, то приложение автоматически блокирует зараженный файл без попытки вылечить и удалить. Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.
Проверять только новые и измененные файлы	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	Проверка дистрибутивов сторонних приложений.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Проверять файлы почтовых форматов	Проверка файлов почтовых форматов. Приложение проверяет MSG- и EML-файлы. К файлам почтовых форматов также относятся OLE-объекты и MHT-файлы. Kaspersky Endpoint Security проверяет файлы почтовых форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Не распаковывать составные файлы большого размера	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.

Параметр	Описание
Распаковывать составные файлы в фоновом режиме	Если флажок установлен, приложение предоставляет доступ к составным файлам, размер которых превышает заданное значение, до проверки этих файлов. При этом приложение Kaspersky Endpoint Security в фоновом режиме распаковывает и проверяет составные файлы. Приложение предоставляет доступ к составным файлам, размер которых меньше данного значения, только после распаковки и проверки этих файлов. Если флажок снят, приложение предоставляет доступ к составным файлам только после распаковки и проверки файлов любого размера.
Режим проверки *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Kaspersky Endpoint Security проверяет файлы, с которыми работает пользователь, операционная система или приложение от имени пользователя. **Интеллектуальный**. Режим проверки, при котором Защита от файловых угроз проверяет объект на основании анализа операций, выполняемых над объектом. Например, при работе с документом Microsoft Office приложение Kaspersky Endpoint Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются. **При доступе и изменении**. Режим проверки, при котором Защита от файловых угроз проверяет объекты при попытке их открыть или изменить. **При доступе**. Режим проверки, при котором Защита от файловых угроз проверяет объекты только при попытке их открыть. **При выполнении**. Режим проверки, при котором Защита от файловых угроз проверяет объекты только при попытке их запустить.
Использовать технологию iSwift *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
Использовать технологию iChecker *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз приложения Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Приостановка Защиты от файловых угроз *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Временная автоматическая приостановка работы Защиты от файловых угроз в указанное время или во время работы с указанными приложениями.
Проверка файловых операций, исполняемых в контейнерах Windows	При обнаружении угрозы внутри контейнера, приложение применяет действие, выбранное для компонента Защита от файловых угроз. **Останавливать контейнер, если лечение невозможно**. У приложения может не быть прав на чтение и запись обнаруженного объекта. В этом случае вылечить или удалить обнаруженный объект невозможно. Если флажок установлен, приложение блокирует обнаруженный объект и останавливает контейнер. Если флажок снят, приложение только блокирует обнаруженный объект. **Не проверять файловые операции, исполняемые в контейнерах Windows**. Если флажок установлен, приложение проверяет контейнер только при запуске контейнера. Если флажок снят, приложение проверяет контейнер постоянно в режиме реального времени.

Защита от веб-угроз

Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует соединение с вредоносными и фишинговыми веб-сайтами. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Kaspersky Endpoint Security проверяет HTTP-, HTTPS- и FTP-трафик. Kaspersky Endpoint Security проверяет URL- и IP-адреса.

Для работы Защиты от веб-угроз необходимо выполнить первоначальную настройку приложения:

- Для контроля HTTPS-трафика включите проверку защищенных соединений (по умолчанию проверка включена).
- Выберите порты, которые Kaspersky Endpoint Security будет контролировать (по умолчанию приложение контролирует все порты).
- Выберите приложения, трафик которых будет контролировать Kaspersky Endpoint Security. Основные браузеры уже добавлены в список, рекомендованный "Лабораторией Касперского". Если вашего браузера нет в списке, добавьте приложение вручную.
- Рекомендуется внедрить в трафик скрипт для взаимодействия с веб-страницами (по умолчанию внедрение скрипта выключено). Скрипт позволяет регистрировать события работы Защиты от веб-угроз для журнала событий приложения, журнала событий ОС, отчетов.

При попытке пользователя открыть вредоносный или фишинговый веб-сайт, Kaspersky Endpoint Security заблокирует доступ и покажет предупреждение.

Параметры компонента Защита от веб-угроз

Параметр	Описание
Уровень безопасности *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Для работы Защиты от веб-угроз приложение применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Высокий**. Уровень безопасности веб-трафика, при котором компонент Защита от веб-угроз максимально проверяет веб-трафик, поступающий на компьютер по HTTP- и FTP-протоколам. Защита от веб-угроз детально проверяет все объекты веб-трафика, используя полный набор баз приложения, а также выполняет максимально глубокий эвристический анализ. • **Рекомендуемый**. Уровень безопасности веб-трафика, обеспечивающий оптимальный баланс между производительностью приложения и безопасностью веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на среднем уровне. Этот уровень безопасности веб-трафика рекомендован для использования специалистами "Лаборатории Касперского". • **Низкий**. Уровень безопасности веб-трафика, параметры которого обеспечивают максимальную скорость проверки веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на поверхностном уровне.
Действие при обнаружении угрозы	**Блокировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере. **Информировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта Kaspersky Endpoint Security разрешает загрузку этого объекта на компьютер и добавляет информацию о зараженном объекте в список активных угроз.
Проверять веб-адрес по базе вредоносных веб-адресов *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Проверка ссылок на принадлежность к базе вредоносных веб-адресов позволяет отследить веб-сайты, которые находятся в списке запрещенных веб-адресов. База вредоносных веб-адресов формируется специалистами "Лаборатории Касперского", входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security.
Использовать эвристический анализ *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки веб-трафика на наличие вирусов и других приложений, представляющих угрозу, эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

Параметр	Описание
Проверять веб-адрес по базе фишинговых веб-адресов *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	В состав базы фишинговых веб-адресов включены веб-адреса известных на настоящее время веб-сайтов, которые используются для фишинг-атак. Базу фишинговых веб-адресов специалисты "Лаборатории Касперского" пополняют веб-адресами, предоставленными международной организацией по борьбе с фишингом The Anti-Phishing Working Group. База фишинговых веб-адресов входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security.
Не проверять веб-трафик с доверенных веб-адресов	Если флажок установлен, компонент Защита от веб-угроз не проверяет содержимое веб-страниц / веб-сайтов, адреса которых включены в список доверенных веб-адресов. Вы можете добавить в список доверенных веб-адресов как конкретный адрес веб-страницы / веб-сайта, так и маску адреса веб-страницы / веб-сайта. Вы также можете сформировать общий список исключений защищенных соединений. В этом случае Kaspersky Endpoint Security не будет проверять HTTPS-трафик доверенных веб-адресов при работе компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль.

Защита от почтовых угроз

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других приложений, представляющих угрозу. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Защита от почтовых угроз может проверять и получаемые, и отправляемые сообщения. Приложение поддерживает протоколы POP3, SMTP, IMAP, NNTP в следующих почтовых клиентах:

- Microsoft Office Outlook;
- Mozilla Thunderbird;
- Windows Mail;
- МойОфис Почта;
- Органайзер Р7-Офис.

Для проверки защищенного трафика в почтовых клиентах Mozilla Thunderbird, МойОфис Почта и Органайзер Р7-Офис вам нужно включить использование хранилища сертификатов Windows для приложений на основе технологий Mozilla.

Другие протоколы и почтовые клиенты Защита от почтовых угроз не поддерживает.

Защита от почтовых угроз не всегда может получить доступ к сообщениям на *уровне протокола* (например, при использовании решения Microsoft Exchange). Поэтому дополнительно в состав Защиты от почтовых угроз включено расширение для Microsoft Office Outlook. Расширение позволяет проверять сообщения на *уровне почтового клиента*. Расширение компонента Защита от почтовых угроз поддерживает работу с 32- и 64-разрядными версиями Outlook 2010, 2013, 2016, 2019, 2021, 2024, 365. На компьютерах с архитектурой Arm расширение компонента Защита от почтовых угроз поддерживает работу с 32- и 64-разрядной версией Outlook 2016 и Outlook 2021, 2024, 365 для Arm64.

Компонент Защита от почтовых угроз не проверяет сообщения, если почтовый клиент открыт в браузере.

При обнаружении вредоносного файла во вложении Kaspersky Endpoint Security добавляет информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

Параметры компонента Защита от почтовых угроз

Параметр	Описание
Уровень безопасности *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Для работы Защиты от почтовых угроз приложение применяет разные наборы настроек. Наборы настроек, сохраненные в приложении, называются *уровнями безопасности*. • **Высокий**. Уровень безопасности почты, при котором компонент Защита от почтовых угроз максимально контролирует сообщения. Компонент Защита от почтовых угроз проверяет входящие и исходящие сообщения электронной почты, а также выполняет глубокий эвристический анализ. Высокий уровень безопасности почты рекомендуется применять для работы в опасной среде. Примером опасной среды может служить подключение к одному из бесплатных почтовых сервисов из домашней сети, не обеспечивающей централизованной защиты почты. • **Рекомендуемый**. Уровень безопасности почты, обеспечивающий оптимальный баланс между производительностью приложения и безопасностью почты. Компонент Защита от почтовых угроз проверяет входящие и исходящие сообщения электронной почты, а также выполняет эвристический анализ среднего уровня. Этот уровень безопасности почты рекомендован для использования специалистами "Лаборатории Касперского". • **Низкий**. Уровень безопасности почты, при котором компонент Защита от почтовых угроз проверяет только входящие сообщения электронной почты, а также выполняет поверхностный эвристический анализ и не проверяет архивы, вложенные в сообщения. Если используется этот уровень безопасности почты, компонент Защита от почтовых угроз проверяет сообщения электронной почты максимально быстро и затрачивает минимум ресурсов операционной системы. Низкий уровень безопасности почты рекомендуется применять для работы в хорошо защищенной среде. Примером такой среды может служить локальная сеть организации с централизованным обеспечением безопасности почты.
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*. **Лечить. Блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение пытается вылечить обнаруженный объект. Если вылечить объект не удалось, приложение блокирует отправку сообщения, почтовый клиент показывает ошибку. **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.
Область защиты *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	*Область защиты* – это объекты, которые проверяет компонент во время своей работы: входящие и исходящие сообщения или только входящие сообщения. Для защиты компьютеров достаточно проверять только входящие сообщения. Вы можете включить проверку исходящих сообщений для предотвращения отправки зараженных файлов в архивах. Вы также можете включить проверку исходящих сообщений, если вы хотите запретить обмен файлами определенных форматов, например, аудио или видео.
Проверять трафик POP3, SMTP, NNTP, IMAP	Проверка компонентом Защита от почтовых угроз почтового трафика, проходящего по протоколам POP3, SMTP, NNTP и IMAP.
Подключить расширение для Microsoft Outlook	Если флажок установлен, включена проверка сообщений электронной почты, передающихся по протоколам POP3, SMTP, NNTP, IMAP на стороне расширения, интегрированного в Microsoft Outlook. В случае проверки почты с помощью расширения для Microsoft Outlook рекомендуется использовать режим кеширования Exchange (Cached Exchange Mode). Более подробную информацию о режиме кеширования Exchange и рекомендации по его использованию вы можете найти в базе знаний Microsoft.
Эвристический анализ *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз приложений "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

Параметр	Описание
Проверять вложенные архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива). Если во время проверки приложение обнаружило в тексте сообщения пароль к архиву, пароль будет использован для проверки содержания этого архива на наличие вредоносных приложений. Пароль при этом не сохраняется. При проверке архива выполняется его распаковка. Если во время распаковки архива произошел сбой в работе приложения, вы можете вручную удалить файлы, которые при распаковке сохраняются по следующему пути: %systemroot%\temp. Файлы имеют префикс PR.
Проверять вложенные файлы форматов Microsoft Office	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Не проверять архивы размером более N МБ	Если флажок установлен, компонент Защита от почтовых угроз исключает из проверки вложенные в сообщения электронной почты архивы, размер которых больше заданного. Если флажок снят, компонент Защита от почтовых угроз проверяет архивы любого размера, вложенные в сообщения электронной почты.
Ограничить время проверки архива до N с	Если флажок установлен, то время проверки архивов, вложенных в сообщения электронной почты, ограничено указанным периодом.
Фильтр вложений	Фильтр вложений не работает для исходящих сообщений электронной почты. **Не применять фильтр**. Если выбран этот вариант, компонент Защита от почтовых угроз не фильтрует файлы, вложенные в сообщения электронной почты. **Переименовывать вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_). Таким образом, чтобы открыть файл, пользователю нужно переименовать файл. **Удалять вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз удаляет из сообщений электронной почты вложенные файлы указанных типов. Типы вложенных файлов, которые нужно переименовывать или удалять из сообщений электронной почты, вы можете указать в списке масок файлов.

Защита от сетевых угроз

Компонент *Защита от сетевых угроз* (также Intrusion Detection System (IDS) – система обнаружения вторжений) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, приложение блокирует сетевое соединение с атакующим компьютером. Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах приложения. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей приложения.

Параметр	Описание
Считать атаками сканирование портов и интенсивные сетевые запросы	*Атака типа Интенсивные сетевые запросы (англ. Network Flooding)* – атака на сетевые ресурсы организации (например, веб-серверы). Атака заключается в отправке большого количества запросов для превышения пропускной способности сетевых ресурсов. Таким образом, пользователи не могут получить доступ к сетевым ресурсам организации. *Атака типа Сканирование портов* заключается в сканировании UDP- и TCP-портов, а также сетевых служб на компьютере. Атака позволяет определить степень уязвимости компьютера перед более опасными видами сетевых атак. Сканирование портов также позволяет злоумышленнику определить операционную систему на компьютере и выбрать подходящие для нее сетевые атаки. Если функция включена, Kaspersky Endpoint Security проверяет сетевой трафик на наличие признаков сканирования портов и интенсивных сетевых запросов. При обнаружении атак данных типов приложение блокирует сетевое соединение с атакующим компьютером, уведомляет об атаке пользователя и отправляет соответствующее событие в Kaspersky Security Center. Также при обнаружении атак типа *Интенсивные сетевые запросы* приложение добавляет атакующий компьютер в список блокирования. Вы можете выключить обнаружение этих типов атак, так как некоторые разрешенные приложения выполняют действия, характерные для таких атак. Таким образом, вы можете избежать ложных срабатываний.
Блокировать атакующие устройства на N мин	Если функция включена, компонент Защита от сетевых угроз добавляет атакующий компьютер в список блокирования. Это означает, что компонент Защита от сетевых угроз блокирует сетевое соединение с атакующим компьютером после первой попытки сетевой атаки в течение заданного времени, чтобы автоматически защитить компьютер пользователя от возможных будущих сетевых атак с этого адреса. Минимальное время, на которое атакующий компьютер можно добавить в список блокирования, составляет одну минуту. Максимальное – 999 минут. Вы можете посмотреть список блокирования в окне инструмента Мониторинг сети. Kaspersky Endpoint Security очищает список блокирования при перезапуске приложения и при изменении параметров Защиты от сетевых угроз.
Исключения	Список содержит IP-адреса, сетевые атаки с которых компонент Защита от сетевых угроз не блокирует. Вы можете добавить IP-адрес с указанием используемого порта и протокола. Приложение не заносит в отчет информацию о сетевых атаках с IP-адресов, входящих в список исключений.
Защита от MAC-спуфинга	*Атака типа MAC-спуфинг* заключается в изменении MAC-адреса сетевого устройства (сетевой карты). В результате злоумышленник может перенаправить данные, отправленные на устройство, на другое устройство и получить доступ к этим данным. Kaspersky Endpoint Security позволяет блокировать атаки MAC-спуфинга и получать уведомления об атаках.

Сетевой экран

Сетевой экран блокирует несанкционированные подключения к компьютеру во время работы в интернете или локальной сети. Также Сетевой экран контролирует сетевую активность приложений на компьютере. Это позволяет защитить локальную сеть организации от кражи персональных данных и других атак. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и предустановленных *сетевых правил*.

Для взаимодействия с Kaspersky Security Center приложение использует Агент администрирования. При этом Сетевой экран автоматически создает сетевые правила, необходимые для работы Агента администрирования и приложения. В результате Сетевой экран открывает некоторые порты на компьютере. Набор портов отличается в зависимости от роли компьютера (например, точка распространения). Подробнее о портах, которые будут открыты на компьютере, см. в справке Kaspersky Security Center.

Сетевые правила

Вы можете настроить сетевые правила на следующих уровнях:

- *Сетевые пакетные правила*. Используются для ввода ограничений на сетевые пакеты независимо от приложения. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных. Kaspersky Endpoint Security имеет предустановленные сетевые пакетные правила с разрешениями, рекомендованными специалистами "Лаборатории Касперского".

- *Сетевые правила приложений*. Используются для ограничения сетевой активности конкретного приложения. Учитываются не только характеристики сетевого пакета, но и конкретное приложение, которому адресован этот сетевой пакет, либо которое инициировало отправку этого сетевого пакета.

Контроль доступа приложений к ресурсам операционной системы, процессам и персональным данным обеспечивает компонент Предотвращение вторжений с помощью *прав приложений*.

Во время первого запуска приложения Сетевой экран выполняет следующие действия:

1. Проверяет безопасность приложения с помощью загруженных антивирусных баз.

2. Проверяет безопасность приложения в Kaspersky Security Network.

   Для более эффективной работы Сетевого экрана вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает приложение в одну из групп доверия: *Доверенные*, *Слабые ограничения*, *Сильные ограничения*, *Недоверенные*.

   Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля активности приложений. Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от уровня опасности, которую это приложение может представлять для компьютера.

   Kaspersky Endpoint Security помещает приложение в группу доверия для компонентов Сетевой экран и Предотвращение вторжений. Изменить группу доверия только для Сетевого экрана или только для Предотвращения вторжений невозможно.

   Если вы отказались принимать участие в KSN или отсутствует сеть, Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации приложения от KSN группа доверия может быть изменена автоматически.

4. Блокирует сетевую активность приложения в зависимости от группы доверия. Например, приложениям из группы доверия *Сильные ограничения* запрещены любые сетевые соединения.

При следующем запуске приложения Kaspersky Endpoint Security проверяет целостность приложения. Если приложение не было изменено, компонент применяет к нему текущие сетевые правила. Если приложение было изменено, Kaspersky Endpoint Security исследует приложение как при первом запуске.

Приоритеты сетевых правил

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если сетевая активность добавлена в несколько правил, Сетевой экран регулирует сетевую активность по правилу с высшим приоритетом.

Сетевые пакетные правила имеют более высокий приоритет, чем сетевые правила приложений. Если для одного и того же вида сетевой активности заданы и сетевые пакетные правила, и сетевые правила приложений, то эта сетевая активность обрабатывается по сетевым пакетным правилам.

Сетевые правила приложений имеют особенность. Сетевое правило приложений включает в себя правила доступа по статусу сети: *Публичная сеть*, *Локальная сеть*, *Доверенная сеть*. Например, для группы доверия *Сильные ограничения* по умолчанию запрещена любая сетевая активность приложения в сетях всех статусов. Если для отдельного приложения (родительское приложение) задано сетевое правило, то дочерние процессы других приложений будут выполнены в соответствии с сетевым правилом родительского приложения. Если сетевое правило для приложения отсутствует, дочерние процессы будут выполнены в соответствии с правилом доступа к сетям группы доверия.

Например, вы запретили любую сетевую активность всех приложений для сетей всех статусов, кроме браузера X. Если в браузере X (родительское приложение) запустить установку браузера Y (дочерний процесс), то установщик браузера Y получит доступ к сети и загрузит необходимые файлы. После установки браузеру Y будут запрещены любые сетевые соединения в соответствии с параметрами Сетевого экрана. Чтобы запретить установщику браузера Y сетевую активность в качестве дочернего процесса, необходимо добавить сетевое правило для установщика браузера Y.

Типы сетевых соединений

Сетевой экран позволяет контролировать сетевую активность в зависимости от типа сетевого соединения. Kaspersky Endpoint Security получает тип сетевого соединения от операционной системы компьютера. Тип сетевого соединения в операционной системе задает пользователь при настройке подключения. Вы можете изменить тип сетевого соединения в параметрах Kaspersky Endpoint Security. Сетевой экран будет контролировать сетевую активность в зависимости от типа сети в параметрах Kaspersky Endpoint Security, а не операционной системы.

Выделены следующие типы сетевого соединения:

- **Публичная сеть**. Сеть не защищена антивирусными приложениями, сетевыми экранами, фильтрами (например, Wi-Fi в кафе). Пользователю компьютера, подключенного к такой сети, Сетевой экран закрывает доступ к файлам и принтерам этого компьютера. Сторонние пользователи также не могут получить доступ к информации через папки общего доступа и удаленный доступ к рабочему столу этого компьютера. Сетевой экран фильтрует сетевую активность каждого приложения в соответствии с сетевыми правилами этого приложения.

  Сетевой экран по умолчанию присваивает тип *Публичная сеть* сети Интернет. Вы не можете изменить тип сети Интернет.

- **Локальная сеть**. Сеть для пользователей, которым ограничен доступ к файлам и принтерам этого компьютера (например, для локальной сети организации или для домашней сети).

- **Доверенная сеть**. Безопасная сеть, во время работы в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. Для сетей с этим статусом Сетевой экран разрешает любую сетевую активность в рамках этой сети.

Параметры компонента Сетевой экран

Параметр	Описание
Пакетные правила	Таблица сетевых пакетных правил. Сетевые пакетные правила используются для ввода ограничений на сетевые пакеты независимо от приложения. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных. В таблице представлены предустановленные сетевые пакетные правила, которые рекомендованы специалистами "Лаборатории Касперского" для оптимальной защиты сетевого трафика компьютеров под управлением операционных систем Microsoft Windows. Сетевой экран устанавливает приоритет выполнения для каждого сетевого пакетного правила. Сетевой экран обрабатывает сетевые пакетные правила в порядке их расположения в списке сетевых пакетных правил, сверху вниз. Сетевой экран находит первое по порядку подходящее для сетевого соединения сетевое пакетное правило и выполняет его действие: либо разрешает, либо блокирует сетевую активность. Далее Сетевой экран игнорирует все последующие сетевые пакетные правила для данного сетевого соединения. Сетевые пакетные правила имеют приоритет над сетевыми правилами приложений.
Доступные сети	Таблица, содержащая информацию о сетевых соединениях, которые Сетевой экран обнаружил на компьютере пользователя. Сети Интернет по умолчанию присвоен статус *Публичная сеть*. Вы не можете изменить статус сети Интернет.
Правила приложений	**Приложение**. Таблица приложений, работу которых контролирует компонент Сетевой экран. Приложения распределены по группам доверия. Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля сетевой активности приложений. Вы можете выбрать приложение из единого списка всех приложений, установленных на компьютерах под действием политики, и добавить приложение в группу доверия. **Сетевые правила**. Таблица сетевых правил приложений, входящих в группу доверия. В соответствии с этими правилами Сетевой экран регулирует сетевую активность для приложений. В таблице отображаются предустановленные сетевые правила, которые рекомендованы специалистами "Лаборатории Касперского". Эти сетевые правила добавлены для оптимальной защиты сетевого трафика компьютеров под управлением операционных систем Windows. Удалить предустановленные сетевые правила невозможно.

Защита от атак BadUSB

Некоторые вирусы изменяют встроенное программное обеспечение USB-устройств так, чтобы операционная система определяла USB-устройство как клавиатуру. В результате вирус может выполнять команды под вашей учетной записью, например, загрузить вредоносное приложение.

Компонент Защита от атак BadUSB позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру.

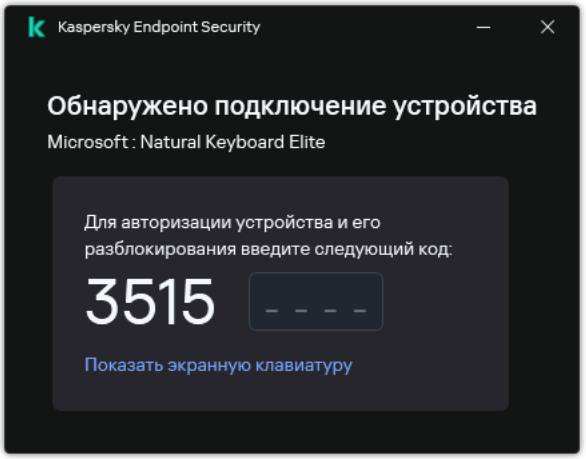
Когда к компьютеру подключается USB-устройство, определенное операционной системой как клавиатура, приложение предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) цифровой код, сформированный приложением (см. рис. ниже). Эта процедура называется авторизацией клавиатуры.

Если код введен правильно, приложение сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется.

При подключении авторизованной клавиатуры через другой USB-порт компьютера приложение снова запрашивает ее авторизацию.

Если цифровой код введен неправильно, приложение формирует новый. Вы можете настроить число попыток для ввода цифрового кода. Если цифровой код введен неправильно несколько раз или закрыто окно авторизации клавиатуры (см. рис. ниже), приложение блокирует ввод с этой клавиатуры. По истечении времени блокировки USB-устройства или перезагрузке операционной системы приложение снова предлагает пройти авторизацию клавиатуры.

Приложение разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.



Авторизация клавиатуры

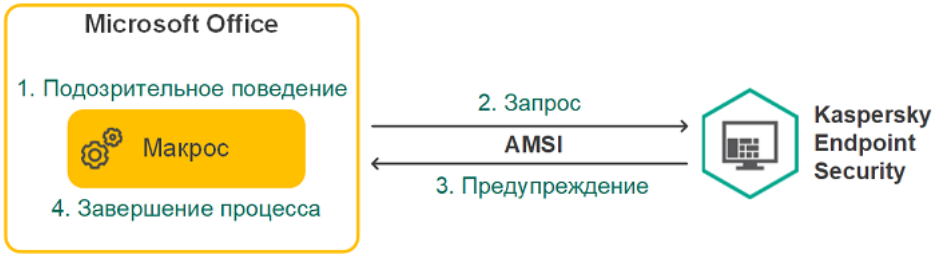
Параметры компонента Защита от атак BadUSB

Параметр	Описание
Запретить использование экранной клавиатуры для авторизации USB-устройств	Если переключатель включен, приложение запрещает использование экранной клавиатуры для авторизации USB-устройства, с которого невозможно ввести код авторизации.
Запретить использование штрихкода для авторизации USB-устройств	Если переключатель включен, приложение не показывает штрихкод в уведомлении для авторизации сканеров штрихкодов.
Максимальное количество попыток авторизации USB-устройства	Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Endpoint Security покажет время блокировки USB-устройства. По истечении указанного времени вам будут снова доступны 5 попыток ввода кода авторизации.
Тайм-аут при достижении максимального количества попыток	Время блокировки USB-устройства после заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).

AMSI-защита

Компонент AMSI-защита предназначен для поддержки интерфейса Antimalware Scan Interface от Microsoft. *Интерфейс Antimalware Scan Interface (AMSI)* позволяет сторонним приложениям с поддержкой AMSI отправлять объекты (например, скрипты PowerShell) в Kaspersky Endpoint Security для дополнительной проверки и получать результаты проверки этих объектов. Сторонними приложениями могут быть, например, приложения Microsoft Office (см. рис. ниже). Подробнее об интерфейсе AMSI см. в документации Microsoft.

AMSI-защита может только обнаруживать угрозу и уведомлять стороннее приложение об обнаруженной угрозе. Стороннее приложение после получения уведомления об угрозе не дает выполнить вредоносные действия (например, завершает работу).



Пример работы AMSI

Компонент AMSI-защита может отклонить запрос от стороннего приложения, например, если это приложение превысило максимальное количество запросов за промежуток времени. Kaspersky Endpoint Security отправляет информацию об отклонении запроса от стороннего приложения на Сервер администрирования. Компонент AMSI-защита не отклоняет запросы от тех сторонних приложений, для которых включена функция постоянного взаимодействия с компонентом AMSI-защита.

AMSI-защита доступна для следующих операционных систем рабочих станций и серверов:

- Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise / Enterprise multi-session;
- Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise / Enterprise multi-session;
- Windows Server 2016 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая режим Server Core);
- Windows Server 2025 Standard / Datacenter.

Параметры компонента AMSI-защита

Параметр	Описание
Проверять архивы	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
Проверять дистрибутивы	Проверка дистрибутивов сторонних приложений.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
Не распаковывать составные файлы большого размера	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.

Защита от эксплойтов

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимое приложение. При обработке этих данных уязвимое приложение выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО. Если попытка запустить исполняемый файл из уязвимого приложения не была произведена пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла или информирует пользователя.

Компонент Защита от эксплойтов дополнительно контролирует сетевые порты для процессов приложений, которые могут представлять угрозу безопасности компьютера. Приложение получает данные о таких процессах с антивирусными базами.

Параметры компонента Защита от эксплойтов

Параметр	Описание
При обнаружении эксплойта	**Блокировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security блокирует операции этого эксплойта и создает в журнале запись, содержащую информацию об этом эксплойте. **Информировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security создает в журнале запись, содержащую информацию об этом эксплойте, и добавляет информацию об этом эксплойте в список активных угроз.
Включить защиту памяти системных процессов	Если переключатель включен, Kaspersky Endpoint Security блокирует сторонние процессы, осуществляющие попытки доступа к памяти системных процессов.

Анализ поведения

Компонент Анализ поведения получает данные о действиях приложений на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы. Компонент Анализ поведения использует шаблоны опасного поведения приложений. Если активность приложения совпадает с одним из шаблонов опасного поведения, Kaspersky Endpoint Security выполняет выбранное ответное действие. Функциональность Kaspersky Endpoint Security, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

Компонент Анализ поведения дополнительно контролирует сетевые порты для процессов приложений, которые могут представлять угрозу безопасности компьютера. Приложение получает данные о таких процессах с антивирусными базами.

Параметры компонента Анализ поведения

Параметр	Описание
Действие при обнаружении вредоносной активности	**Удалять**. Если выбран этот вариант, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security удаляет исполняемый файл вредоносного приложения и создает резервную копию файла в резервном хранилище. **Блокировать**. Если выбран этот вариант, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security завершает работу этого приложения. **Информировать**. Если выбран этот вариант, то в случае обнаружения вредоносной активности приложения Kaspersky Endpoint Security не завершает работу этого приложения и добавляет информацию о вредоносной активности этого приложения в список активных угроз.

Предотвращение вторжений

Компонент Предотвращение вторжений (англ. Host Intrusion Prevention System, HIPS) предотвращает выполнение приложениями опасных для системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и персональным данным. Компонент обеспечивает защиту компьютера с помощью антивирусных баз и облачной службы Kaspersky Security Network.

Компонент контролирует работу приложений с помощью *прав приложений*. Права приложений включают в себя следующие параметры доступа:

- доступ к ресурсам операционной системы (например, параметры автозапуска, ключи реестра);
- доступ к персональным данным (например, к файлам, приложениям).

Сетевую активность приложений контролирует Сетевой экран с помощью *сетевых правил*.

Во время первого запуска приложения компонент Предотвращение вторжений выполняет следующие действия:

1. Проверяет безопасность приложения с помощью загруженных антивирусных баз.
2. Проверяет безопасность приложения в Kaspersky Security Network.

   Для более эффективной работы компонента Предотвращение вторжений вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает приложение в одну из групп доверия: *Доверенные*, *Слабые ограничения*, *Сильные ограничения*, *Недоверенные*.

   Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля активности приложений. Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от уровня опасности, которую это приложение может представлять для компьютера.

   Kaspersky Endpoint Security помещает приложение в группу доверия для компонентов Сетевой экран и Предотвращение вторжений. Изменить группу доверия только для Сетевого экрана или только для Предотвращения вторжений невозможно.

   Если вы отказались принимать участие в KSN или отсутствует сеть, Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации приложения от KSN группа доверия может быть изменена автоматически.

4. Блокирует действия приложения в зависимости от группы доверия. Например, приложениям из группы доверия *Сильные ограничения* запрещен доступ к модулям операционной системы.

При следующем запуске приложения Kaspersky Endpoint Security проверяет целостность приложения. Если приложение не было изменено, компонент применяет к ней текущие права приложения. Если приложение было изменено, Kaspersky Endpoint Security исследует приложение как при первом запуске.

Параметр	Описание
Права приложений	Таблица приложений, работу которых контролирует компонент Предотвращение вторжений. Приложения распределены по группам доверия. Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля активности приложений. Вы можете выбрать приложение из единого списка всех приложений, установленных на компьютерах под действием политики, и добавить приложение в группу доверия. Права доступа приложения приведены в следующих таблицах: • **Файлы и системный реестр**. Таблица прав доступа к ресурсам операционной системы и персональным данным для приложений, входящих в группу доверия. • **Права**. Таблица прав доступа к процессам и ресурсам операционной системы для приложений, входящих в группу доверия. • **Сетевые правила**. Таблица сетевых правил приложений, входящих в группу доверия. В соответствии с этими правилами Сетевой экран регулирует сетевую активность для приложений. В таблице отображаются предустановленные сетевые правила, которые рекомендованы специалистами "Лаборатории Касперского". Эти сетевые правила добавлены для оптимальной защиты сетевого трафика компьютеров под управлением операционных систем Windows. Удалить предустановленные сетевые правила невозможно.
Защищаемые ресурсы	Таблица содержит ресурсы компьютера, распределенные по категориям. Компонент Предотвращение вторжений контролирует доступ других приложений к ресурсам из этой таблицы. Ресурсом может быть категория реестра, файл или папка, ключ реестра.
Группа доверия для приложений, запущенных до Kaspersky Endpoint Security для Windows	Группа доверия, в которую Kaspersky Endpoint Security будет помещать приложения, запускаемые до Kaspersky Endpoint Security.
Обновлять правила для ранее неизвестных приложений из KSN	Если флажок установлен, то компонент Предотвращение вторжений обновляет права ранее неизвестных приложений, используя базы Kaspersky Security Network.
Доверять приложениям, имеющим цифровую подпись	Если флажок установлен, то компонент Предотвращение вторжений помещает приложения с цифровой подписью доверенных производителей в группу доверия *Доверенные*. *Доверенные производители* – производители, которым доверяет "Лаборатория Касперского". Также вы можете добавить сертификат производителя в доверенное хранилище сертификатов вручную. Если флажок снят, компонент Предотвращение вторжений не считает такие приложения доверенными и распределяет их по группам доверия на основании других параметров.
Удалять правила для приложений, не запускавшихся более N дней (от 1 до 90)	Если флажок установлен, то Kaspersky Endpoint Security автоматически удаляет информацию о приложении (группа доверия, права доступа) при выполнении следующих условий: • Вы вручную поместили приложение в группу доверия или настроили права доступа. • Приложение не запускалось в течение заданного периода времени. Если группа доверия и права приложения определены автоматически, Kaspersky Endpoint Security удаляет информацию об этом приложении через 30 дней. Изменить время хранения информации о приложении или выключить автоматическое удаление невозможно. При следующем запуске этого приложения Kaspersky Endpoint Security исследует приложение как при первом запуске.
Группа доверия для приложений, не включенных в другие группы	Раскрывающийся список, элементы которого определяют, в какую группу доверия Kaspersky Endpoint Security будет помещать неизвестное приложение. Вы можете выбрать один из следующих элементов: • **Слабые ограничения**. • **Сильные ограничения**. • **Недоверенные**.

Откат вредоносных действий

Компонент Откат вредоносных действий позволяет Kaspersky Endpoint Security отменять действия, произведенные вредоносными приложениями в операционной системе.

Во время отката действий вредоносного приложения в операционной системе Kaspersky Endpoint Security обрабатывает следующие типы активности вредоносного приложения:

- **Файловая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет исполняемые файлы, созданные вредоносным приложением (на всех носителях, кроме сетевых дисков);
  - удаляет исполняемые файлы, созданные приложениями, в которые внедрилось вредоносное приложение;
  - восстанавливает измененные или удаленные вредоносным приложением файлы.

  Функциональность восстановления файлов имеет ряд ограничений.

- **Реестровая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет разделы и ключи реестра, созданные вредоносным приложением;
  - не восстанавливает измененные или удаленные вредоносным приложением разделы и ключи реестра.

- **Системная активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - завершает процессы, которые запускало вредоносное приложение;
  - завершает процессы, в которые внедрялось вредоносное приложение;
  - не возобновляет процессы, которые остановило вредоносное приложение.

- **Сетевая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - запрещает сетевую активность вредоносного приложения;
  - запрещает сетевую активность тех процессов, в которые внедрялось вредоносное приложение.

Откат действий вредоносного приложения может быть запущен компонентом Защита от файловых угроз, Анализ поведения или при поиске вредоносного ПО.

Откат действий вредоносного приложения затрагивает строго ограниченный набор данных. Откат не оказывает негативного влияния на работу операционной системы и целостность информации на вашем компьютере.

Kaspersky Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть Kaspersky Security Network.

Функциональность KSN может быть недоступна в приложении на территории США.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, приложение Kaspersky Endpoint Security получает от служб KSN сведения о репутации проверяемых веб-адресов, а также сведения о категории и репутации проверяемых файлов. Подробнее о настройке доступа к KSN см. в справке Kaspersky Security Center.

Использование Kaspersky Security Network является добровольным. Приложение предлагает использовать KSN во время первоначальной настройки приложения. Начать или прекратить использование KSN можно в любой момент.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского". Файл ksn_<ID языка>.txt с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения.

Инфраструктура репутационных баз "Лаборатории Касперского"

Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения для работы с репутационными базами "Лаборатории Касперского":

- *Kaspersky Security Network (KSN)* – это решение, которое используют большинство приложений "Лаборатории Касперского". Участники KSN получают информацию от "Лаборатории Касперского", а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.

- *Kaspersky Private Security Network (KPSN)* – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров. KPSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

  - отсутствие подключения локальных рабочих мест к сети Интернет;

законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

Параметр	Описание
Включить расширенный режим KSN	*Расширенный режим KSN* – режим работы приложения, при котором Kaspersky Endpoint Security передает в "Лабораторию Касперского" дополнительные данные. Независимо от положения переключателя, Kaspersky Endpoint Security использует KSN для обнаружения угроз.
Включить облачный режим	*Облачный режим* – режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию антивирусных баз. Работу приложения с облегченными антивирусными базами обеспечивает Kaspersky Security Network. Облегченная версия антивирусных баз позволяет снизить нагрузку на оперативную память компьютера примерно в два раза. Если вы не участвуете в Kaspersky Security Network или облачный режим выключен, Kaspersky Endpoint Security загружает полную версию антивирусных баз с серверов "Лаборатории Касперского". Если переключатель включен, то Kaspersky Endpoint Security использует облегченную версию антивирусных баз, за счет чего снижается нагрузка на ресурсы операционной системы. Kaspersky Endpoint Security загружает облегченную версию антивирусных баз в ходе ближайшего обновления после того, как флажок был установлен. Если переключатель выключен, то Kaspersky Endpoint Security использует полную версию антивирусных баз. Kaspersky Endpoint Security загружает полную версию антивирусных баз в ходе ближайшего обновления после того, как флажок был снят.
Статус компьютера при недоступности серверов KSN *(доступен только в консоли Kaspersky Security Center)*	Раскрывающийся список, элементы которого определяют статус компьютера в Kaspersky Security Center при недоступности серверов KSN.
Использовать Сервер администрирования как прокси-сервер KSN *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, то Kaspersky Endpoint Security использует службу KSN Proxy. Вы можете настроить параметры службы KSN Proxy в свойствах Сервера администрирования.
Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, Kaspersky Endpoint Security использует серверы KSN, когда служба KSN Proxy недоступна. Серверы KSN могут быть расположены как в "Лаборатории Касперского", так и на сторонних серверах, в случае использования Kaspersky Private Security Network.

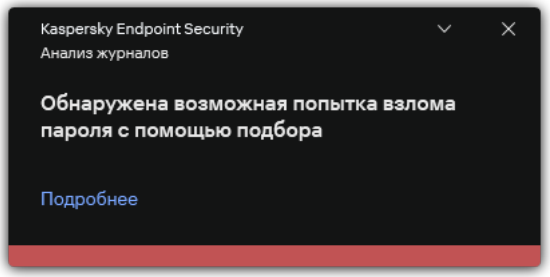
Анализ журналов

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций.

Анализ журналов контролирует целостность защищаемой среды на основе журналов событий Windows. При обнаружении признаков нетипичного поведения в системе приложение информирует администратора, так как это поведение может указывать на попытки кибератак.

Kaspersky Endpoint Security анализирует журналы событий Windows и выявляет нарушения в соответствии с правилами. В компонент включены предустановленные правила. Для работы предустановленных правил приложение использует эвристический анализ. Также вы можете добавить собственные правила (пользовательские правила). При срабатывании правила, приложение создает событие со статусом *Критическое* (см. рис. ниже).

Для работы Анализа журналов убедитесь, что параметры политики аудита безопасности настроены и система регистрирует нужные события (подробнее см. на сайте Службы технической поддержки Microsoft).



Уведомление Анализа журналов

Параметры компонента Анализ журналов

Параметр	Описание
Предустановленные правила	Список правил Анализа журналов. Предустановленные правила включают шаблоны аномальной активности на защищаемом компьютере. Аномальная активность может являться признаком попытки атаки.
Пользовательские правила	Список правил Анализа журналов, которые добавил пользователь. Вы можете задать собственные критерии срабатывания правила Анализа журналов. Для этого вам нужно ввести идентификатор события и выбрать источник событий. Для выбора источника событий доступны стандартные журналы: *Application*, *Security* или *System*. Также вы можете указать журнал стороннего приложения.

Защита от шифрования

Компонент Защита от шифрования обеспечивает анализ активности в папках общего доступа. Если активность совпадает с одним из шаблонов поведения, характерного для внешнего шифрования, Kaspersky Endpoint Security выполняет выбранное действие.

Kaspersky Endpoint Security защищает от попыток внешнего шифрования только те файлы, которые расположены на носителях информации с файловой системой NTFS и не зашифрованы системой EFS.

Параметр	Описание
Исключения по имени или IP-адресу	**Исключения по имени или IP-адресу**. Список компьютеров, с которых не будут отслеживаться попытки шифрования папок общего доступа. Для работы списка исключений компьютеров из защиты папок общего доступа от внешнего шифрования требуется включить аудит входа в систему в политике аудита безопасности Windows. По умолчанию аудит входа в систему выключен. Подробнее о политике аудита безопасности Windows см. на сайте Microsoft. **Исключения по маске**. Исключения из области защиты. Исключение папки из области защиты позволит сократить количество ложных срабатываний, если в вашей организации используется шифрование данных при обмене файлами с помощью папок общего доступа. Например, Анализ поведения может создавать ложные срабатывания при работе пользователя с файлами с расширением ENC в папке общего доступа. Такая активность совпадает с шаблоном поведения, характерного для внешнего шифрования. Если вы зашифровали файлы в папке общего доступа для защиты данных, добавьте эту папку в исключения. Используйте маски: • Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках. • Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает. • Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.
Действие при обнаружении угрозы	• **Информировать**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security добавляет информацию об этой попытке изменения файлов в папках общего доступа в список активных угроз, добавляет запись в отчеты локального интерфейса приложения и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности. • **Блокировать соединение на (мин) N мин**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security блокирует доступ на изменение файлов для сессии, которая инициировала вредоносную активность, и создает резервные копии измененных файлов. Если включен компонент Откат вредоносных действий и выбран вариант **Блокировать соединение на (мин) N мин**, то выполняется восстановление измененных файлов из резервных копий.
Область защиты	*Область защиты* – список путей к папкам общего доступа, в которых Kaspersky Endpoint Security отслеживает файловую активность. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. По умолчанию приложение автоматически определяет папки общего доступа и отслеживает файловую активность во всех папках.

Веб-Контроль

Веб-Контроль управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени. При попытке пользователя открыть веб-сайт, доступ к которому ограничен Веб-Контролем, Kaspersky Endpoint Security заблокирует доступ или покажет предупреждение (см. рис. ниже).

Для работы Веб-Контроля необходимо выполнить первоначальную настройку приложения:

- Для контроля HTTPS-трафика включите проверку защищенных соединений (по умолчанию проверка включена).
- Выберите порты, которые Kaspersky Endpoint Security будет контролировать (по умолчанию приложение контролирует все порты).

- Выберите приложения, трафик которых будет контролировать Kaspersky Endpoint Security. Основные браузеры уже добавлены в список, рекомендованный "Лабораторией Касперского". Если вашего браузера нет в списке, добавьте приложение вручную.

- Рекомендуется внедрить в трафик скрипт для взаимодействия с веб-страницами (по умолчанию внедрение скрипта выключено). Скрипт позволяет регистрировать события работы Веб-Контроля для журнала событий приложения, журнала событий ОС, отчетов.

Способы управления доступом к веб-сайтам

Веб-Контроль позволяет настраивать доступ к веб-сайтам следующими способами:

- **Категория веб-сайта**. Категоризацию веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз приложения). Вы можете ограничить доступ пользователей, например, к категории *Социальные сети* или другим категориям.

- **Тип данных**. Вы можете ограничить доступ пользователей к данным на веб-сайте и, например, скрыть графические изображения. Kaspersky Endpoint Security определяет тип данных по формату файла, а не по расширению.

  > Kaspersky Endpoint Security не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, Kaspersky Endpoint Security определит тип данных *Архивы*, а не *Графические файлы*.

- **Отдельный адрес**. Вы можете ввести веб-адрес или использовать маски.

Вы можете использовать одновременно несколько способов регулирования доступа к веб-сайтам. Например, вы можете ограничить доступ к типу данных *Файлы офисных приложений* только для категории веб-сайтов *Веб-почта*.

Правила доступа к веб-сайтам

Веб-Контроль управляет доступом пользователей к веб-сайтам с помощью *правил доступа*. Вы можете настроить следующие дополнительные параметры правила доступа к веб-сайтам:

- Пользователи, на которых распространяется правило.

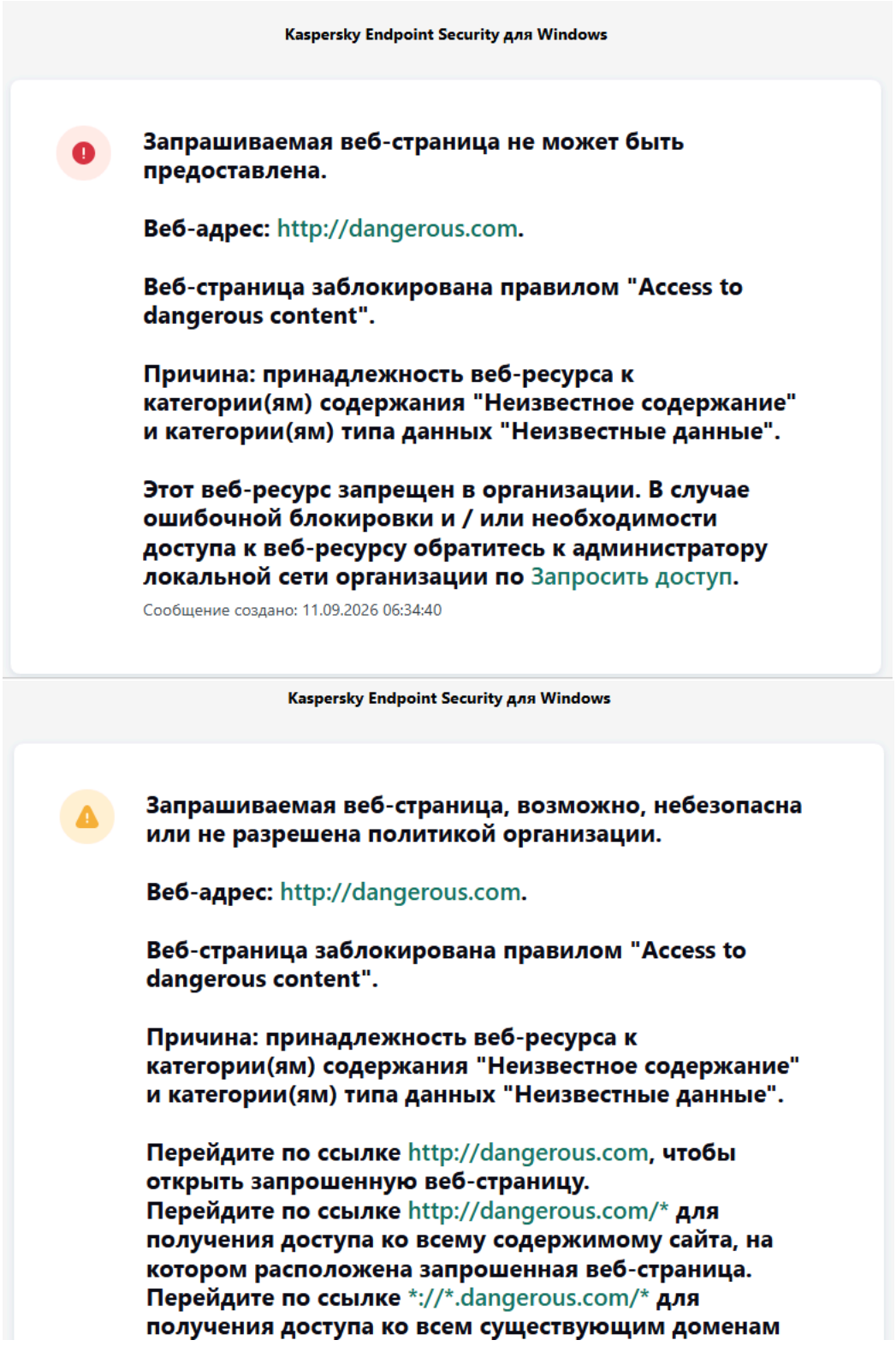
  Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

- Расписание работы правила.

  Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Приоритеты правил доступа

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом. Например, Kaspersky Endpoint Security может определить корпоративный портал как социальную сеть. Чтобы ограничить доступ к социальным сетям и предоставить доступ к корпоративному веб-порталу, создайте два правила: запрещающее правило для категории веб-сайтов *Социальные сети* и разрешающее правило для корпоративного веб-портала. Правило доступа к корпоративному веб-порталу должно иметь приоритет выше, чем правило доступа к социальным сетям.



Параметр	Описание
Правила доступа к веб-ресурсам	Список с правилами доступа к веб-ресурсам. Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом.
Правило по умолчанию	*Правило по умолчанию* – правило доступа к веб-ресурсам, которые не входят ни в одно из правил. Возможны следующие варианты: • **Разрешать все, не указанное в списке правил** – режим списка запрещенных веб-сайтов. • **Запрещать все, не указанное в списке правил** – режим списка разрешенных веб-сайтов.
Завершать активные пользовательские сеансы браузера после применения правила	Если флажок установлен, Веб-Контроль разрывает подключение к запрещенным веб-ресурсам сразу после применения политики. Браузер немедленно прекращает загрузку данных на веб-странице. При обновлении веб-страницы или переходе на другую запрещенную веб-страницу приложение показывает предупреждение. Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения. Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.
Шаблоны	**Предупреждение**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу. **Сообщение о блокировке**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу. **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете доступа к веб-странице**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты. Для работы с шаблонами сообщений предусмотрены специальные переменные (например, `%USER_NAME%`). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров.
Записывать данные о посещении разрешенных страниц в журнал	Kaspersky Endpoint Security записывает данные о посещении всех веб-сайтов, в том числе и разрешенных. Kaspersky Endpoint Security отправляет события в Kaspersky Security Center, локальный журнал Kaspersky Endpoint Security, журнал событий Windows. Для мониторинга активности пользователя в интернете нужно настроить параметры сохранения событий. Браузеры, которые поддерживают функцию мониторинга: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Яндекс.Браузер, Mozilla Firefox. Мониторинг активности пользователей не работает в других браузерах. Мониторинг активности пользователя в интернете может потребовать больше ресурсов компьютера при расшифровке HTTPS-трафика.

Контроль устройств

Контроль устройств управляет доступом пользователей к установленным или подключенным к компьютеру устройствам (например, жестким дискам, камере или модулю Wi-Fi). Это позволяет защитить компьютер от заражения при подключении этих устройств и предотвратить потерю или утечку данных.

Если Контроль устройств включен, приложение передает в Kaspersky Security Center информацию о подключенных устройствах. Вы можете просмотреть список подключенных устройств в Kaspersky Security Center в папке **Дополнительно → Хранилища → Оборудование**.

Уровни доступа к устройствам

Контроль устройств управляет доступом на следующих уровнях:

- **Тип устройства**. Например, принтеры, съемные диски, CD/DVD-приводы.

  Вы можете настроить доступ устройств следующим образом:

  - Разрешать – ✓.
  - Запрещать – ⊘.
  - По правилам (только принтеры и портативные устройства) – .
  - Зависит от шины подключения (кроме Wi-Fi) – .
  - Запрещать с исключениями (только Wi-Fi) – .

- **Шина подключения**. *Шина подключения* – интерфейс, с помощью которого устройства подключаются к компьютеру (например, USB, FireWire). Если для типа устройств выбран режим **Зависит от шины подключения**, приложение разрешает или запрещает доступ к устройству в зависимости от интерфейса подключения (например, через USB).

  Вы можете настроить доступ устройств следующим образом:

  - Разрешать – ✓.
  - Запрещать – ⊘.

- **Доверенные устройства**. *Доверенные устройства* – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

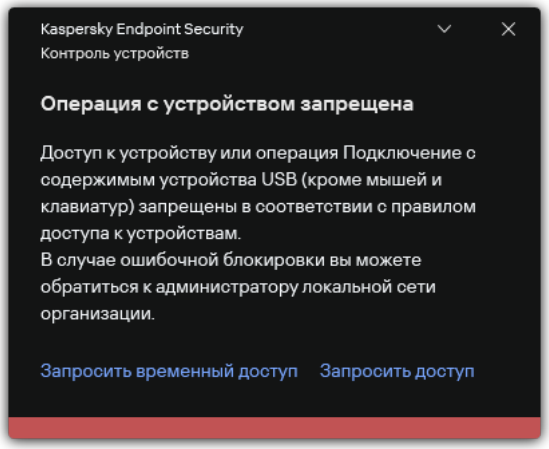
  Вы можете добавить доверенные устройства по следующим данным:

  - **Устройства по идентификатору**. Каждое устройство имеет уникальный идентификатор (англ. Hardware ID, HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы. Пример идентификатора устройства: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств.
  - **Устройства по модели**. Каждое устройство имеет идентификатор производителя (англ. Vendor ID, VID) и идентификатор продукта (англ. Product ID, PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы. Шаблон для ввода VID и PID: `VID_1234&PID_5678`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.
  - **Устройства по маске идентификатора**. Если вы используете несколько устройств с похожими идентификаторами, вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security не поддерживает символ `?` при вводе маски. Например, `WDC_C*`.
  - **Устройства по маске модели**. Если вы используете несколько устройств с похожими VID или PID (например, устройства одного производителя), вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security не поддерживает символ `?` при вводе маски. Например, `VID_05AC&PID_*`.

Контроль устройств регулирует доступ пользователей к устройствам с помощью *правил доступа*. Также Контроль устройств позволяет сохранять события подключения / отключения устройств. Для сохранения событий вам нужно настроить отправку событий в политике.

Если доступ к устройству зависит от шины подключения (статус), Kaspersky Endpoint Security не сохраняет события подключения / отключения устройства. Чтобы приложение Kaspersky Endpoint Security сохраняло события подключения / отключения устройства, разрешите доступ к соответствующему типу устройств (статус) или добавьте устройство в список доверенных.

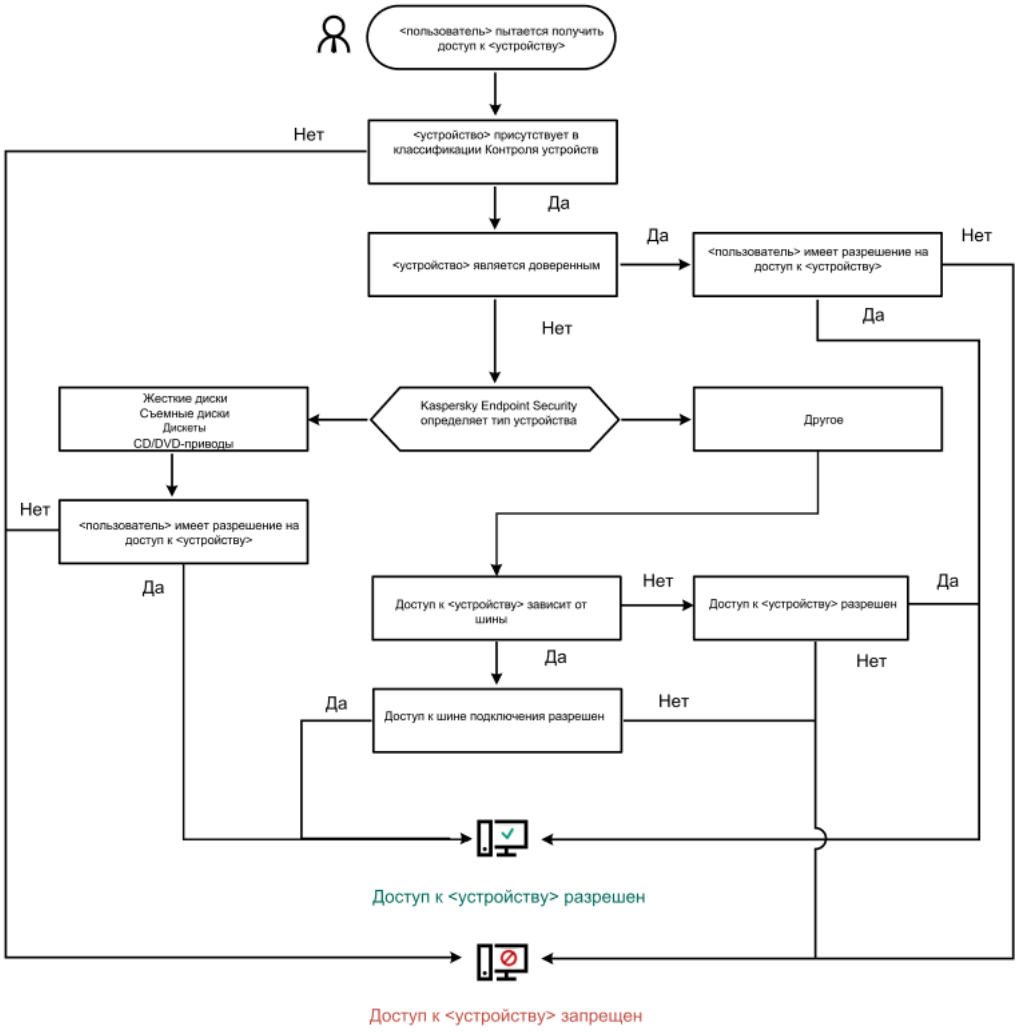
При подключении к компьютеру устройства, доступ к которому запрещен Контролем устройств, Kaspersky Endpoint Security заблокирует доступ и покажет уведомление (см. рис. ниже).



Уведомление Контроля устройств

Алгоритм работы Контроля устройств

Kaspersky Endpoint Security принимает решение о доступе к устройству после того, как пользователь подключил это устройство к компьютеру (см. рис. ниже).



Алгоритм работы Контроля устройств

Если устройство подключено и доступ разрешен, вы можете изменить правило доступа и запретить доступ. В этом случае при очередном обращении к устройству (просмотр дерева папок, чтение, запись) Kaspersky Endpoint Security блокирует доступ. Блокирование устройства без файловой системы произойдет только при последующем подключении устройства.

Если пользователю компьютера с установленным приложением Kaspersky Endpoint Security требуется запросить доступ к устройству, которое, по его мнению, было заблокировано ошибочно, передайте ему инструкцию по запросу доступа.

Параметр	Описание
Разрешать запрашивать временный доступ *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, то кнопка **Запросить доступ** в локальном интерфейсе Kaspersky Endpoint Security доступна. С помощью этой кнопки пользователь может запросить временный доступ к заблокированному устройству.
Устройства и сети Wi-Fi	Таблица со всеми возможными типами устройств по классификации компонента Контроль устройств и статусом доступа к ним.
Шины подключения	Список всех возможных шин подключения по классификации компонента Контроль устройств и статусом доступа к ним. Kaspersky Endpoint Security разрешает или запрещает доступ к устройствам по шине подключения, если выбран режим **Зависит от шины подключения**.
Доверенные устройства	Список доверенных устройств и пользователей, которым разрешен доступ к этим устройствам.
Объединять значения при наследовании *(доступен только в консоли Kaspersky Security Center)*	Объединение списка доверенных устройств в родительских и дочерних политиках Kaspersky Security Center. Для объединения списков необходимо в дочерней политике включить наследование параметров родительской политики Kaspersky Security Center. Если флажок установлен, элементы списка родительской политики Kaspersky Security Center отображаются в дочерних политиках и доступны для просмотра. Таким образом, вы можете, например, создать общий список доверенных устройств для всей организации. Удалить или изменить унаследованные элементы списка в дочерней политике невозможно. Элементы списка доверенных устройств, объединенные при наследовании, доступны для удаления и изменения только в родительской политике. Добавление, изменение и удаление элементов списка возможно на нижестоящих уровнях. Если элементы списков дочерней и родительской политик совпадают, эти элементы отображаются как один элемент родительской политики. Если флажок снят, то элементы списков не объединяются при наследовании параметров политик Kaspersky Security Center. Также эта функция позволяет объединять списки в профилях политик. Для объединения списков необходимо в профиле высшего приоритета включить наследование параметров из профиля низшего приоритета. Подробнее о приоритетах профилей политики см. в справке Kaspersky Security Center.
Анти-Бриджинг	Анти-Бриджинг предотвращает создание сетевых мостов, исключая возможность одновременной установки нескольких сетевых соединений для компьютера. Это позволяет защитить корпоративную сеть от атак через незащищенные, несанкционированные сети. Анти-Бриджинг блокирует установку нескольких соединений в соответствии с приоритетами устройств. Чем выше находится устройство в списке, тем выше его приоритет. Если активное и новое соединения относятся к одному типу (например, Wi-Fi), Kaspersky Endpoint Security блокирует активное соединение и разрешает установку нового соединения. Если активное и новое соединения относятся к разным типам (например, сетевой адаптер и Wi-Fi), Kaspersky Endpoint Security блокирует соединение с более низким приоритетом и разрешает соединение с более высоким приоритетом. Анти-Бриджинг поддерживает работу со следующими типами устройств: сетевой адаптер, Wi-Fi и модем.
Шаблоны сообщений	**Сообщение о блокировке**. Шаблон сообщения, которое появляется при обращении пользователя к заблокированному устройству. Также сообщение появляется при попытке пользователя совершить операцию над содержимым устройства, которая запрещена для этого пользователя. **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к устройству или запрет операции над содержимым устройства, по мнению пользователя, произошли ошибочно. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете доступа к устройству**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

Контроль приложений

Контроль приложений управляет запуском приложений на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании приложений. Также Контроль приложений снижает риск заражения компьютера, ограничивая доступ к приложениям.

Настройка Контроля приложений состоит из следующих этапов:

1. Создание категорий приложений.

   Администратор создает категории приложений, которыми администратор хочет управлять. Категории приложений предназначены для всех компьютеров сети организации независимо от групп администрирования. Для создания категории вы можете использовать следующие критерии: KL-категория (например, *Браузеры* или другая категория), хеш файла, производитель приложения и другие.

2. Создание правил Контроля приложений.

   Администратор создает правила Контроля приложений в политике для группы администрирования. Правило включает в себя категории приложений и статус запуска приложений из этих категорий: запрещен или разрешен. Администратор может создать множество правил. При этом одно приложение может соответствовать критериям нескольких правил. Приоритет запрещающего правила выше разрешающего. Kaspersky Endpoint Security проверяет приложение на принадлежность к правилу при каждом запуске. Kaspersky Endpoint Security последовательно проверяет приложение по всем правилам Контроля приложения.

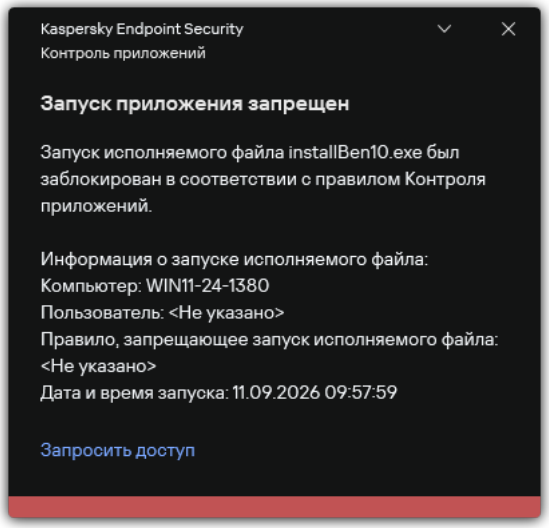
3. Выбор режима работы Контроля приложений.

   Администратор выбирает режим работы с приложениями, которые не входят ни в одно из правил (списки запрещенных и разрешенных приложений).

При попытке пользователя запустить запрещенное приложение, Kaspersky Endpoint Security заблокирует запуск приложения и покажет уведомление (см. рис. ниже).

Для проверки настройки Контроля приложений предусмотрен *тестовый режим*. В этом режиме Kaspersky Endpoint Security выполняет следующие действия:

- разрешает запуск приложений, в том числе запрещенных;
- показывает уведомление о запуске запрещенного приложения и добавляет информацию в отчет на компьютере пользователя;
- отправляет данные о запуске запрещенных приложений в Kaspersky Security Center.



Уведомление Контроля приложений

Режимы работы Контроля приложений

Компонент Контроль приложений может работать в двух режимах:

- **Список запрещенных**. Режим, при котором Контроль приложений разрешает пользователям запуск любых приложений, кроме тех, которые запрещены в правилах Контроля приложений.

  Этот режим работы Контроля приложений установлен по умолчанию.

- **Список разрешенных**. Режим, при котором Контроль приложений запрещает пользователям запуск любых приложений, кроме тех, которые разрешены и не запрещены в правилах Контроля приложений.

  Если разрешающие правила Контроля приложений сформированы максимально полно, компонент запрещает запуск всех новых приложений, не проверенных администратором локальной сети организации, но обеспечивает работоспособность операционной системы и проверенных приложений, которые нужны пользователям для выполнения должностных обязанностей.

  Вы можете ознакомиться с рекомендациями по настройке правил Контроля приложений в режиме списка разрешенных приложений.

Настройка Контроля приложений для работы в этих режимах возможна как в локальном интерфейсе Kaspersky Endpoint Security, так и с помощью Kaspersky Security Center.

Однако Kaspersky Security Center предоставляет инструменты, недоступные в локальном интерфейсе Kaspersky Endpoint Security и необходимые для следующих задач:

- Создание категорий приложений.

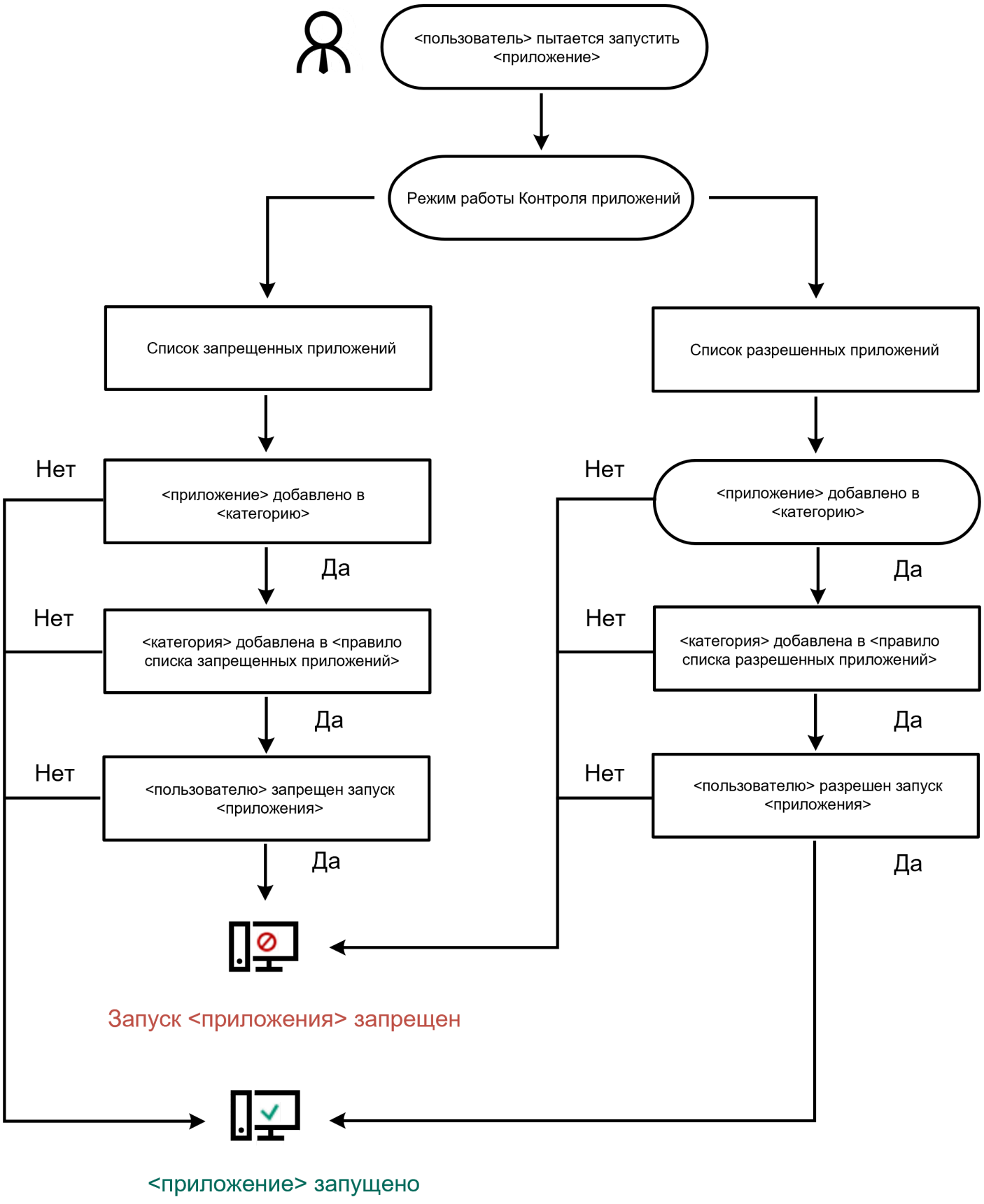
  Правила Контроля приложений, сформированные в Консоли администрирования Kaspersky Security Center, основываются на созданных вами категориях приложений, а не на включающих и исключающих условиях, как в локальном интерфейсе Kaspersky Endpoint Security.

- Получение информации о приложениях, которые установлены на компьютерах локальной сети организации.

Поэтому настройку работы компонента Контроль приложений рекомендуется выполнять с помощью Kaspersky Security Center.

Алгоритм работы Контроля приложений

Kaspersky Endpoint Security использует алгоритм для принятия решения о запуске приложения (см. рис. ниже).



Параметры компонента Контроль приложений

Параметр	Описание
Действие при запуске приложений, запрещенных правилами	**Применять правила**. Kaspersky Endpoint Security управляет запуском приложений в соответствии с выбранным режимом. **Тестировать правила**. Kaspersky Endpoint Security разрешает запуск приложения, запрещенного в текущем режиме Контроля приложений, но заносит информацию о запуске приложения в отчет.
Режим контроля запуска приложений	Вы можете выбрать один из следующих вариантов: • **Список запрещенных**. Если выбран этот вариант, Контроль приложений разрешает всем пользователям запуск любых приложений, кроме случаев, удовлетворяющих условиям запрещающих правил Контроля приложений. • **Список разрешенных**. Если выбран этот вариант, Контроль приложений запрещает всем пользователям запуск любых приложений, кроме случаев, удовлетворяющих условиям разрешающих правил Контроля приложений. При выборе режима **Список разрешенных** автоматически создается два правила Контроля приложений: • **Приложения ОС**. • **Доверенные приложения обновления**. Изменение параметров и удаление автоматически созданных правил недоступно. Вы можете включить или выключить эти правила.
Контролировать загрузку динамических библиотек	Если флажок установлен, то Kaspersky Endpoint Security контролирует загрузку DLL-модулей при запуске пользователями приложений. Информация о DLL-модуле и приложении, загрузившем этот DLL-модуль, сохраняется в отчет. При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в параметрах Контроля приложений включено правило по умолчанию **Приложения ОС** или другое правило, которое содержит KL-категорию **Приложения ОС\Доверенные сертификаты** и обеспечивает загрузку доверенных DLL-модулей и драйверов до запуска Kaspersky Endpoint Security. Включение контроля загрузки DLL-модулей и драйверов при выключенном правиле **Приложения ОС** может привести к нестабильности операционной системы. Kaspersky Endpoint Security контролирует только DLL-модули и драйверы, загруженные с момента установки флажка. Рекомендуется перезагрузить компьютер после установки флажка, чтобы приложение контролировало все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security.
Использовать строгую проверку цифровой подписи	Вы можете выбрать сертификат в качестве условия срабатывания правила Контроля приложений. Если флажок установлен, то Kaspersky Endpoint Security применяет правила к приложениям, подписанным сертификатом только из доверенного системного хранилища сертификатов приложения. Приложения, подписанные таким сертификатом, также являются доверенными для компонентов защиты, например, для задачи *Поиск вредоносного ПО*. При этом, если в правиле Контроля приложений указать сертификат из другого хранилища, Kaspersky Endpoint Security не применит такое правило. Если флажок снят, Kaspersky Endpoint Security применяет правила к приложениям, подписанным сертификатом из хранилища доверенных корневых центров Windows (англ. Trusted Root Certificate Store). Такие приложения не входит в доверенную зону. Компоненты защиты контролируют активность таких приложений.
Шаблоны сообщений о блокировке приложений	**Сообщение о блокировке**. Шаблон сообщения, которое появляется при срабатывании правила Контроля приложений, блокирующего запуск приложения. **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка приложения, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете запуска приложения**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

Адаптивный контроль аномалий

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов.

Компонент Адаптивный контроль аномалий отслеживает и блокирует действия, нехарактерные для компьютеров сети организации. Для отслеживания нехарактерных действий Адаптивный контроль аномалий использует набор правил (например, правило *Запуск Windows PowerShell из офисного приложения*). Правила созданы специалистами "Лаборатории Касперского" на основе типичных сценариев вредоносной активности. Вы можете выбрать поведение Адаптивного контроля аномалий для каждого из правил и, например, разрешить запуск PowerShell-скриптов для автоматизации решения корпоративных задач. Kaspersky Endpoint Security обновляет набор правил с базами приложения. Обновление набора правил нужно подтверждать вручную.

Настройка Адаптивного контроля аномалий

Настройка Адаптивного контроля аномалий состоит из следующих этапов:

1. Обучение Адаптивного контроля аномалий.

   После включения Адаптивного контроля аномалий правила работают в *обучающем режиме*. В ходе обучения Адаптивный контроль аномалий отслеживает срабатывание правил и отправляет события срабатывания в Kaspersky Security Center. Каждое правило имеет свой срок действия обучающего режима. Срок действия обучающего режима устанавливают специалисты "Лаборатории Касперского". Обычно срок действия обучающего режима составляет 2 недели.

   Если в ходе обучения правило ни разу не сработало, Адаптивный контроль аномалий будет считать действия, связанные с этим правилом, нехарактерным. Kaspersky Endpoint Security будет блокировать все действия, связанные с этим правилом.

   Если в ходе обучения правило сработало, Kaspersky Endpoint Security регистрирует события в отчете о срабатываниях правил и в хранилище **Правила срабатываний в статусе Интеллектуальное обучение**.

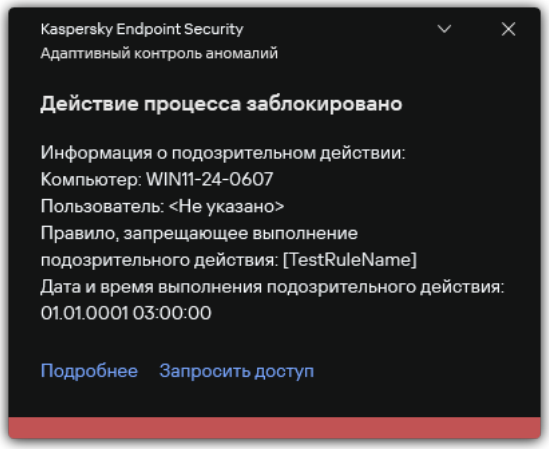
2. Анализ отчета о срабатывании правил.

   Администратор анализирует отчет о срабатываниях правил или содержание хранилища **Правила срабатываний в статусе Интеллектуальное обучение**. Далее администратор может выбрать поведение Адаптивного контроля аномалий при срабатывании правила: блокировать или разрешить. Также администратор может продолжить отслеживать срабатывание правила и продлить работу приложения в обучающем режиме. Если администратор не предпринимает никаких мер, приложение также продолжит работать в обучающем режиме. Отсчет срока действия обучающего режима начинается заново.

Настройка Адаптивного контроля аномалий происходит в режиме реального времени и осуществляется по следующим каналам:

- Адаптивный контроль аномалий автоматически начинает блокировать действия, связанные с правилами, которые не сработали в течение обучающего режима.
- Kaspersky Endpoint Security добавляет новые правила или удаляет неактуальные.
- Администратор настраивает работу Адаптивного контроля аномалий после анализа отчета о срабатывании правил и содержимого хранилища **Правила срабатываний в статусе Интеллектуальное обучение**. Рекомендуется проверять отчет о срабатывании правил и содержимое хранилища **Правила срабатываний в статусе Интеллектуальное обучение**.

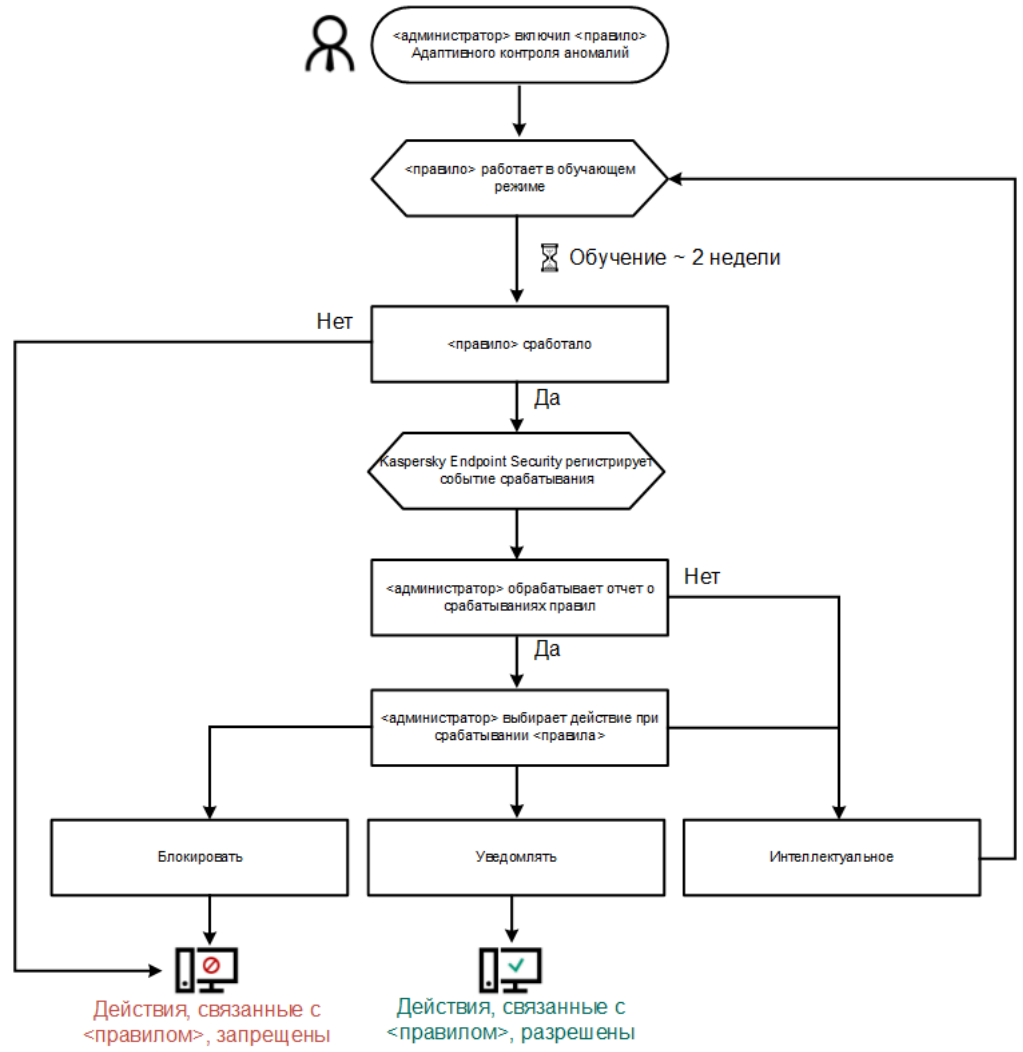
При попытке вредоносного приложения выполнить действие, Kaspersky Endpoint Security заблокирует действие и покажет уведомление (см. рис. ниже).



Уведомление Адаптивного контроля аномалий

Алгоритм работы Адаптивного контроля аномалий

Kaspersky Endpoint Security принимает решение о выполнении действия, связанного с правилом, по следующему алгоритму (см. рис. ниже).



Алгоритм работы Адаптивного контроля аномалий

Параметры компонента Адаптивный контроль аномалий

Параметр	Описание
Отчет о состоянии правил Адаптивного контроля аномалий *(доступен только в консоли Kaspersky Security Center)*	В этом отчете содержится информация о статусе правил обнаружения Адаптивного контроля аномалий (например, статусы *Выключено* или *Блокировать*). Отчет формируется для всех групп администрирования.
Отчет о срабатываниях правил Адаптивного контроля аномалий *(доступен только в консоли Kaspersky Security Center)*	В этом отчете содержится информация о нехарактерных действиях, обнаруженных с помощью Адаптивного контроля аномалий. Отчет формируется для всех групп администрирования.

Параметр	Описание
Правила	Таблица правил Адаптивного контроля аномалий. Правила созданы специалистами "Лаборатории Касперского" на основе типичных сценариев вредоносной активности.
Шаблоны	**Сообщение о блокировке**. Шаблон сообщения для пользователя, которое появляется при срабатывании правила Адаптивного контроля аномалий, блокирующего нехарактерное действие. **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка действия, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие **Сообщение администратору о запрете действия приложения**. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в консоли Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

Контроль целостности системы

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций.

Начиная с версии Kaspersky Endpoint Security для Windows 12.6 вместо компонента Мониторинг файловых операций добавлен компонент Контроль целостности системы. Контроль целостности системы включает в себя все функции Мониторинга файловых операций, а также позволяет контролировать изменения в реестре и подключение внешних устройств.

Контроль целостности системы отслеживает изменения в операционной системе, которые могут указывать на нарушения безопасности компьютера. Обнаружив такие изменения, Kaspersky Endpoint Security формирует соответствующие события и предупреждает администратора. Контроль целостности системы может работать в режиме реального времени, а также выполнять проверку целостности системы по запросу.

Контроль целостности системы в режиме реального времени

При работе в режиме реального времени Контроль целостности системы отслеживает изменения в объектах, которые вы включили в область действия компонента (*область мониторинга*). Также Контроль целостности системы позволяет блокировать несанкционированный доступ к этим объектам в режиме реального времени.

Проверка целостности системы по запросу

Проверка целостности системы по запросу представляет собой задачу, которую вы можете запускать вручную или по расписанию. Для выполнения задачи *Проверка целостности системы* требуется настроить область действия компонента (*область мониторинга*) и создать снимок состояния системы. *Снимок состояния системы* – зафиксированное состояние объектов системы, с которым приложение сравнивает текущее состояние.

Параметр	Описание
Режим работы для блокирующих правил	• **Блокировать**. В этом режиме Контроль целостности системы блокирует действия с файлами и реестром в области мониторинга и формирует соответствующее событие. • **Информировать**. В этом режиме Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга и формирует соответствующее событие.
Контроль целостности системы в режиме реального времени	При работе в режиме реального времени Контроль целостности системы отслеживает изменения в объектах, которые вы включили в область действия компонента (*область мониторинга*). Также Контроль целостности системы позволяет блокировать несанкционированный доступ к этим объектам в режиме реального времени.
Следить за устройствами	Контроль целостности системы осуществляет мониторинг подключения и отключения внешних устройств.
Следить за файлами и реестром	Контроль целостности системы осуществляет мониторинг изменений в файлах, папках и реестре.
Проверка целостности системы	Проверка целостности системы по запросу представляет собой задачу, которую вы можете запускать вручную или по расписанию. Для выполнения задачи *Проверка целостности системы* требуется настроить область действия компонента (*область мониторинга*) и создать снимок состояния системы. *Снимок состояния системы* – зафиксированное состояние объектов системы, с которым приложение сравнивает текущее состояние.

Endpoint Sensor

В Kaspersky Endpoint Security 11.4.0 компонент Endpoint Sensor исключен из приложения.

Вы можете управлять Endpoint Sensor в Kaspersky Security Center Web Console и Консоли администрирования Kaspersky Security Center. Управлять Endpoint Sensor в Kaspersky Security Center Cloud Console невозможно.

Endpoint Sensor предназначен для взаимодействия с Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* – решение, предназначенное для своевременного обнаружения сложных угроз, таких как целевые атаки, сложные постоянные угрозы (англ. Advanced Persistent Threat, APT), атаки "нулевого дня" и другие. Kaspersky Anti Targeted Attack Platform включает в себя три функциональных блока:

- Kaspersky Anti Targeted Attack (далее также "*KATA*");
- Kaspersky Endpoint Detection and Response (далее также "*EDR (KATA)*");
- Network Detection and Response (далее также "*NDR (KATA)*").

Вы можете приобрести все функциональные блоки или приобрести функциональные блоки по отдельности. Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform.

Управление Endpoint Sensor имеет следующие особенности:

- Если на компьютере установлено приложение Kaspersky Endpoint Security версий 11.0.0 – 11.3.0, вы можете настроить параметры Endpoint Sensor с помощью политики. Подробнее о настройке параметров Endpoint Sensor с помощью политики см. в справке Kaspersky Endpoint Security предыдущих версий.
- Если на компьютере установлено приложение Kaspersky Endpoint Security версии 11.4.0 и выше, настроить параметры Endpoint Sensor с помощью политики невозможно.

Endpoint Sensor устанавливается на клиентских компьютерах. На этих компьютерах компонент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Endpoint Sensor передает информацию на сервер KATA.

Функциональность компонента доступна для следующих операционных систем:

- Windows 7 Service Pack 1 Home / Professional / Enterprise;
- Windows 8.1.1 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-разрядная);
- Windows Server 2012 Foundation / Standard / Enterprise (64-разрядная);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64-разрядная);
- Windows Server 2016 Essentials / Standard (64-разрядная).

Подробную информацию о работе KATA см. в справке Kaspersky Anti Targeted Attack Platform.

Sandbox

В Kaspersky Endpoint Security для Windows включен встроенный агент для интеграции с решением Kaspersky Sandbox. *Sandbox* обнаруживает и автоматически блокирует сложные угрозы на компьютерах. Sandbox анализирует поведение объектов для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации. Sandbox выполняет анализ и проверку объектов на специальных серверах с развернутыми виртуальными образами операционных систем Microsoft Windows (серверы Sandbox). Подробнее о решении см. в справке Kaspersky Sandbox и справке Kaspersky Anti Targeted Attack Platform.

Начиная с версии Kaspersky Endpoint Security для Windows 12.7 в приложении добавлена поддержка компонента Sandbox, который входит в состав решения Kaspersky Anti Targeted Attack Platform. В отличие от решения Kaspersky Sandbox компонент KATA Sandbox позволяет проверять файлы не только в автоматическом режиме, но и вручную из контекстного меню файла.

Для работы KATA Sandbox должно быть развернуто решение Kaspersky Anti Targeted Attack Platform версии 7.0 или выше.

Управление компонентом доступно только в Kaspersky Security Center Web Console. Управлять компонентом в Консоли администрирования (MMC) невозможно.

Параметры компонента Sandbox

Параметр	Описание
Режим интеграции	**Kaspersky Sandbox**. Интеграция с решением Kaspersky Sandbox. Приложение отправляет файлы на проверку в Kaspersky Sandbox только в автоматическом режиме. **KATA Sandbox**. Интеграция с компонентом Sandbox, который входит в состав решения Kaspersky Anti Targeted Attack Platform. Вы можете выбрать режим отправки файлов на проверку: • **Вручную**. Пользователь вручную отправляет файл на проверку из контекстного меню (**Отправить в Sandbox**). • **Автоматически**. Приложение автоматически обнаруживает объекты и отправляет их на проверку в Sandbox. • **Комбинированный**.
Настройки подключения к серверам	**Время ожидания (мсек.)**. Время ожидания соединения с сервером Sandbox (для Kaspersky Sandbox) или Central Node (для KATA). По истечению заданного времени ожидания Kaspersky Endpoint Security отправит запрос на следующий сервер. Вы можете увеличить время ожидания соединения с сервером, если у вас низкая скорость соединения или соединение нестабильно. Рекомендованное значение времени ожидания запроса не более 0,5 сек. **Очередь запросов**. Размер папки хранения очереди запросов. При отправке нескольких объектов на проверку в Sandbox приложение Kaspersky Endpoint Security создает очередь запросов. По умолчанию размер папки хранения очереди запросов ограничен 100 МБ. После достижения максимального размера Sandbox перестает добавлять новые запросы в очередь и отправляет соответствующее событие в Kaspersky Security Center. Вы можете настроить размер папки хранения очереди запросов в зависимости от конфигурации сервера. **TLS-сертификат сервера**. Для настройки доверенного соединения с сервером Sandbox (для Kaspersky Sandbox) или Central Node (для KATA) вам нужно подготовить TLS-сертификат. Далее вам нужно добавить сертификат на компьютер с помощью политики. Также вам нужно добавить сертификат на сервер Sandbox (для Kaspersky Sandbox) или Central Node (для KATA). **Использовать двустороннюю аутентификацию** (только для KATA Sandbox). Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.
Подключение к серверам Sandbox	**Kaspersky Sandbox**. Параметры подключения к серверам Sandbox. На серверах развернуты виртуальные образы операционных систем Microsoft Windows, в которых запускаются проверяемые объекты. Вы можете ввести IP-адрес (IPv4 или IPv6) или полное доменное имя. **KATA Sandbox**. Параметры подключения к серверу Central Node. Central Node выбирает оптимальные параметры для проверки и обеспечивает распределение нагрузки между серверами Sandbox.
Действие при обнаружении угрозы	**Копию поместить на карантин, объект удалить**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удаляет вредоносный объект, обнаруженный на компьютере. Перед удалением объекта Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин. **Запустить проверку важных областей**. Если выбран этот вариант действия, то Kaspersky Endpoint Security запускает задачу *Проверка важных областей*. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы. **Создать задачу поиска IOC**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически создает задачу *Поиск IOC (автономная задача поиска IOC)*. Вы можете настроить режим запуска задачи, область поиска и действие при обнаружении IOC (*Копию поместить на карантин, объект удалить* или *Запустить проверку важных областей*). Для настройки других параметров задачи *Поиск IOC* перейдите в свойства задачи.
Область поиска IOC	**Важные файловые области**. Если выбран этот вариант, Kaspersky Endpoint Security выполняет поиск IOC только в важных файловых областях компьютера: память ядра и загрузочные секторы. **Файловые области на системном диске компьютера**. Если выбран этот вариант, Kaspersky Endpoint Security выполняет поиск IOC на системном диске компьютера.
Запуск задачи поиска IOC	**Вручную**. Режим запуска, при котором вы запускаете задачу *Поиск IOC* вручную в удобное для вас время. **Автоматически**. Режим запуска, при котором Kaspersky Endpoint Security запускает задачу *Поиск IOC* автоматически после обнаружения угрозы. **Выполнять только во время простоя компьютера**. Режим запуска, при котором Kaspersky Endpoint Security запускает задачу *Поиск IOC*, если включена экранная заставка или компьютер заблокирован. Если пользователь разблокировал компьютер, Kaspersky Endpoint Security приостанавливает выполнение задачи. Таким образом, приложение может выполнять задачу несколько дней.

Managed Detection and Response

Kaspersky Endpoint Security для Windows поддерживает работу с решением Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* – решение, которое автоматически обнаруживает и анализирует инциденты безопасности в вашей инфраструктуре. Для этого MDR использует данные телеметрии, полученные от конечных точек, и машинное обучение. Данные об инцидентах MDR передает экспертам "Лаборатории Касперского". Далее эксперты могут самостоятельно обработать инцидент и, например, добавить новую запись в антивирусные базы. Или эксперты могут дать рекомендации по обработке инцидента и, например, предложить изолировать компьютер от сети. Подробную информацию о работе решения см. в справке Kaspersky Managed Detection and Response.

Параметры компонента Managed Detection and Response

Параметр	Описание
Конфигурационный файл MDR	BLOB-файл содержит идентификатор клиента и информацию о лицензии Kaspersky Managed Detection and Response. BLOB-файл находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробную информацию о BLOB-файле см. в справке Kaspersky Managed Detection and Response.

Endpoint Detection and Response

В Kaspersky Endpoint Security для Windows включен встроенный агент для работы решения Kaspersky Endpoint Detection and Response Optimum (далее также "EDR Optimum"). Начиная с версии Kaspersky Endpoint Security для Windows 11.8.0 в приложение добавлен встроенный агент для работы решения Kaspersky Endpoint Detection and Response Expert (далее также "EDR Expert"). *Решения Kaspersky Endpoint Detection and Response* – решения, предназначенные для защиты IT-инфраструктуры организации от сложных кибернетических угроз. Функционал решений сочетает автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для противодействия сложным атакам, в том числе новым эксплойтам (exploits), программам-вымогателям (ransomware), бесфайловым атакам (fileless attacks), а также методам, использующим законные системные инструменты. EDR Expert предлагает пользователю больше функций для мониторинга и реагирования на угрозы информационной безопасности, чем EDR Optimum. Подробнее о решениях см. в справке Kaspersky Endpoint Detection and Response Optimum и в справке Kaspersky Endpoint Detection and Response Expert.

Kaspersky Endpoint Detection and Response выполняет обзор и анализ развития угрозы и предоставляет *Сотруднику службы безопасности* или *Администратору* информацию о потенциальной атаке, необходимую для принятия своевременных действий по реагированию. Kaspersky Endpoint Detection and Response показывает детали алерта в отдельном окне. *Алерт* – это событие в ИТ-инфраструктуре организации, которое приложение отметило как необычное или подозрительное и которое может представлять угрозу безопасности ИТ-инфраструктуры организации. *Детали алерта* – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum и в справке Kaspersky Endpoint Detection and Response Expert.

Вы можете настроить параметры компонента Endpoint Detection and Response Optimum в Web Console и Cloud Console. Параметры компонента Endpoint Detection and Response Expert (cloud) доступны только в Cloud Console.

Параметр	Описание
Включить расширенное логирование активности в системе	Расширенный сбор телеметрии позволяет более точно определять индикаторы компрометации, но требует больше ресурсов компьютера. Для ретроспективного поиска IOC рекомендуется включить расширенный сбор телеметрии на компьютере. *Ретроспективный поиск IOC* – это режим работы задачи *Поиск IOC*, при котором Kaspersky Endpoint Security выполняет поиск индикаторов компрометации по данным, полученным за определенный интервал времени. Режим предназначен для поиска индикаторов компрометации по телеметрии защищаемого компьютера, такой как сетевая активность, процессы, файлы и другие. Если расширенный сбор телеметрии выключен, то Kaspersky Endpoint Security может выполнять ротацию данных об обнаруженных индикаторах компрометации.
Сетевая изоляция	Автоматическая изоляция компьютера от сети в результате реагирования на обнаруженные угрозы. После включения Сетевой изоляции приложение разрывает все активные соединения и блокирует все новые соединения TCP/IP на компьютере. Приложение оставляет активными только следующие соединения: • соединения, указанные в исключениях из Сетевой изоляции; • соединения, инициированные службами Kaspersky Endpoint Security; • соединения, инициированные Агентом администрирования Kaspersky Security Center.
Разблокировать автоматически изолированное устройство через (часы)	Сетевая изоляция может быть выключена автоматически по истечении заданного периода времени или вручную. По умолчанию, Kaspersky Endpoint Security выключает Сетевую изоляцию через 5 часов после начала изоляции.
Исключения из сетевой изоляции	Список правил исключений из Сетевой изоляции. Сетевые соединения, подпадающие под заданные правила, не будут заблокированы на компьютерах после включения Сетевой изоляции. Для настройки исключений из Сетевой изоляции в приложении доступен список *стандартных сетевых профилей*. По умолчанию в исключения входят сетевые профили, состоящие из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент. Также вы можете изменить параметры стандартных сетевых профилей или задать исключения вручную. Исключения, заданные в свойствах политики, применяются, только если Сетевая изоляция включена приложением автоматически, в результате реагирования на обнаружение угрозы. Исключения, заданные в свойствах компьютера, применяются, только если Сетевая изоляция включена вручную в свойствах компьютера в консоли Kaspersky Security Center или в деталях алерта.
Запрет запуска	Контроль запуска исполняемых файлов и скриптов, а также открытия файлов офисного формата. Например, вы можете запретить запуск приложений, использование которых считается небезопасным, на выбранном компьютере. Запрет запуска объектов поддерживает определенный набор расширений файлов офисного формата и определенный набор интерпретаторов скриптов. Для работы Запрета запуска объектов вам нужно добавить правила запрета запуска объектов. *Правило запрета запуска* – это набор критериев, которые приложение учитывает при реагировании на запуск объекта, например, при блокировании запуска объекта. Приложение идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.
Действие при запуске или открытии объекта	**Заблокировать и записать в журнал событий**. В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета. Также приложение публикует в журнал событий Windows и Kaspersky Security Center событие о попытках запуска объектов или открытия документов. **Записать в журнал событий**. В этом режиме Kaspersky Endpoint Security публикует в журнал событий Windows и Kaspersky Security Center событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.
Правила запрета запуска	*Правило запрета запуска* – это набор критериев, которые приложение учитывает при реагировании на запуск объекта, например, при блокировании запуска объекта. Приложение идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.

Параметр	Описание
Cloud Sandbox	*Cloud Sandbox* – технология, которая позволяет обнаруживать сложные угрозы на компьютере. Kaspersky Endpoint Security автоматически отправляет обнаруженные файлы в Cloud Sandbox для анализа. Cloud Sandbox запускает эти файлы в изолированной среде для выявления вредоносной активности и принимает решение о репутации этих файлов. Далее данные об этих файлах попадают в Kaspersky Security Network. Таким образом, если Cloud Sandbox обнаружил вредоносный файл, Kaspersky Endpoint Security выполнит действие для устранения угрозы на всех компьютерах, на которых обнаружит этот файл. Технология Cloud Sandbox включена постоянно и доступна всем пользователям Kaspersky Security Network независимо от типа лицензии, которую вы используете. Если флажок установлен, Kaspersky Endpoint Security включит счетчик угроз, обнаруженных с помощью Cloud Sandbox, в главном окне приложения в разделе **Технологии обнаружения угроз**. Также Kaspersky Endpoint Security будет указывать технологию обнаружения угроз Cloud Sandbox в событиях приложения и в *Отчет об угрозах* в консоли Kaspersky Security Center.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security для Windows поддерживает работу с решением Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* – решение для кибербезопасности бизнеса, которое включает в себя приложения "Лаборатории Касперского", с помощью которых организация получает возможность защититься от большинства киберрисков и покрыть основные сценарии распространения угроз. Компоненты EDR Expert (on-premises) развернуты на единой платформе управления Open Single Management Platform (OSMP). Платформа обеспечивает выполнение кросс-программных сценариев в рамках единого интерфейса и позволяет интегрировать приложения "Лаборатории Касперского" и приложения сторонних производителей в единую систему безопасности.

Один из центральных элементов решения – *SIEM*. SIEM позволяет отслеживать события, полученные от всех компонентов, и выполняет взаимную корреляцию этих событий с помощью готовых и пользовательских правил. На основании журналов и телеметрии, полученных от инфраструктуры организации, EDR Expert (on-premises) автоматически выявляет атаки и позволяет проводить расследование инцидентов с помощью единого графа расследования, который комбинирует все собираемые в EDR Expert (on-premises) события – как от приложений "Лаборатории Касперского", так и от сторонних ИБ-продуктов.

Для реагирования на сложные инциденты EDR Expert (on-premises) использует предустановленные и пользовательские сценарии. Также доступны действия по реагированию от приложений сторонних производителей и сценарии реагирования, в которых задействовано несколько приложений.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security для Windows поддерживает работу с компонентом Kaspersky Endpoint Detection and Response в составе решения Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* – решение, предназначенное для своевременного обнаружения сложных угроз, таких как целевые атаки, сложные постоянные угрозы (англ. Advanced Persistent Threat, APT), атаки "нулевого дня" и другие. Kaspersky Anti Targeted Attack Platform включает в себя три функциональных блока:

- Kaspersky Anti Targeted Attack (далее также "*KATA*");
- Kaspersky Endpoint Detection and Response (далее также "*EDR (KATA)*");
- Network Detection and Response (далее также "*NDR (KATA)*").

Вы можете приобрести все функциональные блоки или приобрести функциональные блоки по отдельности. Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform.

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

Настройка интеграции с EDR (KATA) и NDR (KATA) выполняется в консоли Kaspersky Security Center. Дальнейшее управление встроенным агентом осуществляется в консоли Kaspersky Anti Targeted Attack Platform, включая запуск задач, управление объектами на карантине, просмотр отчетов и другие действия.

Параметры Endpoint Detection and Response Expert (on-premises)

Параметр	Описание
Подключение к серверам сбора телеметрии	*Сервер сбора телеметрии* – сервер, входящий в состав SIEM, который предназначен для сбора, нормализации, корреляции, анализа и хранения данных о событиях на компьютере. Настройте следующие параметры для подключения к серверам сбора телеметрии (KUMA): • **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу. • **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером. Вы можете получить TLS-сертификат в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером. Для использования двусторонней аутентификации вам нужно в параметрах сервера включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)). После настройки параметров сервера вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер. Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.
Адрес и **Порт** (серверы сбора телеметрии)	Параметры подключения к серверам сбора телеметрии. Вы можете ввести IP-адрес (IPv4 или IPv6). Вы можете добавить несколько адресов сервера сбора телеметрии. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.
Отправлять телеметрию на серверы сбора телеметрии	Функция позволяет полностью выключить отправку телеметрии на сервер KATA. Например, если вы используете Kaspersky Anti Targeted Attack Platform совместно с другим решением, которое также использует телеметрию, вы можете выключить отправку телеметрии для KATA (EDR). Это позволит оптимизировать нагрузку на серверы для этих решений. Если у вас развернуто решение Managed Detection and Response и KATA (EDR), вы можете использовать телеметрию MDR, а создавать задачи реагирования на угрозы в KATA (EDR). • **Отправлять телеметрию только с IOA**. Функция позволяет оптимизировать отправку телеметрии на сервер и отправлять только телеметрию с IOA. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию *потоковой проверки*, которая позволяет отслеживать такие события в режиме реального времени. • **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд. • **Ограничить количество пакетов событий в рамках одной передачи**. Приложение выполняет синхронизацию с сервером при заполнении буфера событиями. По умолчанию установлено значение 1024 события. Функция позволяет выключить буферизацию событий перед синхронизацией с сервером.
Включить регулирование количества запросов	Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события. Настройте параметры отправки телеметрии: • **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час. • **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Endpoint Security восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.
Отправлять запрос на синхронизацию на сервер каждые (мин.)	Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Endpoint Security передает данные об изменениях в параметрах приложения и задачах.

Параметр	Описание
Подключение к серверам реагирования	*Сервер реагирования* – сервер, который предназначен для приема и проверки данных, исследования поведения объектов, а также публикации результатов исследования. Настройте следующие параметры для подключения к серверам реагирования: • **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу. • **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером. Вы можете получить TLS-сертификат в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером. Для использования двусторонней аутентификации вам нужно в параметрах сервера включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)). После настройки параметров сервера вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.
Адрес и **Порт** (серверы реагирования)	Параметры подключения к серверам реагирования. Вы можете ввести IP-адрес (IPv4 или IPv6). Вы можете добавить несколько адресов сервера сбора телеметрии. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.

Параметры Endpoint Detection and Response (KATA)

Параметр	Описание
Отправлять запрос на синхронизацию на сервер каждые (мин.)	Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Endpoint Security передает данные об изменениях в параметрах приложения и задачах.
Подключение к серверам KATA	Настройте следующие параметры для подключения к серверу Central Node: • **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу Central Node. • **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). • **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер. Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.
Адрес и **Порт** (серверы KATA)	Параметры подключения к серверам Kaspersky Anti Targeted Attack Platform. Введите IP-адрес сервера Central Node (IPv4 или IPv6) и порт подключения к серверу. Вы можете добавить несколько адресов сервера Central Node. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.
Отправлять телеметрию в KATA	Функция позволяет полностью выключить отправку телеметрии на сервер KATA. Например, если вы используете Kaspersky Anti Targeted Attack Platform совместно с другим решением, которое также использует телеметрию, вы можете выключить отправку телеметрии для KATA (EDR). Это позволит оптимизировать нагрузку на серверы для этих решений. Если у вас развернуто решение Managed Detection and Response и KATA (EDR), вы можете использовать телеметрию MDR, а создавать задачи реагирования на угрозы в KATA (EDR). Настройте параметры отправки телеметрии: • **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд. • **Максимальное количество пакетов событий**. Приложение выполняет синхронизацию с сервером при заполнении буфера событиями. По умолчанию установлено значение 1024 события.

Параметр	Описание
Включить регулирование количества запросов	Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события. Настройте параметры отправки телеметрии: • **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час. • **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Endpoint Security восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.

Network Detection and Response (KATA)

Kaspersky Endpoint Security для Windows поддерживает работу с компонентом Kaspersky Network Detection and Response в составе решения Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* – решение, предназначенное для своевременного обнаружения сложных угроз, таких как целевые атаки, сложные постоянные угрозы (англ. Advanced Persistent Threat, APT), атаки "нулевого дня" и другие. Kaspersky Anti Targeted Attack Platform включает в себя три функциональных блока:

- Kaspersky Anti Targeted Attack (далее также "*KATA*");
- Kaspersky Endpoint Detection and Response (далее также "*EDR (KATA)*");
- Network Detection and Response (далее также "*NDR (KATA)*").

Вы можете приобрести все функциональные блоки или приобрести функциональные блоки по отдельности. Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform.

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

Настройка интеграции с EDR (KATA) и NDR (KATA) выполняется в консоли Kaspersky Security Center. Дальнейшее управление встроенным агентом осуществляется в консоли Kaspersky Anti Targeted Attack Platform, включая запуск задач, управление объектами на карантине, просмотр отчетов и другие действия.

Параметр	Описание
Настройки подключения к серверам	**Время ожидания (сек.)**. Максимальное время ожидания ответа от Сервера интеграции. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому Серверу интеграции. **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер. Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.
Адрес и **Порт**	Параметры подключения к серверам Kaspersky Anti Targeted Attack Platform. Введите IP-адрес сервера Central Node (IPv4 или IPv6) и порт подключения к серверу. Вы можете добавить несколько адресов сервера Central Node. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.
Отправлять запрос на синхронизацию на сервер NDR каждые (мин.)	Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Endpoint Security передает данные об изменениях в параметрах приложения и задачах.
Максимальная задержка отправки событий (сек.)	Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд.
Включить регулирование количества запросов	Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события.
Максимальное количество событий в час	Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.
Процент превышения лимита событий	Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Endpoint Security восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.

Интеграция с KUMA

Kaspersky Endpoint Security для Windows поддерживает работу с решением Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* – решение класса SIEM для управления информацией о безопасности и событиями безопасности в ИТ-инфраструктуре организации. KUMA позволяет обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб организации.

Параметр	Описание
Коннекторы агентов KUMA	*Коннекторы* используются для получения событий от источников, чтобы в дальнейшем отправить эти события в KUMA. KUMA приводит эти события к общему виду, удобному для поиска корреляций, а также для хранения и ручного анализа. Kaspersky Endpoint Security поддерживает следующие типы коннекторов: • **file**. Коннекторы с типом file используются для получения данных из текстовых файлов. • **tcp**. Коннекторы с типом tcp используются для пассивного получения событий по протоколу TCP. • **udp**. Коннекторы с типом udp используются для пассивного получения событий по протоколу UDP. • **http**. Коннекторы с типом http используются для получения событий по протоколу HTTP. • **wec**. Коннекторы с типом wec используются для получения данных с помощью Windows Event Forwarding (WEF) и Windows Event Collector (WEC) или локальных журналов ОС компьютера. • **etw**. Коннекторы с типом etw используются для получения расширенных журналов DNS-серверов.

Точки назначения агентов KUMA	*Точки назначения* задают сетевые параметры для передачи событий от источников в KUMA. Kaspersky Endpoint Security поддерживает передачу событий только по протоколу HTTP.
	Дополнительные параметры точки назначения:
	• **Обработчики**. Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
	• Размер буфера (байт). Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
	• **Интервал очистки буфера (сек.)**. Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
	• **Ограничить размер дискового буфера**. Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
	• **Режим TLS**. Режим шифрования TLS. Доступные значения:
	  • **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию.
	  • **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации.
	  • **Нестандартный PFX с аутентификацией клиента** – использовать шифрование TLS с PFX-секретом. В этом режиме выполняется аутентификация клиента по сертификату. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации.
	• **Прокси-сервер**.
	• **Политика выбора URL**. Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов:
	  • **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию.
	  • **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него.
	  • **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле Размер буфера, а также указать интервал в секундах для отправки событий в точку назначения в поле Интервал очистки буфера.
	• **Проверка работоспособности**. Переключатель, включающий проверку работоспособности. По умолчанию этот переключатель выключен.
	• **Путь проверки работоспособности**. URL-адрес для отправки запросов для получения данных о работоспособности системы, с которой ресурс точки назначения устанавливает связь.
	• **Время ожидания (сек.)**. Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.

Прокси-серверы агентов KUMA	*Прокси-серверы* используются для хранения параметров конфигурации прокси-серверов, например в точках назначения. Поддерживается тип http.

Параметр	Описание
События Windows	Параметры подключения к серверам KUMA: • **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд. • **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера KUMA (по умолчанию 5 сек.). По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу KUMA. • **Сертификат сервера**. TLS-сертификат предназначен для установки доверенного соединения с сервером KUMA. Вы можете получить TLS-сертификат в консоли Kaspersky Unified Monitoring and Analysis Platform (см. инструкцию в справке Kaspersky Unified Monitoring and Analysis Platform). Для доверенного соединения вам нужно в консоли KUMA в параметрах коннектора типа tcp выбрать режим TLS **Нестандартный PFX** (см. параметры коннектора типа tcp в справке Kaspersky Unified Monitoring and Analysis Platform). • **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между KES и KUMA. Для использования двусторонней аутентификации вам нужно в консоли KUMA в параметрах коннектора выбрать режим TLS **Нестандартный PFX с аутентификацией клиента** (см. параметры коннектора в справке Kaspersky Unified Monitoring and Analysis Platform). Далее вам нужно загрузить сертификат сервера и установить пароль для защиты криптоконтейнера. Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно. Вы можете добавить несколько адресов сервера KUMA. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.

Полнодисковое шифрование

Вы можете выбрать технологию шифрования: Шифрование диска Kaspersky или Шифрование диска BitLocker (далее также "BitLocker").

Шифрование диска Kaspersky

Шифрование диска Kaspersky не поддерживается на компьютерах с Arm-архитектурой.

После шифрования системных жестких дисков при последующем включении компьютера доступ к ним, а также загрузка операционной системы возможны только после прохождения процедуры аутентификации с помощью Агента аутентификации. Для этого требуется ввести пароль токена или смарт-карты, подключенных к компьютеру, или имя и пароль учетной записи Агента аутентификации, созданной системным администратором локальной сети организации с помощью задачи *Управление учетными записями Агента аутентификации*. Эти учетные записи основаны на учетных записях пользователей Microsoft Windows, под которыми пользователи выполняют вход в операционную систему. Также вы можете использовать технологию единого входа (англ. Single Sign-On, SSO), позволяющую осуществлять автоматический вход в операционную систему с помощью имени и пароля учетной записи Агента аутентификации.

Аутентификация пользователя в Агенте аутентификации может выполняться двумя способами:

- путем ввода имени и пароля учетной записи Агента аутентификации, созданной администратором локальной сети организации средствами Kaspersky Security Center;
- путем ввода пароля подключенного к компьютеру токена или смарт-карты.

Использование токена или смарт-карты доступно, только если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES256. Если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES56, то в добавлении файла электронного сертификата в команду будет отказано.

Шифрование диска BitLocker

BitLocker – встроенная в операционную систему Windows технология шифрования. Kaspersky Endpoint Security позволяет контролировать и управлять Bitlocker с помощью Kaspersky Security Center. BitLocker шифрует логический том. Шифрование съемных дисков с помощью BitLocker невозможно. Подробнее о BitLocker см. в документации Microsoft.

При шифровании диска BitLocker помещает загрузчик и другие служебные файлы в системный раздел (англ. system partition). Этот раздел не зашифрован. Операционная система создает системный раздел автоматически при установке Windows. Если перед установкой Windows диск полностью размечен, операционная система не сможет создать системный раздел. В этом случае при запуске шифрования диска BitLocker операционная система предложит пользователю разметить диск снова и создать системный раздел. После создания системного раздела операционная система запустит шифрование диска BitLocker.

BitLocker обеспечивает безопасность хранения ключей доступа с помощью доверенного платформенного модуля. *Доверенный платформенный модуль* (англ. Trusted Platform Module, TPM) – микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины. Использование TPM является самым безопасным способом хранения ключей доступа BitLocker, так как TPM позволяет проверять целостность операционной системы. На компьютерах без TPM вы также можете зашифровать диски. При этом ключ доступа будет зашифрован паролем. Таким образом, BitLocker использует следующие способы аутентификации:

- TPM.
- TPM и PIN-код.
- Пароль.

После шифрования системного жесткого диска для загрузки операционной системы пользователю нужно пройти процедуру аутентификации BitLocker. После прохождения процедуры аутентификации BitLocker будет доступен вход в систему. BitLocker не поддерживает технологию единого входа (SSO).

После шифрования диска BitLocker создает ключ восстановления. Kaspersky Endpoint Security отправляет ключ восстановления в Kaspersky Security Center, чтобы вы имели возможность восстановить доступ к диску, если пользователь, например, забыл пароль.

Если пользователь самостоятельно зашифровал диск с помощью BitLocker, Kaspersky Endpoint Security отправит ключ восстановления и информацию о шифровании диска в Kaspersky Security Center.

Если вы используете групповые политики для Windows, выключите управление BitLocker в параметрах политики. Параметры политики для Windows могут противоречить параметрам политики Kaspersky Endpoint Security. При шифровании диска могут возникнуть ошибки.

Параметр	Описание
Режим шифрования	**Шифровать все жесткие диски**. Если выбран этот элемент, то при применении политики приложение шифрует все жесткие диски. Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой установлено приложение. **Расшифровывать все жесткие диски**. Если выбран этот элемент, то при применении политики приложение расшифровывает все зашифрованные ранее жесткие диски. **Оставлять без изменений**. Если выбран этот элемент, то при применении политики приложение оставляет диски в прежнем состоянии. Если диск был зашифрован, то он остается зашифрованным, а если диск был расшифрован, то он остается расшифрованным. Этот элемент выбран по умолчанию.
Автоматически создавать учетные записи Агента аутентификации для пользователей при применении шифрования на компьютере	Если флажок установлен, приложение создает учетные записи Агента аутентификации на основе списков учетных записей Windows на компьютере. По умолчанию Kaspersky Endpoint Security использует все локальные и доменные учетные записи, с помощью которых пользователь выполнял вход в операционную систему за последние 30 дней.
Настройки создания учетных записей Агента аутентификации	**Все учетные записи компьютера**. Все учетные записи компьютера, которые когда-либо были активными. **Все доменные учетные записи компьютера**. Все учетные записи компьютера, которые принадлежат какому-либо домену и которые когда-либо были активными. **Все локальные учетные записи компьютера**. Все локальные учетные записи компьютера, которые когда-либо были активными. **Служебная учетная запись с одноразовым паролем**. Служебная учетная запись нужна для доступа к компьютеру в случаях, когда пользователь, например, забыл пароль. Также вы можете использовать служебную учетную запись в качестве резервной учетной записи. Вам нужно указать имя учетной записи (по умолчанию `ServiceAccount`). Kaspersky Endpoint Security создаст пароль автоматически. Пароль вы можете посмотреть в консоли Kaspersky Security Center. **Локальный администратор**. Kaspersky Endpoint Security создает учетную запись Агента аутентификации для локального администратора компьютера. **Менеджер компьютера**. Kaspersky Endpoint Security создает учетную запись Агента аутентификации для учетной записи менеджера компьютера. Вы можете посмотреть какая учетная запись имеет роль менеджера компьютера в свойствах компьютера в Active Directory. По умолчанию роль менеджера компьютера не определена, то есть не соответствует ни одной учетной записи. **Активная учетная запись**. Kaspersky Endpoint Security автоматически создает учетную запись Агента аутентификации для учетной записи активной в момент выполнения шифрования диска.
Автоматически создавать учетные записи Агента аутентификации для всех пользователей на компьютере при входе	Если флажок установлен, приложение проверяет информацию об учетных записях Windows на компьютере перед запуском Агента аутентификации. Если Kaspersky Endpoint Security обнаружит учетную запись Windows, для которой нет учетной записи Агента аутентификации, приложение создаст новую учетную запись для доступа к зашифрованным дискам. Новая учетная запись Агента аутентификации будет иметь параметры по умолчанию: вход только по паролю, смена пароля при первой аутентификации. Таким образом, вам не нужно вручную добавлять учетные записи Агента аутентификации с помощью задачи *Управление учетными записями Агента аутентификации* для компьютеров с уже зашифрованными дисками.
Сохранять введенное в Агенте аутентификации имя пользователя	Если флажок установлен, то приложение сохраняет имя учетной записи Агента аутентификации. При последующей аутентификации в Агенте аутентификации под той же учетной записью имя учетной записи вводить не требуется.

Параметр	Описание
Шифровать только занятое пространство (сокращает время шифрования)	Флажок включает / выключает функцию, ограничивающую область шифрования только занятыми секторами жесткого диска. Это ограничение позволяет сократить время шифрования. Включение / выключение функции **Шифровать только занятое пространство (сокращает время шифрования)** после запуска шифрования не изменяет этого параметра до тех пор, пока жесткие диски не будут расшифрованы. Требуется установить или снять флажок до начала шифрования. Если флажок установлен, то шифруется только та часть жесткого диска, которая занята файлами. Kaspersky Endpoint Security зашифровывает новые данные автоматически по мере их добавления. Если флажок снят, то шифруется весь жесткий диск, в том числе остатки удаленных и отредактированных ранее файлов. Данную функцию рекомендуется применять для новых жестких дисков, данные которых не редактировались и не удалялись. Если вы применяете шифрование на уже используемом жестком диске, рекомендуется зашифровать весь жесткий диск. Это гарантирует защиту всех данных – даже удаленных, но потенциально восстанавливаемых. По умолчанию флажок снят.
Использовать Legacy USB Support (не рекомендуется)	Флажок включает / выключает функцию Legacy USB Support. *Legacy USB Support* – функция BIOS / UEFI, которая позволяет использовать USB-устройства (например, токен) на этапе загрузки компьютера до запуска операционной системы (BIOS-режим). Функция Legacy USB Support не влияет на поддержку USB-устройств после запуска операционной системы. Если флажок установлен, то будет включена поддержка USB-устройств на этапе начальной загрузки компьютера. При включенной функции Legacy USB Support Агент аутентификации в BIOS-режиме не поддерживает работу с токенами по USB. Функцию рекомендуется использовать только при возникновении проблемы несовместимости с аппаратным обеспечением и только для тех компьютеров, на которых возникла проблема.
Настройки паролей	Параметры надежности пароля учетной записи Агента аутентификации. При использовании технологии единого входа Агент аутентификации игнорирует требования к надежности пароля, заданные в Kaspersky Security Center. Вы можете задать требования к надежности пароля в параметрах операционной системы.
Использовать технологию единого входа (SSO)	Технология единого входа позволяет использовать одни и те же учетные данные для доступа к зашифрованным жестким дискам и для входа в операционную систему. Если флажок установлен, то для доступа к зашифрованным жестким дискам и последующего автоматического входа в операционную систему требуется ввести учетные данные доступа к зашифрованным дискам. Если флажок снят, то для доступа к зашифрованным жестким дискам и последующего входа в операционную систему требуется отдельно ввести учетные данные для доступа к зашифрованным жестким дискам и учетные данные пользователя в операционной системе.
Включить поддержку сторонних поставщиков учетных данных	Kaspersky Endpoint Security поддерживает стороннего поставщика учетных данных ADSelfService Plus. При работе со сторонними поставщиками учетных данных Агент аутентификации перехватывает пароль перед загрузкой операционной системы. Таким образом, при входе в Windows пользователю нужно ввести пароль только один раз. После входа в Windows пользователь может использовать возможности стороннего поставщика учетных данных, например, для аутентификации в сервисах организации. Также сторонние поставщики учетных данных позволяют пользователям самостоятельно сбрасывать пароль. В этом случае Kaspersky Endpoint Security обновит пароль для Агента аутентификации автоматически. Если вы используете стороннего поставщика учетных данных, который не поддерживается приложением, вы можете столкнуться с ограничениями в работе технологии единого входа.
Справка	**Аутентификация**. Справочный текст, который отображается в окне Агента аутентификации на этапе ввода учетных данных. **Смена пароля**. Справочный текст, который отображается в окне Агента аутентификации на этапе смены пароля для учетной записи Агента аутентификации. **Восстановление пароля**. Справочный текст, который отображается в окне Агента аутентификации на этапе восстановления пароля для учетной записи Агента аутентификации.

Параметр	Описание
Режим шифрования	**Шифровать все жесткие диски**. Если выбран этот элемент, то при применении политики приложение шифрует все жесткие диски. Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой установлено приложение. **Расшифровывать все жесткие диски**. Если выбран этот элемент, то при применении политики приложение расшифровывает все зашифрованные ранее жесткие диски. **Оставлять без изменений**. Если выбран этот элемент, то при применении политики приложение оставляет диски в прежнем состоянии. Если диск был зашифрован, то он остается зашифрованным, а если диск был расшифрован, то он остается расшифрованным. Этот элемент выбран по умолчанию.
Включить использование проверки подлинности BitLocker, требующей предзагрузочного ввода с клавиатуры на планшетах	Использование аутентификации, требующей ввода данных в предзагрузочной среде, даже если у платформы отсутствует возможность предзагрузочного ввода (например, у сенсорных клавиатур на планшетах). Сенсорная клавиатура планшетов недоступна в предзагрузочной среде. Для прохождения аутентификации BitLocker на планшетах пользователю необходимо подключить, например, USB-клавиатуру. Если флажок установлен, то использование аутентификации, требующей предзагрузочного ввода, разрешено. Рекомендуется использовать этот параметр только для устройств, у которых во время предварительной загрузки, помимо сенсорных клавиатур, имеются альтернативные средства ввода данных, например, USB-клавиатура. Если флажок снят, шифрование диска BitLocker на планшетах невозможно.
Использовать аппаратное шифрование (ОС Windows 8 и выше)	Если флажок установлен, то приложение применяет аппаратное шифрование. Это позволяет увеличить скорость шифрования и сократить использование ресурсов компьютера.
Шифровать только занятое пространство (ОС Windows 8 и выше)	Флажок включает / выключает функцию, ограничивающую область шифрования только занятыми секторами жесткого диска. Это ограничение позволяет сократить время шифрования. Включение / выключение функции **Шифровать только занятое пространство (сокращает время шифрования)** после запуска шифрования не изменяет этого параметра до тех пор, пока жесткие диски не будут расшифрованы. Требуется установить или снять флажок до начала шифрования. Если флажок установлен, то шифруется только та часть жесткого диска, которая занята файлами. Kaspersky Endpoint Security зашифровывает новые данные автоматически по мере их добавления. Если флажок снят, то шифруется весь жесткий диск, в том числе остатки удаленных и отредактированных ранее файлов. Данную функцию рекомендуется применять для новых жестких дисков, данные которых не редактировались и не удалялись. Если вы применяете шифрование на уже используемом жестком диске, рекомендуется зашифровать весь жесткий диск. Это гарантирует защиту всех данных – даже удаленных, но потенциально восстанавливаемых. По умолчанию флажок снят.

Параметр	Описание
Способ аутентификации	**Только пароль (ОС Windows 8 и выше)** Если выбран этот вариант, Kaspersky Endpoint Security запрашивает у пользователя пароль при обращении к зашифрованному диску. Этот вариант действия может быть выбран, если не используется доверенный платформенный модуль (TPM). **Доверенный платформенный модуль (TPM)** Если выбран этот вариант, BitLocker использует доверенный платформенный модуль (TPM). *Доверенный платформенный модуль* (англ. Trusted Platform Module, TPM) – микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины. Для компьютеров под управлением операционных систем Windows 7 и Windows Server 2008 R2 доступно только шифрование с использованием модуля TPM. Если модуль TPM не установлен, шифрование BitLocker невозможно. Использование пароля на этих компьютерах не поддерживается. Устройство, оснащенное доверенным платформенным модулем, может создавать ключи шифрования, которые могут быть расшифрованы только с его помощью. Доверенный платформенный модуль шифрует ключи шифрования собственным корневым ключом хранилища. Корневой ключ хранилища хранится внутри доверенного платформенного модуля. Это обеспечивает дополнительную степень защиты ключей шифрования от попыток взлома. Этот вариант действия выбран по умолчанию. Вы можете установить дополнительную защиту для доступа к ключу шифрования и зашифровать ключ паролем или PIN: • **Использовать PIN для TPM**. Если флажок установлен, пользователь может использовать PIN-код для получения доступа к ключу шифрования, который хранится в доверенном платформенном модуле (TPM). Если флажок снят, пользователю запрещено использовать PIN-код. Для получения доступа к ключу шифрования пользователь использует пароль. • **Доверенный платформенный модуль (TPM), если он недоступен, то пароль**. Если выбран этот вариант, то при отсутствии доверенного платформенного модуля (TPM) пользователь может получить доступ к ключам шифрования с помощью пароля. Если флажок снят и модуль TPM недоступен, то полнодисковое шифрование не запускается. Для выбранного способа аутентификации необходимо настроить требования к паролю или PIN-коду: • **Минимальная длина PIN-а (символов)** (по умолчанию 6). • **Минимальная длина пароля (символов)** (по умолчанию 8). • **Максимальное количество хранимых паролей / PIN** (по умолчанию 5). • **Ограничить срок действия пароля / PIN-а для TPM (дни)** (по умолчанию выключено). • **Использовать расширенный PIN (с буквами и цифрами)**. *Расширенный PIN-код* кроме цифр позволяет использовать другие символы: заглавные и строчные латинские буквы, специальные символы и пробел. По умолчанию выключено.
Автоматически пересоздавать ключ восстановления (дни)	Автоматическое обновление пароля для восстановления доступа к диску, защищенному BitLocker. Если флажок установлен, задайте срок действия пароля ключа восстановления. Эта функция позволяет исключить повторное использование пароля ключа восстановления.

Шифрование файлов

Шифрование файлов не поддерживается на компьютерах с Arm-архитектурой.

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов.

Вы можете сформировать списки из файлов по расширению или группам расширений и из папок, расположенных на локальных дисках компьютера, а также создать правила шифрования файлов, создаваемых отдельными приложениями. После применения политики приложение Kaspersky Endpoint Security шифрует и расшифровывает следующие файлы:

- файлы, отдельно добавленные в списки для шифрования и расшифровки;
- файлы, хранящиеся в папках, добавленных в списки для шифрования и расшифровки;
- файлы, создаваемые отдельными приложениями.

Шифрование файлов имеет следующие особенности:

- Kaspersky Endpoint Security шифрует / расшифровывает стандартные папки только для локальных профилей пользователей (англ. local user profiles) операционной системы. Kaspersky Endpoint Security не шифрует и не расшифровывает стандартные папки для перемещаемых профилей пользователей (англ. roaming user profiles), обязательных профилей пользователей (англ. mandatory user profiles), временных профилей пользователей (англ. temporary user profiles), а также перенаправленные папки.
- Kaspersky Endpoint Security не выполняет шифрование файлов, изменение которых может повредить работе операционной системы и установленных приложений. Например, в список исключений из шифрования входят следующие файлы и папки со всеми вложенными в них папками:
  - %WINDIR%;
  - %PROGRAMFILES% и %PROGRAMFILES(X86)%;
  - файлы реестра Windows.

  Список исключений из шифрования недоступен для просмотра и изменения. Файлы и папки из списка исключений из шифрования можно добавить в список для шифрования, но при выполнении шифрования файлов они не будут зашифрованы.

Параметры компонента Шифрование файлов

Параметр	Описание
Режим шифрования	**Оставлять без изменений**. Если выбран этот элемент, то Kaspersky Endpoint Security оставляет файлы и папки в том же состоянии – не шифрует и не расшифровывает их. **Согласно правилам**. Если выбран этот элемент, то Kaspersky Endpoint Security шифрует файлы и папки согласно правилам шифрования, расшифровывает файлы и папки согласно правилам расшифровки, а также регулирует доступ приложений к зашифрованным файлам согласно правилам для приложений. **Расшифровывать все**. Если выбран этот элемент, то Kaspersky Endpoint Security расшифровывает все зашифрованные файлы и папки.
Шифрование	На вкладке отображаются правила шифрования файлов, хранящихся на локальных дисках. Вы можете добавить файлы следующим образом: • **Стандартные папки**. Kaspersky Endpoint Security позволяет добавить следующие области: **Документы**. Файлы в стандартной папке операционной системы *Документы*, а также вложенные папки. **Избранное**. Файлы в стандартной папке операционной системы *Избранное*, а также вложенные папки. **Рабочий стол**. Файлы в стандартной папке операционной системы *Рабочий стол*, а также вложенные папки. **Временные файлы**. Временные файлы, связанные с работой установленных на компьютере приложений. Например, приложения Microsoft Office создают временные файлы с резервными копиями документов. **Файлы Outlook**. Файлы, связанные с работой почтового клиента Outlook: файлы данных (PST), автономные файлы данных (OST), файлы автономной адресной книги (OAB) и файлы персональной адресной книги (PAB). • **Папку вручную**. Вы можете ввести путь к папке. При добавлении пути к папке следует использовать следующие правила: Используйте переменную окружения (например, `%FOLDER%\UserFolder\`). Вы можете использовать переменную окружения только один раз и только в начале пути. Не используйте относительные пути. Не используйте символы `*` и `?`. Не используйте UNC-пути. Используйте `;` или `,` в качестве разделительного символа. • **Файлы по расширению**. Вы можете выбрать группы расширений из списка, например, группу расширений *Архивы*. Также вы можете добавить расширение файла вручную.

Параметр	Описание
Расшифровка	На вкладке отображаются правила расшифровки файлов, хранящихся на локальных дисках.
Правила для приложений	На вкладке отображается таблица с правилами доступа приложений к зашифрованным файлам и правилами шифрования файлов, создаваемых и изменяемых отдельными приложениями.
Зашифрованные архивы	Параметры сложности пароля при создании зашифрованных архивов.

Шифрование съемных дисков

Шифрование съемных дисков не поддерживается на компьютерах с Arm-архитектурой.

Этот компонент доступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов.

Kaspersky Endpoint Security поддерживает шифрование файлов в файловых системах FAT32 и NTFS. Если к компьютеру подключен съемный диск с неподдерживаемой файловой системой, то шифрование этого съемного диска завершается с ошибкой и Kaspersky Endpoint Security устанавливает статус доступа "только чтение" для этого съемного диска.

Для защиты данных на съемных дисках вы можете использовать следующие виды шифрования:

- Полнодисковое шифрование (англ. Full Disk Encryption, FDE).

  Шифрование всего съемного диска, включая файловую систему.

  Получить доступ к зашифрованным данным вне корпоративной сети невозможно. Также невозможно получить доступ к зашифрованным данным внутри корпоративной сети, если компьютер не подключен к Kaspersky Security Center ("гостевой" компьютер).

- Шифрование файлов (англ. File Level Encryption, FLE).

  Шифрование только файлов на съемном диске. Файловая система при этом остается без изменений.

  Шифрование файлов на съемных дисках предоставляет возможность доступа к данным за пределами корпоративной сети с помощью специального режима – *портативный режим*.

Во время шифрования Kaspersky Endpoint Security создает мастер-ключ. Kaspersky Endpoint Security сохраняет мастер-ключ в следующих хранилищах:

- Kaspersky Security Center.
- Компьютер пользователя.

  Мастер-ключ зашифрован секретным ключом пользователя.

- Съемный диск.

  Мастер-ключ зашифрован открытым ключом Kaspersky Security Center.

После завершения шифрования данные на съемном диске доступны внутри корпоративной сети как при использовании обычного съемного диска без шифрования.

Получение доступа к зашифрованным данным

При подключении съемного диска с зашифрованными данными Kaspersky Endpoint Security выполняет следующие действия:

1. Проверяет наличие мастер-ключа в локальном хранилище на компьютере пользователя.

   Если мастер-ключ найден, пользователь получает доступ к данным на съемном диске.

   Если мастер-ключ не найден, Kaspersky Endpoint Security выполняет следующие действия:

   a. Отправляет запрос в Kaspersky Security Center.

      После получения запроса Kaspersky Security Center отправляет ответ, который содержит мастер-ключ.

   b. Kaspersky Endpoint Security сохраняет мастер-ключ в локальном хранилище на компьютере пользователя для дальнейшей работы с зашифрованным съемным диском.

2. Расшифровывает данные.

Особенности шифрования съемных дисков

Шифрование съемных дисков имеет следующие особенности:

- Политика с заданными параметрами шифрования съемных дисков формируется для определенной группы управляемых компьютеров. Поэтому результат применения политики Kaspersky Security Center с настроенным шифрованием / расшифровкой съемных дисков зависит от того, к какому компьютеру подключен съемный диск.

- Kaspersky Endpoint Security не выполняет шифрование / расшифровку файлов со статусом доступа "только чтение", хранящихся на съемных дисках.

- В качестве съемных дисков поддерживаются следующие типы устройств:

  - носители информации, подключаемые по шине USB;

  - жесткие диски, подключаемые по шинам USB и FireWire;

  - SSD-диски, подключаемые по шинам USB и FireWire.

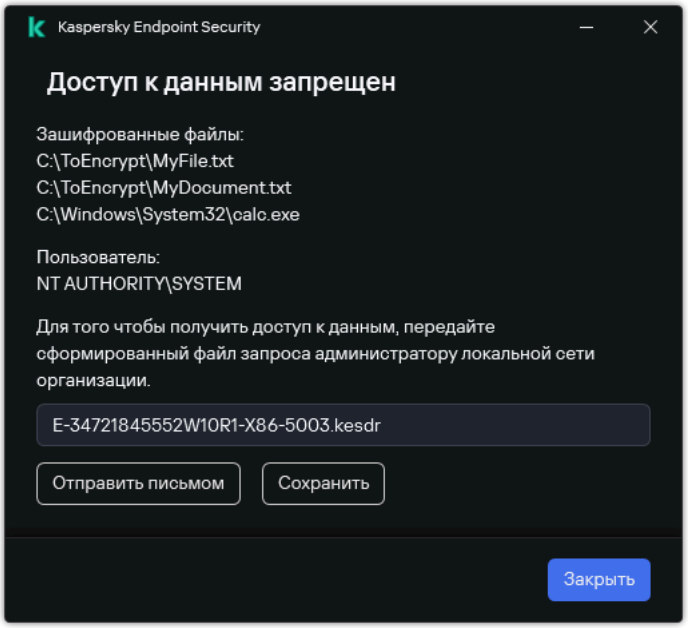
Параметр	Описание
Режим шифрования	**Шифровать весь съемный диск**. Если выбран этот элемент, то при применении политики с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security шифрует съемные диски по секторам, включая их файловые системы. **Шифровать все файлы**. Если выбран этот элемент, то при применении политики с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security шифрует все файлы, которые хранятся на съемных дисках. Уже зашифрованные файлы Kaspersky Endpoint Security повторно не шифрует. Содержимое файловой системы съемных дисков, включая имена зашифрованных файлов и структуру папок, остается доступным и не шифруется. **Шифровать только новые файлы**. Если выбран этот элемент, то при применении политики с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security шифрует на съемных дисках только те файлы, которые были добавлены или изменены после последнего применения политики Kaspersky Security Center. Этот режим шифрования может быть удобным, если пользователь использует съемный диск и в личных целях, и на работе. Режим шифрования позволяет оставлять без изменений все старые файлы и шифровать только те файлы, которые пользователь создает на рабочем компьютере с установленным приложением Kaspersky Endpoint Security и доступной функциональностью шифрования. Таким образом, доступ к личным файлам всегда открыт вне зависимости от того, установлено на компьютере приложение Kaspersky Endpoint Security с доступной функциональностью шифрования или нет. **Расшифровывать весь съемный диск**. Если выбран этот элемент, то при применении политики с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security расшифровывает все зашифрованные файлы, которые хранятся на съемных дисках, а также файловые системы съемных дисков, если они были зашифрованы. **Оставлять без изменений**. Если выбран этот элемент, то при применении политики приложение оставляет диски в прежнем состоянии. Если диск был зашифрован, то он остается зашифрованным, а если диск был расшифрован, то он остается расшифрованным. Этот элемент выбран по умолчанию.
Портативный режим	Флажок включает / выключает подготовку съемного диска, которая позволяет работать с хранящимися на этом съемном диске файлами на компьютерах вне корпоративной сети. Если флажок установлен, то при применении политики перед началом шифрования файлов на съемном диске Kaspersky Endpoint Security запрашивает у пользователя пароль. Пароль требуется для получения доступа к зашифрованным файлам на съемном диске на компьютерах вне корпоративной сети. Вы можете настроить сложность пароля. Портативный режим доступен для режимов **Шифровать все файлы** или **Шифровать только новые файлы**.
Шифровать только занятое пространство	Флажок включает / выключает режим шифрования, при котором шифруются только занятые секторы диска. Этот режим рекомендуется применять для новых дисков, данные которых не редактировались и не удалялись. Если флажок установлен, то шифруется только та часть диска, которая занята файлами. Kaspersky Endpoint Security зашифровывает новые данные автоматически по мере их добавления. Если флажок снят, то шифруется весь диск, в том числе остатки удаленных и отредактированных ранее файлов. Функция шифрования только занятого пространства доступна только для режима **Шифровать весь съемный диск**. Включение / выключение функции **Шифровать только занятое пространство** после запуска шифрования не изменяет этого параметра. Требуется установить или снять флажок до начала шифрования.

Правила, заданные вручную	Таблица устройств, для которых заданы отдельные правила шифрования. Вы можете создать правила шифрования для отдельных съемных дисков следующими способами:
	• Добавьте съемный диск из списка доверенных устройств Контроля устройств.
	• Добавьте съемный диск вручную:
	  • по идентификатору устройства (англ. Hardware ID, HWID);
	  • по модели устройства: идентификатор производителя (англ. Vendor ID, VID) и идентификатор продукта (англ. Product ID, PID).

Параметр	Описание
Разрешать шифрование съемных дисков в офлайн-режиме	Если флажок установлен, то Kaspersky Endpoint Security шифрует съемные диски даже при отсутствии связи с Kaspersky Security Center. Данные, необходимые для расшифровки съемных дисков, сохраняются при этом на жестком диске компьютера, к которому подключен съемный диск, и не передаются на Kaspersky Security Center. Если флажок снят, Kaspersky Endpoint Security не шифрует съемные диски, если связь с Kaspersky Security Center отсутствует.
Настройки паролей для шифрования / Портативный файловый менеджер	Параметры надежности пароля для портативного файлового менеджера.

Шаблоны (шифрование данных)

После шифрования данных Kaspersky Endpoint Security может запретить доступ к данным, например, из-за изменения инфраструктуры организации и смены Сервера администрирования Kaspersky Security Center. Если у пользователя нет доступа к зашифрованным данным, пользователь может запросить доступ к данным у администратора. Т.е. пользователю нужно передать файл запроса администратору. Далее пользователю нужно загрузить в Kaspersky Endpoint Security файл ответа, полученный от администратора. Kaspersky Endpoint Security позволяет запросить доступ к данным у администратора с помощью электронной почты (см. рис. ниже).



Запрос доступа к зашифрованным данным

Для сообщения об отсутствии доступа к зашифрованным данным предусмотрен шаблон. Для удобства пользователей вы можете заполнить следующие поля:

- **Кому**. Введите адрес электронной почты группы администраторов с правами на функции шифрования данных.
- **Тема**. Введите тему письма с запросом доступа к зашифрованным файлам. Вы можете, например, добавить теги для фильтрации сообщений.
- **Сообщение пользователя**. Если требуется измените содержание сообщения. Вы можете использовать переменные, чтобы получить необходимые данные (например, переменная %USER_NAME%).

Исключения

Доверенная зона – это сформированный администратором системы список объектов и приложений, которые Kaspersky Endpoint Security не контролирует в процессе работы.

Доверенную зону администратор системы формирует самостоятельно в зависимости от особенностей объектов, с которыми требуется работать, а также от приложений, установленных на компьютере. Включение объектов и приложений в доверенную зону может потребоваться, например, если Kaspersky Endpoint Security блокирует доступ к какому-либо объекту или приложению, в то время как вы уверены, что этот объект или приложение безвредны. Также администратор может разрешить пользователю формировать собственную локальную доверенную зону для отдельного компьютера. Таким образом, кроме общей доверенной зоны, сформированной в политике, пользователь может создавать собственные локальные списки исключений и доверенных приложений.

Начиная с версии Kaspersky Endpoint Security для Windows 12.5 вы можете добавить EDR-телеметрию в доверенную зону. Это позволяет оптимизировать данные, которые приложение отправляет на Сервер сбора телеметрии для решения Kaspersky Anti Targeted Attack Platform (EDR).

Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы приложения Kaspersky Endpoint Security на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager. То есть вам не нужно формировать доверенную зону вручную для работы приложения на серверах.

Начиная с версии Kaspersky Endpoint Security для Windows 12.8 добавлена установка приложения в режиме Легкого агента для защиты виртуальных сред. Предустановленные исключения из проверки и доверенные приложения позволяют быстро настроить работу приложения Kaspersky Endpoint Security в виртуальных средах Citrix и VMware.

Исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Endpoint Security не проверяет объект на вирусы и другие приложения, представляющие угрозу. Исключения из проверки позволяют работать с легальными приложениями, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие приложения не имеют вредоносных функций, но могут быть использованы злоумышленниками. Подробную информацию о легальных приложениях, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского".

В результате работы Kaspersky Endpoint Security такие приложения могут быть заблокированы. Чтобы избежать блокирования, для используемых приложений вы можете настроить исключения из проверки. Для этого нужно добавить в доверенную зону название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского". Например, вы часто используете в своей работе приложение Radmin, предназначенное для удаленного управления компьютерами. Такая активность приложения рассматривается Kaspersky Endpoint Security как подозрительная и может быть заблокирована. Чтобы исключить блокировку приложения, нужно сформировать исключение из проверки, где указать название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского".

Если у вас на компьютере установлено приложение, выполняющее сбор и отправку информации на обработку, приложение Kaspersky Endpoint Security может классифицировать такое приложение как вредоносное. Чтобы избежать этого, вы можете исключить приложение из проверки, настроив приложение Kaspersky Endpoint Security способом, описанным в этом документе.

Исключения из проверки могут использоваться в ходе работы следующих компонентов и задач приложения, заданных администратором системы:

- Анализ поведения.
- Защита от эксплойтов.
- Предотвращение вторжений.
- Защита от файловых угроз.
- Защита от веб-угроз.
- Защита от почтовых угроз.
- Задача *Поиск вредоносного ПО*.

Список доверенных приложений

Список доверенных приложений – это список приложений, у которых Kaspersky Endpoint Security не контролирует файловую и сетевую активности (в том числе и вредоносную), а также обращения этих приложений к системному реестру. По умолчанию Kaspersky Endpoint Security контролирует объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех приложений и создаваемый ими сетевой трафик. После добавления приложения в список доверенных приложений Kaspersky Endpoint Security перестает контролировать активность приложения.

Отличие исключений из проверки от доверенных приложений заключается в том, что для исключений Kaspersky Endpoint Security не проверяет файлы, а для доверенных приложений инициируемые процессы. То есть, если доверенное приложение создаст вредоносный файл в папке, которая не включена в исключения, Kaspersky Endpoint Security обнаружит этот файл и устранит угрозу. Если папка добавлена в исключения, Kaspersky Endpoint Security пропустит этот файл.

Например, если вы считаете объекты, используемые приложением Microsoft Windows Блокнот, безопасными, то есть доверяете этому приложению, вам следует добавить приложение Microsoft Windows Блокнот в список доверенных приложений, чтобы не контролировать объекты, используемые этим приложением. Это позволит увеличить производительность компьютера, что особенно важно при использовании серверных приложений.

Кроме того, некоторые действия, которые Kaspersky Endpoint Security классифицирует как подозрительные, могут быть безопасны в рамках функциональности ряда приложений. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием приложения автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких приложений и отключить контроль их активности, рекомендуется добавить их в список доверенных приложений.

Доверенные приложения позволяют избежать проблемы совместимости Kaspersky Endpoint Security с другими приложениями (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky Endpoint Security и другого антивирусного приложения).

В то же время исполняемый файл и процесс доверенного приложения по-прежнему проверяются на наличие в них вирусов и других приложений, представляющих угрозу. Для полного исключения приложения из проверки Kaspersky Endpoint Security следует пользоваться исключениями из проверки.

Параметры исключений

Параметр	Описание

Типы обнаруживаемых объектов

Вне зависимости от настроенных параметров приложения Kaspersky Endpoint Security всегда обнаруживает и блокирует вирусы, черви и троянские приложения. Эти приложения могут нанести значительный вред компьютеру.

- **Вирусы и черви**

  Подкатегория: вирусы и черви (Viruses_and_Worms)

  Уровень опасности: высокий

  Классические вирусы и черви выполняют на компьютере действия, не разрешенные пользователем. Они могут создавать свои копии, которые обладают способностью дальнейшего самовоспроизведения.

  Классический вирус

  Попав в систему, классический вирус заражает какой-либо файл, активизируется в нем, выполняет свое вредоносное действие, а затем добавляет свои копии в другие файлы.

  Классический вирус размножается только на локальных ресурсах компьютера и не может самостоятельно проникать на другие компьютеры. Он может попасть на другой компьютер только в том случае, если добавит свою копию в файл, который хранится в папке общего доступа или на установленном компакт-диске, или если пользователь сам перешлет сообщение электронной почты с вложенным в него зараженным файлом.

  Код классического вируса может внедряться в различные области компьютера, операционной системы или приложения. В зависимости от среды обитания вирусы подразделяют на *файловые*, *загрузочные*, *скриптовые* и *макро-вирусы*.

  Вирусы могут заражать файлы различными способами. *Перезаписывающие* (Overwriting) вирусы записывают свой код вместо кода заражаемого файла, уничтожая его содержимое. Зараженный файл перестает работать, и его нельзя восстановить. *Паразитические* (Parasitic) вирусы изменяют файлы, оставляя их полностью или частично работоспособными. *Вирусы-компаньоны* (Companion) не изменяют файлы, но создают их двойники. При открытии зараженного файла запускается его двойник, то есть вирус. Среди вирусов встречаются также *вирусы-ссылки* (Link), вирусы, *заражающие объектные модули* (OBJ), вирусы, *заражающие библиотеки компиляторов* (LIB), вирусы, *заражающие исходные тексты программ*, и другие.

  Червь

  Код червя, как и код классического вируса, попав в систему, активизируется и выполняет свое вредоносное действие. Свое название червь получил благодаря способности "переползать" с компьютера на компьютер – без разрешения пользователя распространять свои копии через различные информационные каналы.

  Основной признак, по которому черви различаются между собой, – способ их распространения. Описание типов червей по способу распространения приводится в следующей таблице.

  Способы распространения червей

Тип	Название	Описание
Email-Worm	Почтовые черви	Распространяются через электронную почту. Зараженное сообщение электронной почты содержит прикрепленный файл с копией червя или ссылку на такой файл на веб-сайте, например, взломанном или специально созданном. Когда вы запускаете прикрепленный файл, червь активизируется; когда вы щелкаете на ссылке, загружаете, а затем открываете файл, червь также начинает выполнять свое вредоносное действие. После этого он продолжает распространять свои копии, разыскивая другие адреса электронной почты и отправляя по ним зараженные сообщения.
IM-Worm	Черви IM-клиентов	Распространяются через IM-клиенты. Обычно такой червь рассылает по контакт-листам сообщения, содержащие ссылку на файл с его копией на веб-сайте. Когда пользователь загружает файл и открывает его, червь активизируется.
IRC-Worm	Черви интернет-чатов	Распространяются через ретранслируемые интернет-чаты (Internet Relay Chats) – сервисные системы, с помощью которых можно общаться через интернет с другими людьми в реальном времени. Такой червь публикует в интернет-чате файл со своей копией или ссылку на файл. Когда пользователь загружает файл и открывает его, червь активизируется.
Net-Worm	Сетевые черви (черви компьютерных сетей)	Распространяются через компьютерные сети. В отличие от червей других типов, сетевой червь распространяется без участия пользователя. Он ищет в локальной сети компьютеры, на которых используются программы, содержащие уязвимости. Для этого он посылает специально сформированный сетевой пакет (эксплойт), который содержит код червя или его часть. Если в сети находится "уязвимый" компьютер, он принимает такой сетевой пакет. Полностью проникнув на компьютер, червь активизируется.
P2P-Worm	Черви файлообменных сетей	Распространяются через файлообменные пиринговые сети. Чтобы внедриться в файлообменную сеть, червь копирует себя в каталог обмена файлами, обычно расположенный на компьютере пользователя. Файлообменная сеть отображает информацию об этом файле, и пользователь может "найти" зараженный файл в сети так же, как и любой другой, загрузить его и открыть. Более сложные черви имитируют сетевой протокол конкретной файлообменной сети: они положительно отвечают на поисковые запросы и предлагают для загрузки свои копии.
Worm	Прочие черви	К прочим сетевым червям относятся: • Черви, которые распространяют свои копии через сетевые ресурсы. Используя функции операционной системы, они перебирают доступные сетевые папки, подключаются к компьютерам в глобальной сети и пытаются открыть их диски на полный доступ. В отличие от описанных выше разновидностей червей, прочие черви активизируются не самостоятельно, а как только пользователь открывает файл с копией червя. • Черви, которые не относятся ни к одному из описанных в этой таблице способов распространения (например, те, которые распространяются через мобильные телефоны).

- **Троянские приложения (в том числе приложения-вымогатели)**

  Подкатегория: троянские программы (Trojan_programs)

  Уровень опасности: высокий

  В отличие от червей и вирусов, троянские программы не создают свои копии. Они проникают на компьютер, например, через электронную почту или через браузер, когда пользователь посещает зараженную веб-страницу. Троянские программы запускаются при участии пользователя. Они начинают выполнять свое вредоносное действие сразу после запуска.

  Разные троянские программы ведут себя на зараженном компьютере по-разному. Основные функции троянских программ – блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей. Кроме этого, троянские программы могут принимать или отправлять файлы, выполнять их, выводить на экран сообщения, обращаться к веб-страницам, загружать и устанавливать программы, перезагружать компьютер.

  Злоумышленники часто используют "наборы" из разных троянских программ.

  Типы поведения троянских программ описаны в следующей таблице.

  Типы поведения троянских программ на зараженном компьютере

Тип	Название	Описание
Trojan-ArcBomb	Троянские программы – "архивные бомбы"	Архивы; при распаковке увеличиваются до таких размеров, что нарушают работу компьютера. Когда пользователь пытается распаковать такой архив, компьютер может начать работать медленно или "зависнуть", диск может заполниться "пустыми" данными. "Архивные бомбы" особенно опасны для файловых и почтовых серверов. Если на сервере используется система автоматической обработки входящей информации, такая "архивная бомба" может остановить сервер.
Backdoor	Троянские программы удаленного администрирования	Считаются наиболее опасными среди троянских программ. По своим функциям напоминают устанавливаемые на компьютеры программы удаленного администрирования. Эти программы устанавливают себя в компьютере незаметно для пользователя и позволяют злоумышленнику удаленно управлять компьютером.
Trojan	Троянские программы	Включают следующие вредоносные программы: • **Классические троянские программы**. Эти программы выполняют только основные функции троянских программ: блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей. Они не имеют дополнительных функций, свойственных другим типам троянских программ, описанным в этой таблице. • **"Многоцелевые" троянские программы**. Эти программы имеют дополнительные функции, присущие сразу нескольким типам троянских программ.
Trojan-Ransom	Троянские программы, требующие выкупа	"Берут в заложники" информацию на компьютере пользователя, изменяя или блокируя ее, или нарушают работу компьютера таким образом, чтобы пользователь не мог воспользоваться информацией. Злоумышленник требует от пользователя выкуп за обещание выслать программу, которая восстановит работоспособность компьютера и данные на нем.
Trojan-Clicker	Троянские программы-кликеры	С компьютера пользователя обращаются к веб-страницам: они или сами посылают команды браузеру, или заменяют хранящиеся в системных файлах веб-адреса. С помощью этих программ злоумышленники организовывают сетевые атаки, повышают посещаемость сайтов, чтобы увеличить количество показов рекламных баннеров.
Trojan-Downloader	Троянские программы-загрузчики	Обращаются к веб-странице злоумышленника, загружают с нее другие вредоносные программы и устанавливают их на компьютере пользователя; могут хранить имя файла загружаемой вредоносной программы в себе или получать его с веб-страницы, к которой обращаются.
Trojan-Dropper	Троянские программы-установщики	Сохраняют на диске компьютера, а затем устанавливают другие троянские программы, которые хранятся в теле этих программ. Злоумышленники могут использовать троянские программы-установщики, чтобы достичь следующих целей: • установить вредоносную программу незаметно для пользователя: троянские программы-установщики не отображают никаких сообщений или выводят на экран ложные сообщения, например, об ошибке в архиве или неверной версии операционной системы; • защитить от обнаружения другую известную вредоносную программу: не все антивирусы могут распознать вредоносную программу внутри троянской программы-установщика.
Trojan-Notifier	Троянские программы-уведомители	Сообщают злоумышленнику о том, что зараженный компьютер находится "на связи"; передают ему информацию о компьютере: IP-адрес, номер открытого порта или адрес электронной почты. Они связываются со злоумышленником по электронной почте, через FTP, обращаясь к его веб-странице или другим способом. Троянские программы-уведомители часто используются в наборах из разных троянских программ. Они извещают злоумышленника о том, что другие троянские программы успешно установлены на компьютере пользователя.
Trojan-Proxy	Троянские программы-прокси	Позволяют злоумышленнику анонимно обращаться через компьютер пользователя к веб-страницам; часто используются для рассылки спама.
Trojan-PSW	Троянские программы, крадущие пароли	Троянские программы, крадущие пароли (Password Stealing Ware); крадут учетные записи пользователей, например, регистрационную информацию к программному обеспечению. Они отыскивают конфиденциальные данные в системных файлах и реестре и пересылают ее "хозяину" по электронной почте, через FTP, обращаясь к веб-странице злоумышленника или другим способом. Некоторые из этих троянских программ выделены в отдельные типы, описанные в этой таблице. Это троянские программы, крадущие банковские счета (Trojan-Banker), троянские программы, крадущие данные пользователей IM-клиентов (Trojan-IM) и троянские программы, крадущие данные пользователей сетевых игр (Trojan-GameThief).
Trojan-Spy	Троянские программы-шпионы	Ведут электронный шпионаж за пользователем: собирают информацию о его действиях на компьютере, например, перехватывают данные, которые пользователь вводит с клавиатуры, делают снимки экрана или собирают списки активных приложений. Получив эту информацию, они передают ее злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.

Trojan-DDoS	Троянские программы – сетевые атаки	Отправляют с компьютера пользователя многочисленные запросы на удаленный сервер. У сервера не хватает ресурсов для обработки запросов, и он перестает работать (Denial-of-Service (DoS) – отказ в обслуживании). Такими программами часто заражают многие компьютеры, чтобы с них одновременно атаковать один сервер. DoS-программы реализуют атаку с одного компьютера с ведома пользователя. DDoS-программы (Distributed DoS) реализуют распределенные атаки с разных компьютеров, причем без ведома пользователя зараженного компьютера.
Trojan-IM	Троянские программы, крадущие данные пользователей IM-клиентов	Крадут номера и пароли пользователей IM-клиентов. Передают данные злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Rootkit	Руткиты	Скрывают другие вредоносные программы и их активность и таким образом продлевают пребывание этих программ в системе; могут скрывать файлы, процессы в памяти зараженного компьютера или ключи реестра, которые запускают вредоносные программы; могут скрывать обмен данными между приложениями на компьютере пользователя и других компьютерах в сети.
Trojan-SMS	Троянские программы – SMS-сообщения	Заражают мобильные телефоны и с них отправляют SMS-сообщения на платные номера.
Trojan-GameThief	Троянские программы, крадущие данные пользователей сетевых игр	Крадут учетные данные пользователей сетевых компьютерных игр; передают их злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Trojan-Banker	Троянские программы, крадущие банковские счета	Крадут данные банковских счетов или счетов в системах электронных денег; передают данные злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Trojan-Mailfinder	Троянские программы – сборщики адресов электронной почты	Собирают адреса электронной почты на компьютере и передают их злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом. По собранным адресам злоумышленники могут рассылать спам.

- **Вредоносные утилиты**

  Подкатегория: вредоносные утилиты (Malicious_tools)

  Уровень опасности: средний

  Вредоносные утилиты, в отличие от других вредоносных программ, не выполняют своих действий сразу при запуске и могут безопасно храниться и запускаться на компьютере пользователя. Злоумышленники используют функции этих программ для создания вирусов, червей и троянских программ, организации сетевых атак на удаленные серверы, "взлома" компьютеров или других вредоносных действий.

  Разнообразные функции вредоносных утилит делятся на типы, которые описаны в следующей таблице.

  Функции вредоносных утилит

Тип	Название	Описание
Constructor	Конструкторы	Позволяют создавать новые вирусы, черви и троянские программы. Некоторые конструкторы имеют стандартный оконный интерфейс, в котором с помощью меню можно выбирать тип создаваемой вредоносной программы, способ ее противодействия отладчику и другие свойства.
Dos	Сетевые атаки	Отправляют с компьютера пользователя многочисленные запросы на удаленный сервер. У сервера не хватает ресурсов для обработки запросов, и он перестает работать (Denial-of-Service (DoS) – отказ в обслуживании).
Exploit	Эксплойты	*Эксплойт* – это набор данных или программный код, использующий уязвимости приложения, в котором он обрабатывается, чтобы выполнить на компьютере вредоносное действие. Например, эксплойт может записывать или считывать файлы либо обращаться к "зараженным" веб-страницам. Разные эксплойты используют уязвимости разных приложений или сетевых служб. Эксплойт в виде сетевого пакета передается по сети на многие компьютеры, выискивая компьютеры с уязвимыми сетевыми службами. Эксплойт в файле DOC использует уязвимости текстового редактора. Он может начать выполнять заложенные в него злоумышленником функции, когда пользователь откроет зараженный файл. Эксплойт, внедренный в сообщение электронной почты, ищет уязвимости в каком-либо почтовом клиенте. Он может начать выполнять вредоносное действие, как только пользователь откроет зараженное сообщение в этом почтовом клиенте. С помощью эксплойтов распространяются сетевые черви (Net-Worm). Эксплойты-ньюкеры (Nuker) представляют собой сетевые пакеты, которые выводят компьютеры из строя.
FileCryptor	Шифровальщики	Шифруют другие вредоносные программы, чтобы скрыть их от антивирусного приложения.
Flooder	Программы для "замусоривания" сетей	Рассылают многочисленные сообщения по сетевым каналам. К этому типу относятся, например, программы для замусоривания ретранслируемых интернет-чатов (Internet Relay Chats). К типу Flooder не относятся программы, "забивающие мусором" каналы электронной почты, IM-клиентов и мобильных систем. Эти программы выделяют в отдельные типы, описанные в этой таблице (Email-Flooder, IM-Flooder и SMS-Flooder).
HackTool	Инструменты хакера	Позволяют взламывать компьютер, на котором они установлены, или атаковать другой компьютер (например, без разрешения пользователя добавлять других пользователей системы; очищать системные журналы, чтобы скрыть следы присутствия в системе). К этому типу относят некоторые снифферы, которые обладают вредоносными функциями, например перехватывают пароли. Снифферы (Sniffers) – это программы, которые позволяют просматривать сетевой трафик.
Hoax	Злые шутки	Пугают пользователя вирусоподобными сообщениями: могут "обнаружить" вирус в незараженном файле или объявить о форматировании диска, которого на самом деле не происходит.
Spoofer	Утилиты-имитаторы	Отправляют сообщения и сетевые запросы с поддельным адресом отправителя. Злоумышленники используют утилиты-имитаторы, чтобы, например, выдать себя за отправителя.
VirTool	Инструменты для модификации вредоносных программ	Позволяют модифицировать другие вредоносные программы так, чтобы скрыть их от антивирусных приложений.
Email-Flooder	Программы для "замусоривания" адресов электронной почты	Отправляют многочисленные сообщения по адресам электронной почты ("забивают их мусором"). Большой поток сообщений не дает пользователям просматривать полезную входящую почту.

IM-Flooder	Программы для "замусоривания" IM-клиентов	Отправляют многочисленные сообщения пользователям IM-клиентов. Большой поток сообщений не дает пользователям просматривать полезные входящие сообщения.
SMS-Flooder	Программы для "замусоривания" SMS-сообщениями	Отправляют многочисленные SMS-сообщения на мобильные телефоны.

- **Рекламные приложения**

  Подкатегория: рекламные программы (Adware)

  Уровень опасности: средний

  Рекламные программы связаны с показом пользователю рекламной информации. Они отображают в интерфейсе других программ рекламные баннеры, перенаправляют поисковые запросы на рекламные веб-страницы. Некоторые из них собирают и переправляют своему разработчику маркетинговую информацию о пользователе: например, сведения о том, какие тематические веб-сайты он посещает, какие поисковые запросы делает. В отличие от троянских программ-шпионов, рекламные программы передают эту информацию разработчику с разрешения пользователя.

- **Приложения автодозвона**

  Подкатегория: легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

  Уровень опасности: средний

  Большинство этих программ являются полезными, и многие пользователи применяют их. Среди таких программ – IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

  Однако если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать некоторые их функции для нарушения безопасности.

  Подобные программы различают по функциям, типы которых описаны в таблице ниже.

Тип	Название	Описание
Client-IRC	Клиенты интернет-чатов	Пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.
Downloader	Программы-загрузчики	Могут загружать файлы с веб-страниц в скрытом режиме.
Monitor	Программы-мониторы	Позволяют наблюдать за активностью на компьютере, на котором установлены (видеть, какие приложения работают и как они обмениваются данными с приложениями на других компьютерах).
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры пользователей злоумышленники.
RemoteAdmin	Программы удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры пользователей для наблюдения за удаленными компьютерами и управления ими. Легальные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные программы этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на локальном компьютере	Дают пользователю дополнительные возможности при работе на своем компьютере (позволяют скрывать на своем компьютере файлы или окна активных приложений, закрывать активные процессы).
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

- **Легальные приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя**

  Подкатегория: легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

  Уровень опасности: средний

  Большинство этих программ являются полезными, и многие пользователи применяют их. Среди таких программ – IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

  Однако если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать некоторые их функции для нарушения безопасности.

  Подобные программы различают по функциям, типы которых описаны в таблице ниже.

Тип	Название	Описание
Client-IRC	Клиенты интернет-чатов	Пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.
Downloader	Программы-загрузчики	Могут загружать файлы с веб-страниц в скрытом режиме.
Monitor	Программы-мониторы	Позволяют наблюдать за активностью на компьютере, на котором установлены (видеть, какие приложения работают и как они обмениваются данными с приложениями на других компьютерах).
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры пользователей злоумышленники.
RemoteAdmin	Программы удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры пользователей для наблюдения за удаленными компьютерами и управления ими. Легальные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные программы этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на локальном компьютере	Дают пользователю дополнительные возможности при работе на своем компьютере (позволяют скрывать на своем компьютере файлы или окна активных приложений, закрывать активные процессы).
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

- **Упакованные объекты, способ упаковки которых может использоваться для защиты вредоносного кода**

  Подкатегория: Упакованные файлы, которые могут нанести вред.

  Уровень опасности: средний.

  Файл упакован специальным упаковщиком, который используется для упаковки вредоносных программ: вирусов, червей, троянских программ. Kaspersky Endpoint Security проверяет модуль-распаковщик в составе самораспаковывающихся архивов SFX (self-extracting archive).

  Чтобы скрыть вредоносные программы от обнаружения антивирусом, злоумышленники упаковывают их с помощью специальных упаковщиков. Специалисты "Лаборатории Касперского" выделили упаковщики, которые злоумышленники используют чаще всего.

- **Многократно упакованные объекты**

  Подкатегория: Упакованные файлы, которые могут нанести вред.

Уровень опасности: средний.

Файл упакован специальным упаковщиком, который используется для упаковки вредоносных программ: вирусов, червей, троянских программ. Kaspersky Endpoint Security проверяет модуль-распаковщик в составе самораспаковывающихся архивов SFX (self-extracting archive).

Чтобы скрыть вредоносные программы от обнаружения антивирусом, злоумышленники упаковывают их с помощью специальных упаковщиков. Специалисты "Лаборатории Касперского" выделили упаковщики, которые злоумышленники используют чаще всего.

Исключения

Таблица содержит информацию об исключениях из проверки.

Рекомендуется указывать относительные пути вместо абсолютных. Это позволяет исключить из проверки не только объекты файловой системы, но и бесфайловые объекты. Например, `*\Program Files (x86)\Folder\Subfolder`.

Вы можете исключать из проверки объекты следующими способами:

- Укажите путь к файлу или папке.
- Введите хеш объекта.
- Используйте маски:
  - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.
  - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.
  - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

    Вы можете использовать маски в любом месте пути к файлу или папке. Например, если вы хотите включить в область проверки папку Загрузки для всех учетных записей пользователей компьютера, введите маску `C:\Users\*\Downloads\`.

    Kaspersky Endpoint Security поддерживает переменные среды.

    Kaspersky Endpoint Security не поддерживает переменную среды `%userprofile%` при формировании списка исключений через консоль Kaspersky Security Center. Чтобы применить запись ко всем учетным записям, вы можете использовать символ * (например, `C:\Users\*\Documents\File.exe`). При добавлении новой переменной среды нужно перезапустить приложение.
- Введите название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`). Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, приложение исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

Kaspersky Endpoint Security скрывает для просмотра список исключений из проверки в интерфейсе приложения, если администратор в консоли запретил настройку исключений из проверки ("замок" закрыт) и запретил использование локальных исключений из проверки (флажок **Разрешить использование локальных исключений** снят).

Доверенные приложения	Таблица доверенных приложений, активность которых Kaspersky Endpoint Security не проверяет в процессе своей работы. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. Kaspersky Endpoint Security не поддерживает переменную среды `%userprofile%` при формировании списка доверенных приложений через консоль Kaspersky Security Center. Чтобы применить запись ко всем учетным записям, вы можете использовать символ `*` (например, `C:\Users\*\Documents\File.exe`). При добавлении новой переменной среды нужно перезапустить приложение. Компонент Контроль приложений регулирует запуск каждого из приложений независимо от того, указано ли это приложение в таблице доверенных приложений или нет. Kaspersky Endpoint Security скрывает для просмотра список доверенных приложений в интерфейсе приложения, если администратор в консоли запретил настройку доверенных приложений ("замок" закрыт) и запретил использование локальных доверенных приложений (флажок **Разрешить использование локальных доверенных приложений** снят).
Объединять значения при наследовании *(доступен только в консоли Kaspersky Security Center)*	Объединение списка исключений из проверки и списка доверенных приложений в родительских и дочерних политиках Kaspersky Security Center. Для объединения списков необходимо в дочерней политике включить наследование параметров родительской политики Kaspersky Security Center. Если флажок установлен, элементы списка родительской политики Kaspersky Security Center отображаются в дочерних политиках и доступны для просмотра. Таким образом, вы можете, например, создать общий список доверенных приложений для всей организации. Удалить или изменить унаследованные элементы списка в дочерней политике невозможно. Элементы списка исключений из проверки и списка доверенных приложений, объединенные при наследовании, доступны для удаления и изменения только в родительской политике. Добавление, изменение и удаление элементов списка возможно на нижестоящих уровнях. Если элементы списков дочерней и родительской политик совпадают, эти элементы отображаются как один элемент родительской политики. Если флажок снят, то элементы списков не объединяются при наследовании параметров политик Kaspersky Security Center. Также эта функция позволяет объединять списки в профилях политик. Для объединения списков необходимо в профиле высшего приоритета включить наследование параметров из профиля низшего приоритета. Подробнее о приоритетах профилей политики см. в справке Kaspersky Security Center.
Разрешить использование локальных исключений / **Разрешить использование локальных доверенных приложений** *(доступен только в консоли Kaspersky Security Center)*	*Локальные исключения и локальные доверенные приложения (локальная доверенная зона)* – список объектов и приложений, сформированные пользователем в Kaspersky Endpoint Security для отдельного компьютера. Kaspersky Endpoint Security в процессе работы не контролирует объекты и приложения из локальной доверенной зоны. Таким образом, кроме общей доверенной зоны, сформированной в политике, пользователь может создавать собственные локальные списки исключений и доверенных приложений. Если флажок установлен, пользователь может сформировать локальный список исключений из проверки и локальный список доверенных приложений. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера. Если флажок снят, пользователю доступны только общие списки исключений из проверки и доверенных приложений, сформированные в политике.
Телеметрия EDR (KATA) / NDR (KATA) *(доступен только в консоли Kaspersky Security Center)*	Таблица содержит информацию об исключениях из EDR-телеметрии.
Телеметрия KUMA *(доступен только в консоли Kaspersky Security Center)*	Список событий для отправки в Kaspersky Unified Monitoring and Analysis Platform (KUMA). Kaspersky Endpoint Security работает в следующих режимах: • **Отправлять все события**. В этом режиме приложение отправляет все события журнала Windows кроме событий, добавленных в правила исключения. • **Отправлять только выбранные события**. В этом режиме приложение отправляет только события, добавленные в правила включения.
Доверенное системное хранилище сертификатов	Если выбрано одно из доверенных системных хранилищ сертификатов, приложение Kaspersky Endpoint Security исключает из проверки приложения, подписанные доверенной цифровой подписью. Kaspersky Endpoint Security автоматически помещает такие приложения в группу **Доверенные**. Если выбрано **Не использовать**, то Kaspersky Endpoint Security проверяет приложения независимо от наличия цифровой подписи. Приложение Kaspersky Endpoint Security помещает приложение в группу доверия в зависимости от уровня опасности, которую это приложение может представлять для компьютера.

Настройки приложения

Вы можете настроить следующие общие параметры приложения:

- режим работы;
- самозащита;
- производительность;
- отладочная информация;
- статус компьютера при применении параметров.

Параметры приложения

Параметр	Описание
Запускать приложение при включении компьютера (рекомендуется)	Если флажок установлен, то приложение Kaspersky Endpoint Security запускается после загрузки операционной системы и защищает компьютер пользователя в течение всего сеанса работы. Если флажок не установлен, то приложение Kaspersky Endpoint Security не запускается после загрузки операционной системы до того момента, как пользователь запустит приложение вручную. Защита компьютера выключена и данные пользователя могут находиться под угрозой.
Применять технологию лечения активного заражения (использует значительные ресурсы компьютера)	Как правило, компоненты Kaspersky Endpoint Security при обнаружении вредоносной активности завершают работу вредоносного приложения до заражения компьютера. Технология лечения активного заражения обеспечивает защиту компьютера от уже действующих вредоносных приложений (активное заражение), минимизируя риски потери данных и распространения угрозы. Если технология включена, при обнаружении вредоносной активности Kaspersky Endpoint Security показывает всплывающее уведомление. В уведомлении приложение Kaspersky Endpoint Security предлагает провести процедуру лечения активного заражения компьютера. После подтверждения пользователем этой процедуры приложение Kaspersky Endpoint Security устраняет угрозу, затем выполняет перезагрузку компьютера. Применение технологии лечения активного заражения требует значительных ресурсов компьютера, что может замедлить работу других приложений. Во время обнаружения приложением активного заражения некоторые функции операционной системы могут быть недоступны. Доступность операционной системы восстановится после завершения лечения активного заражения и перезагрузки компьютера. Если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов, Kaspersky Endpoint Security не показывает уведомление. Таким образом, пользователь не может выбрать действие для лечения активного заражения. Для устранения угрозы вам необходимо включить технологию лечения активного заражения в параметрах приложения и включить немедленное лечение активного заражения в свойствах задачи *Поиск вредоносного ПО*. Далее вам нужно запустить задачу *Поиск вредоносного ПО*.
Использовать Kaspersky Security Center в качестве прокси-сервера для активации *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, то для подключения к серверам активации приложение использует Сервер администрирования Kaspersky Security Center в качестве прокси-сервера. Это нужно при активации приложения в изолированном сегменте сети без доступа в интернет с помощью кода активации. При активации приложения с помощью файла ключа доступ в интернет не нужен.
Включить самозащиту	Если функция включена, то Kaspersky Endpoint Security предотвращает изменение и удаление файлов приложения на жестком диске, процессов в памяти и записей в системном реестре.

Параметр	Описание
Блокировать внешнее управление службами приложения	Если функция включена, то Kaspersky Endpoint Security запрещает управление службами приложения с помощью сторонних приложений (например, CMD). При попытке управления службами приложениями с помощью сторонних приложений, над значком приложения в области уведомлений панели задач Microsoft Windows отображается уведомление (если служба уведомлений не выключена пользователем). Вы можете предоставить возможность внешнего управления службами приложения только на компьютерах без поддержки технологии AM-PPL или с выключенной технологией.
Откладывать задачи по расписанию при работе от аккумулятора	Если флажок установлен, то режим энергосбережения при работе от аккумулятора включен. Приложение Kaspersky Endpoint Security откладывает выполнение задач, для которых задан запуск по расписанию. По мере необходимости вы можете самостоятельно запускать задачи проверки и обновления. Если включен режим энергосбережения, при работе от аккумулятора не запускаются следующие задачи, даже если для них задан запуск по расписанию: • *Полная проверка*; • *Проверка важных областей*; • *Выборочная проверка*; • *Проверка целостности приложения*; • *Поиск IOC*; • *Обновление баз и модулей приложения* (только патчи). Приложение пропускает обновление антивирусных баз по расписанию только в том случае когда ноутбук работает от аккумулятора и уровень заряда аккумулятора ниже 30% (значение по умолчанию). Вы можете изменить минимальный уровень заряда аккумулятора, при котором приложение пропускает обновление антивирусных баз по расписанию, через реестр. В остальных случаях Kaspersky Endpoint Security обновляет антивирусные базы по расписанию независимо от того, подключен ноутбук к сети или работает от аккумулятора, а также от статуса режима энергосбережения приложения.
Уступать ресурсы другим приложениям	Потребление ресурсов компьютера Kaspersky Endpoint Security при проверке компьютера может увеличить нагрузку на центральный процессор и дисковые подсистемы. Это может замедлить работу других приложений. Для оптимизации производительности в Kaspersky Endpoint Security предусмотрен *режим передачи ресурсов другим приложениям*. В этом режиме операционная система может понизить приоритет потоков задач проверки Kaspersky Endpoint Security при высокой нагрузке на центральный процессор. Это позволит перераспределить ресурсы операционной системы для других приложений. То есть задачи проверки получат меньше процессорного времени. В результате Kaspersky Endpoint Security будет проверять компьютер дольше. По умолчанию режим передачи ресурсов другим приложениям включен.
Ограничить потребление ресурсов процессора для задач проверки	Для оптимизации производительности Kaspersky Endpoint Security вы можете ограничить использование ресурсов процессора для задачи *Поиск вредоносного ПО*. Если флажок установлен, средняя нагрузка на все ядра процессора при выполнении задачи *Поиск вредоносного ПО* стремится к указанному значению. По умолчанию флажок снят.
Включить запись дампов	Если флажок установлен, то Kaspersky Endpoint Security записывает дампы в случае сбоев в работе. Если флажок снят, то Kaspersky Endpoint Security не записывает дампы. Приложение удаляет уже существующие на жестком диске компьютера файлы дампов.
Включить защиту файлов дампов и файлов трассировки	Если флажок установлен, то доступ к файлам дампов предоставляется системному и локальному администраторам, а также пользователю, включившему запись дампов. Доступ к файлам трассировки предоставляется только системному и локальному администраторам. Если флажок снят, доступ к файлам дампов и файлам трассировки имеет любой пользователь.
Статус компьютера при применении настроек *(доступен только в консоли Kaspersky Security Center)*	Параметры отображения статусов клиентских компьютеров с установленным приложением Kaspersky Endpoint Security в Web Console при появлении ошибок применения политики или выполнения задачи. Доступны статусы *OK*, *Предупреждение* и *Критический*.

Параметр	Описание
Устанавливать обновления без перезагрузки компьютера	Обновление приложения без перезагрузки компьютера позволяет обеспечить бесперебойную работу серверов при обновлении приложения. Вы можете обновлять версию приложения без перезагрузки начиная с версии 11.10.0. Для обновления более ранних версий приложения необходимо выполнять перезагрузку компьютера. Начиная с версии 11.11.0 вы можете выполнять следующие действия без перезагрузки: • устанавливать патчи; • изменять состав компонентов приложения; • устанавливать Kaspersky Endpoint Security поверх Kaspersky Security для Windows Server. Значение параметра по умолчанию отличается в зависимости от типа операционной системы. Если приложение установлено на рабочую станцию, функция обновления без перезагрузки выключена. Если приложение установлено на сервер, функция обновления без перезагрузки включена.
Включить совместимость с приложениями для удаленного администрирования *(доступен только в консоли Kaspersky Security Center)*	При появлении сбоев в работе Kaspersky Endpoint Security с инструментами для удаленного администрирования (англ. Remote Administration Tool, RAT) вы можете включить режим совместимости. Сбои могут быть связаны с проблемами совместимости RAT и функции безопасного рабочего стола (англ. Secure Desktop) приложения. Эта функция предназначена для подтверждения действий, которые могут снизить безопасность компьютера. Функция позволяет приложению показывать диалоговое окно подтверждения, изолированное от других процессов. Функция обеспечивает безопасность запроса за счет повышенных прав. Таким образом, подтвердить действие может только пользователь, а не вредоносное ПО. Если флажок установлен, режим совместимости с RAT включен. Приложение показывает диалоговое окно подтверждения без этой функции. Это может снизить уровень безопасности компьютера. Рекомендуется не включать режим совместимости, если Kaspersky Endpoint Security с RAT работает корректно. Если флажок снят, режим совместимости с RAT выключен. По умолчанию флажок снят. Пример. При работе с браузером в режиме RemoteApp Kaspersky Endpoint Security может не показывать диалоговое окно подтверждения при переходе на сайт с недоверенным сертификатом, так как RemoteApp не поддерживает функцию безопасного рабочего стола приложения. Это может привести к тому, что браузер перестает отвечать. Для корректной работы браузера в режиме RemoteApp нужно включить режим совместимости. Вы также можете попробовать включить режим совместимости при появлении сбоев в работе функции безопасного рабочего стола с другим сторонним ПО.

Отчеты и хранилище

Отчеты

Информация о работе каждого компонента Kaspersky Endpoint Security, о событиях шифрования данных, о выполнении каждой задачи проверки, задачи обновления и задачи проверки целостности, а также о работе приложения в целом сохраняется в отчетах.

Отчеты хранятся в папке `C:\ProgramData\Kaspersky Lab\KES.14.3\Report`.

Резервное хранилище

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES.14.3\QB`.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security.

В Kaspersky Endpoint Security отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Карантин

Карантин – это специальное локальное хранилище на компьютере. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства. Kaspersky Endpoint Security использует карантин только при работе с решениями Detection and Response от "Лаборатории Касперского". В остальных случаях Kaspersky Endpoint Security помещает файл в резервное хранилище. Подробнее о работе с карантином в составе решений см. в справке Kaspersky Sandbox, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Endpoint Detection and Response Expert, Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Detection and Response Expert (on-premises).

Вы можете настроить параметры карантина только в Web Console. Также в Web Console вы можете выполнить действия с объектами на карантине (восстановить, удалить, добавить и другие). Восстановление объектов доступно на компьютере локально из командной строки.

Kaspersky Endpoint Security помещает файлы на карантин под системной учетной записью (SYSTEM).

Параметры отчетов и хранения

Параметр	Описание
Удалять отчеты через (дни)	Если флажок установлен, то максимальный срок хранения отчетов ограничен заданным интервалом времени. По умолчанию максимальный срок хранения отчетов составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчета.
Ограничить размер файла отчетов до (МБ)	Если флажок установлен, то максимальный размер файла отчетов ограничен заданным значением. По умолчанию максимальный размер файла составляет 1024 МБ. После достижения максимального размера файла отчета Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчетов таким образом, чтобы размер файла отчетов не превышал максимального значения.
Удалять объекты через (дни)	Если флажок установлен, то максимальный срок хранения файлов ограничен заданным интервалом времени. По умолчанию максимальный срок хранения файлов составляет 30 дней. По истечении максимального срока хранения Kaspersky Endpoint Security удаляет наиболее старые файлы из резервного хранилища.
Ограничить размер резервного хранилища до (МБ)	Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. По умолчанию максимальный размер составляет 1024 МБ. После достижения максимального размера резервного хранилища приложение Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения.
Ограничить размер карантина	Если флажок установлен, то максимальный размер карантина ограничен заданным значением. По умолчанию максимальный размер составляет 1024 МБ. При достижении максимального размера карантина Kaspersky Endpoint Security отправляет событие в Kaspersky Security Center *Недостаточно места в хранилище карантина* и публикует событие в Журнале событий Windows. При этом приложение прекращает помещать новые объекты на карантин. Вам нужно вручную очистить карантин.
Уведомлять при заполнении карантина на (%)	Пороговое значение карантина. Например, вы можете задать пороговое значение карантина 50 %. При достижении порогового значения карантина, Kaspersky Endpoint Security отправляет соответствующее событие в Kaspersky Security Center и публикует событие в Журнале событий Windows. При этом приложение продолжает помещать новые объекты на карантин.

Параметр	Описание
Передача данных на Сервер администрирования *(доступен только в Kaspersky Security Center)*	Категории событий на клиентских компьютерах, информация о которых должна передаваться на Сервер администрирования. Вы можете выключить передачу некоторых данных для оптимизации дискового пространства на Сервере администрирования. Приложение передает следующие категории событий: • **О файлах карантина**. Вы можете просмотреть список файлов в карантине в консоли Kaspersky Security Center в папке **Дополнительно → Хранилища → Карантин**. Kaspersky Endpoint Security использует карантин только при работе с решениями Detection and Response от "Лаборатории Касперского". • **О файлах в резервном хранилище**. Вы можете просмотреть список файлов в резервном хранилище в консоли Kaspersky Security Center в папке **Дополнительно → Хранилища → Резервное хранилище**. • **О необработанных файлах**. Вы можете просмотреть список необработанных файлов в консоли Kaspersky Security Center в папке **Дополнительно → Хранилища → Активные угрозы**. • **Об установленных устройствах**. Вы можете просмотреть список подключенных устройств в консоли Kaspersky Security Center в папке **Дополнительно → Хранилища → Оборудование**. Также список устройств доступен в свойствах компьютера и в политике для Kaspersky Endpoint Security для Windows (раздел **Контроль устройств**). • **О запускаемых приложениях**. Вы можете просмотреть список исполняемых файлов в консоли Kaspersky Security Center в папке **Дополнительно → Управление приложениями → Исполняемые файлы**. Также список исполняемых файлов доступен в свойствах компьютера. • **Об ошибках шифрования файлов**. Вы можете просмотреть список ошибок при шифровании файлов в консоли Kaspersky Security Center в папке **Дополнительно → Шифрование и защита данных → События шифрования**. Также список ошибок доступен в свойствах компьютера. • **Отчет о состоянии правил Адаптивного контроля аномалий**. Вы можете просмотреть отчет в консоли Kaspersky Security Center в узле **Сервер администрирования** на вкладке **Отчеты**. Также отчет доступен в свойствах политики Kaspersky Endpoint Security для Windows (раздел **Адаптивный контроль аномалий**). • **Отчет о срабатываниях правил Адаптивного контроля аномалий**. Вы можете просмотреть отчет в консоли Kaspersky Security Center в узле **Сервер администрирования** на вкладке **Отчеты**. Также отчет доступен в свойствах политики Kaspersky Endpoint Security для Windows (раздел **Адаптивный контроль аномалий**). • **О цепочке развития угрозы**. Вы можете просмотреть детали обнаружения в Kaspersky Security Center Web Console в разделе **Мониторинг → Алерты**. Данные о цепочке развития угрозы используют решения Endpoint Detection and Response от "Лаборатории Касперского".

Настройки сети

Вы можете настроить параметры прокси-сервера для подключения к интернету и обновления антивирусных баз, выбрать режим контроля сетевых портов и настроить проверку защищенных соединений.

Параметры сети

Параметр	Описание
Ограничивать трафик при лимитном подключении	Если флажок установлен, приложение ограничивает собственный сетевой трафик в том случае, если подключение к интернету является лимитным. Приложение Kaspersky Endpoint Security определяет высокоскоростное мобильное подключение к интернету как лимитное, а подключение по Wi-Fi – как безлимитное. Учет стоимости подключения работает на компьютерах под управлением Windows 8 и выше.
Внедрять в трафик скрипт взаимодействия с веб-страницами	Если флажок установлен, Kaspersky Endpoint Security внедряет в трафик скрипт взаимодействия с веб-страницами. Этот скрипт обеспечивает работу компонента Веб-Контроль. Скрипт позволяет регистрировать события работы Веб-Контроля. Включить мониторинг активности пользователя в интернете без скрипта невозможно. Специалисты "Лаборатории Касперского" рекомендуют внедрить в трафик скрипт взаимодействия с веб-страницами для корректной работы Веб-Контроля.
Настройки прокси-сервера	Параметры прокси-сервера для доступа пользователей клиентских компьютеров в интернет. Приложение Kaspersky Endpoint Security использует эти параметры в работе некоторых компонентов защиты, в том числе для обновления баз и модулей приложения. Для автоматической настройки прокси-сервера приложение Kaspersky Endpoint Security использует протокол WPAD (Web Proxy Auto-Discovery Protocol). В случае если по этому протоколу не удается определить IP-адрес прокси-сервера, приложение использует адрес прокси-сервера, указанный в параметрах браузера Microsoft Internet Explorer.
Не использовать прокси-сервер для локальных адресов	Если флажок установлен, то при обновлении Kaspersky Endpoint Security из папки общего доступа прокси-сервер не используется.

Параметр	Описание
Настройки аутентификации на прокси-сервере	Для аутентификации приложения на прокси-сервере для доступа в интернет нужно ввести учетные данные пользователя. Kaspersky Endpoint Security поддерживает автоматическую аутентификацию на прокси-сервере. Если выполнить аутентификацию автоматически не удалось, приложение предлагает ввести учетные данные вручную. **Не использовать аутентификацию**. **NTLM-аутентификация**. NTLM-аутентификация с помощью учетной записи текущего пользователя (значение по умолчанию). **NTLM-аутентификация с именем пользователя и паролем**. NTLM-аутентификация с помощью учетных данных, заданных вручную. **Имя пользователя и пароль**. Аутентификация с использованием учетных данных, заданных вручную. **Автоматическая аутентификация**. **Kerberos-аутентификация**. Kerberos-аутентификация с помощью учетной записи текущего пользователя. Для обеспечения корректной работы Kerberos-аутентификации при использовании CNAME-записей для адреса прокси-сервера вам необходимо зарегистрировать имя субъекта-службы (SPN) для каждой CNAME-записи. **Kerberos-аутентификация с именем пользователя и паролем**. Kerberos-аутентификация с использованием учетных данных, заданных вручную. Если выбрана Kerberos-аутентификация, Kaspersky Endpoint Security может в зависимости от настроек прокси-сервера осуществлять аутентификацию как по протоколу Kerberos, так и по протоколу NTLM.
Контролируемые порты	**Контролировать все сетевые порты**. Режим контроля сетевых портов, при котором компоненты защиты (Защита от файловых угроз, Защита от веб-угроз, Защита от почтовых угроз) контролируют потоки данных, передаваемые через любые открытые сетевые порты компьютера. **Контролировать только выбранные сетевые порты**. Режим контроля сетевых портов, при котором компоненты защиты контролируют выбранные сетевые порты компьютера и сетевую активность выбранных приложений. Список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика, настроен в соответствии с рекомендациями специалистов "Лаборатории Касперского". **Контролировать все порты для приложений из списка, рекомендованного "Лабораторией Касперского"**. Предустановленный список приложений, сетевые порты которых контролирует Kaspersky Endpoint Security. В список включены, например, Google Chrome, Adobe Reader, Java и другие приложения. **Контролировать все порты для указанных приложений**. Список приложений, сетевые порты которых контролирует Kaspersky Endpoint Security.
Проверка защищенных соединений	Kaspersky Endpoint Security проверяет зашифрованный сетевой трафик, передаваемый по следующим протоколам: • SSL 3.0; • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security поддерживает следующие режим проверки защищенных соединений: • **Не проверять защищенные соединения**. Kaspersky Endpoint Security не имеет доступ к содержанию сайтов, адрес которых начинается с `https://`. • **Проверять защищенные соединения по запросу компонентов защиты**. Kaspersky Endpoint Security проверяет зашифрованный трафик только по запросу компонентов Защита от веб-угроз, Защита от почтовых угроз и Веб-Контроль. • **Всегда проверять защищенные соединения**. Kaspersky Endpoint Security проверяет зашифрованный сетевой трафик, даже если компоненты защиты выключены. Kaspersky Endpoint Security не проверяет защищенные соединения, установленные доверенными приложениями, для которых выключена проверка трафика. Также Kaspersky Endpoint Security не проверяет защищенные соединения из предустановленного списка доверенных сайтов. Предустановленный список доверенных сайтов составляют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами приложения. Вы можете просмотреть предустановленный список доверенных сайтов только в интерфейсе Kaspersky Endpoint Security. В консоли Kaspersky Security Center просмотреть список невозможно.

Параметр	Описание
Доверенные корневые сертификаты	Список доверенных корневых сертификатов. Kaspersky Endpoint Security позволяет устанавливать доверенные корневые сертификаты на компьютеры пользователей, если, например, вам нужно развернуть новый центр сертификации. Приложение позволяет добавить сертификат в специальное хранилище сертификатов Kaspersky Endpoint Security. При этом сертификат будет доверенным только для приложения Kaspersky Endpoint Security. То есть пользователь будет иметь доступ к веб-сайту с новым сертификатом в браузере. Если другое приложение попытается получить доступ к веб-сайту, вы можете получить ошибку соединения из-за проблем с сертификатом. Для добавления сертификата в системное хранилище сертификатов, вы можете использовать групповые политики Active Directory.
Переход на домен с недоверенным сертификатом	• **Разрешать**. При переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security разрешает установку сетевого соединения. При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security отображает HTML-страницу с предупреждением и информацией о причине, по которой этот домен не рекомендован для посещения. По ссылке из HTML-страницы с предупреждением пользователь может получить доступ к запрошенному веб-ресурсу. Если стороннее приложение или служба устанавливает соединение с доменом с недоверенным сертификатом, Kaspersky Endpoint Security создаст собственный сертификат для проверки трафика. Новый сертификат будет иметь статус *Недоверенный*. Это нужно, чтобы предупредить стороннее приложение о недоверенном соединении, так как показать HTML-страницу в этом случае невозможно и соединение может быть установлено в фоновом режиме. • **Блокировать**. При переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security блокирует сетевое соединение. При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security отображает HTML-страницу с информацией о причине, по которой переход на этот домен заблокирован.
Переход на домен с ошибкой проверки защищенного соединения	• **Блокировать**. При возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security блокирует это сетевое соединение. • **Разрешать и добавлять домен в исключения**. При возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security добавляет домен, при переходе на который возникла ошибка, в список доменов с ошибками проверки и не контролирует зашифрованный сетевой трафик при переходе на этот домен. Вы можете просмотреть список доменов с ошибками проверки защищенных соединений только в локальном интерфейсе приложения. Чтобы сбросить содержание списка, нужно выбрать элемент **Блокировать**. Также Kaspersky Endpoint Security формирует событие об ошибке проверки защищенного соединения.
Блокировать соединения по протоколу SSL 2.0	Если флажок установлен, то приложение контролирует и блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. При этом приложение не контролирует сетевой трафик по этому протоколу.
Блокировать соединения по протоколу SSL 3.0	Если флажок установлен, то приложение блокирует сетевые соединения, устанавливаемые по протоколу SSL 3.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу SSL 3.0. Приложение контролирует сетевой трафик по этому протоколу. Все компоненты приложения работают без ограничений.
Блокировать соединения по протоколу TLS 1.0	Если флажок установлен, то приложение блокирует сетевые соединения, устанавливаемые по протоколу TLS 1.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу TLS 1.0. Приложение контролирует сетевой трафик по этому протоколу. Все компоненты приложения работают без ограничений.
Расшифровывать защищенное соединение с сайтом, использующим EV-сертификат	EV-сертификаты (англ. Extended Validation Certificate) подтверждают подлинность веб-сайтов и повышают безопасность соединения. Браузеры сообщают о наличии на веб-сайте EV-сертификата с помощью значка замка в адресной строке браузера. Также браузеры могут полностью или частично окрашивать адресную строку в зеленый цвет. Если флажок установлен, приложение расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если флажок снят, приложение не имеет доступа к содержанию HTTPS-трафика. Поэтому приложение контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://bing.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.

Параметр	Описание
Настроить доверенные адреса	Список веб-адресов, для которых Kaspersky Endpoint Security не проверяет сетевые соединения. В этом случае Kaspersky Endpoint Security не будет проверять HTTPS-трафик доверенных веб-адресов при работе компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль. Вы можете ввести имя домена или IP-адрес. Kaspersky Endpoint Security поддерживает символ `*` для ввода маски в имени домена. Kaspersky Endpoint Security не поддерживает символ `*` для IP-адресов. Вы можете выбрать диапазон IP-адресов с помощью маски подсети (например, 198.51.100.0/24). Примеры: • `domain.com` – запись включает в себя следующие адреса: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Запись исключает поддомены (например, `subdomain.domain.com`). • `subdomain.domain.com` – запись включает в себя следующие адреса: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Запись исключает домен `domain.com`. • `*.domain.com` – запись включает в себя следующие адреса: `https://movies.domain.com`, `https://images.domain.com/page123`. Запись исключает домен `domain.com`.
Настроить доверенные приложения	Список приложений, активность которых приложение Kaspersky Endpoint Security не проверяет в процессе своей работы. Вы можете выбрать виды активности приложения, которые приложение Kaspersky Endpoint Security не будет контролировать (например, не проверять сетевой трафик). Приложение Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
В приложениях с собственным хранилищем сертификатов для проверки защищенных соединений использовать *(доступен только в интерфейсе Kaspersky Endpoint Security)*	Если флажок установлен, приложение проверяет зашифрованный трафик в браузере Mozilla Firefox и почтовом клиенте Thunderbird. Доступ к некоторым сайтам по протоколу HTTPS может быть заблокирован. Для проверки трафика в браузере Mozilla Firefox и почтовом клиенте Thunderbird должна быть включена проверка защищенных соединений. Если проверка защищенных соединений выключена, приложение не проверяет трафик в браузере Mozilla Firefox и почтовом клиенте Thunderbird. Приложение расшифровывает и анализирует зашифрованный трафик с помощью корневого сертификата "Лаборатории Касперского". Вы можете выбрать хранилище сертификатов, в котором будет находиться корневой сертификат "Лаборатории Касперского": • **Хранилище сертификатов Windows (рекомендуется)**. Это хранилище, в которое корневой сертификат "Лаборатории Касперского" добавляется при установке приложения Kaspersky Endpoint Security. • **Собственное хранилище сертификатов**. Приложения Mozilla Firefox и Thunderbird используют собственное хранилище сертификатов. Если выбрано хранилище сертификатов Mozilla, корневой сертификат "Лаборатории Касперского" нужно добавить в это хранилище вручную через свойства браузера.

Интерфейс

Вы можете настроить параметры интерфейса приложения.

Параметр	Описание
Взаимодействие с пользователем *(доступен только в консоли Kaspersky Security Center)*	**Отображать упрощенный интерфейс**. На клиентском компьютере недоступно главное окно приложения, а доступен только значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять ограниченный список операций с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает над значком приложения только уведомления, требующие действий со стороны пользователя компьютера. **Отображать пользовательский интерфейс**. На клиентском компьютере доступно главное окно Kaspersky Endpoint Security и значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает уведомления над значком приложения. **Скрыть раздел Мониторинг активности приложений**. На клиентском компьютере в главном окне Kaspersky Endpoint Security недоступна кнопка **Мониторинг активности приложений**. *Мониторинг активности приложений* – это инструмент, предназначенный для просмотра информации об активности приложений на компьютере пользователя в режиме реального времени. **Не отображать пользовательский интерфейс**. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security. Также недоступны значок в области уведомлений Windows и уведомления.
Доступ к локальным задачам	Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь, при отсутствии дополнительных ограничений политики, может настраивать и запускать задачи. При этом параметры расписания запуска задачи остаются недоступными для пользователя. Пользователь может запускать задачи только вручную. Если флажок снят, то локальные задачи скрыты в интерфейсе приложения. В этом режиме локальные задачи не запускаются по расписанию. Задачи недоступны для запуска и настройки в локальном интерфейсе Kaspersky Endpoint Security, а также при работе с командной строкой. Пользователь по-прежнему может запустить проверку файла или папки, выбрав пункт **Проверить на вирусы** в контекстном меню файла или папки. При этом задача проверки запустится со значениями параметров, установленными по умолчанию для задачи выборочной проверки.
Просмотр групповых задач	Если флажок установлен, то групповые задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь может просмотреть полный список задач в интерфейсе приложения. Если флажок снят, Kaspersky Endpoint Security показывает пустой список задач.
Управление групповыми задачами	Если флажок установлен, пользователь может запускать и останавливать заданные в консоли Kaspersky Security Center групповые задачи. Пользователь может запускать и останавливать задачи в интерфейсе приложения или в упрощенном интерфейсе приложения. Если флажок снят, Kaspersky Endpoint Security запускает задачи автоматически по расписанию, или администратор запускает задачи вручную в консоли Kaspersky Security Center.
Настроить уведомления	Таблица с параметрами уведомлений о событиях различного уровня важности, которые могут происходить во время работы компонента или приложения в целом, а также выполнения задачи. Уведомления об этих событиях Kaspersky Endpoint Security выводит на экран, доставляет по электронной почте или сохраняет в журналы.
Настроить почтовые уведомления	Параметры SMTP-сервера для рассылки оповещений о событиях, регистрируемых при работе приложения. По умолчанию Kaspersky Endpoint Security использует параметры отправки почтовых уведомлений Kaspersky Security Center. Подробнее о настройке почтовых уведомлений см. в справке Kaspersky Security Center. Если вам нужно настроить отдельные почтовые уведомления, вы можете настроить следующие параметры: • **Адрес отправителя**. Адрес отправителя электронной почты. Не рекомендуется использовать несуществующий адрес. • **SMTP-сервер**. Адрес или адреса почтовых серверов вашей организации (например, `mail.company.com`). Вы можете ввести IP-адрес (IPv4 или IPv6). Для аутентификации пользователя на SMTP-сервере введите учетные данные отправителя в соответствующие поля. Для проверки работы почтовых уведомлений вы можете отправить пробное сообщение. • **Адрес получателя**. Адреса электронной почты пользователей, которым приложение будет отправлять уведомления. • **Режим рассылки**. Режим отправки почтовых уведомлений. Kaspersky Endpoint Security может отправлять сообщения сразу после возникновения события или по составленному расписанию.
Отображать состояние приложения в области уведомлений	Категории событий приложения, при возникновении которых меняется значок Kaspersky Endpoint Security в области уведомлений панели задач Microsoft Windows (или).
Уведомления о состоянии локальных антивирусных баз	Параметры уведомлений о неактуальности антивирусных баз, которые использует приложение.

Параметр	Описание
Защита паролем	Если переключатель включен, Kaspersky Endpoint Security запрашивает пароль при попытке пользователя совершить операцию, входящую в область действия Защиты паролем. Область действия Защиты паролем включает в себя запрещенные операции (например, выключение компонентов защиты) и учетные записи пользователей, на которые распространяется область действия Защиты паролем. После включения Защиты паролем Kaspersky Endpoint Security предлагает задать пароль для учетной записи KLAdmin.
Поддержка пользователей / **Ссылки на веб-ресурсы** *(доступен только в консоли Kaspersky Security Center)*	Список ссылок на веб-сайты с информацией о технической поддержке приложения Kaspersky Endpoint Security. Добавленные ссылки отображаются в окне **Поддержка** локального интерфейса Kaspersky Endpoint Security вместо стандартных ссылок.
Поддержка пользователей / **Описание** *(доступен только в консоли Kaspersky Security Center)*	Сообщение, которое отображается в окне **Поддержка** локального интерфейса Kaspersky Endpoint Security.

Управление настройками

Вы можете сохранить текущие параметры работы Kaspersky Endpoint Security в файл и использовать их для быстрой настройки приложения на другом компьютере. Также вы можете использовать конфигурационный файл при развертывании приложения через Kaspersky Security Center при помощи инсталляционного пакета. Вы можете в любой момент вернуться к параметрам по умолчанию.

Параметры управления настройками приложения доступны только в интерфейсе Kaspersky Endpoint Security.

Параметры управления настройками приложения

Настройка	Описание
Импортировать	Извлечь настройки работы приложения из файла формата CFG и применить их.
Экспортировать	Сохранить текущие настройки работы приложения в файл формата CFG.
Восстановить	Вы в любое время можете восстановить настройки приложения, рекомендуемые "Лабораторией Касперского". В результате восстановления настроек для всех компонентов защиты будет установлен уровень безопасности **Рекомендуемый**.

Обновление баз и модулей приложения

Обновление баз и модулей приложения Kaspersky Endpoint Security обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие приложения, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули приложения.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) может быть недоступна в приложении на территории США.

Для регулярного обновления требуется действующая лицензия на использование приложения. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

Для успешной загрузки пакета обновлений с серверов обновлений "Лаборатории Касперского" компьютер должен быть подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, требуется настроить параметры прокси-сервера.

Загрузка обновлений осуществляется по протоколу HTTPS. Загрузка по протоколу HTTP может осуществляться в случае, когда загрузка обновлений по протоколу HTTPS невозможна.

В процессе обновления на ваш компьютер загружаются и устанавливаются следующие объекты:

- Базы Kaspersky Endpoint Security. Защита компьютера обеспечивается на основании баз данных, содержащих сигнатуры вирусов и других приложений, представляющих угрозу, и информацию о способах борьбы с ними. Компоненты защиты используют эту информацию при поиске и обезвреживании зараженных файлов на компьютере. Базы регулярно пополняются записями о появляющихся угрозах и способах борьбы с ними. Поэтому рекомендуется регулярно обновлять базы.

  Наряду с базами Kaspersky Endpoint Security обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.

- Модули приложения. Помимо баз Kaspersky Endpoint Security, можно обновлять и модули приложения. Обновления модулей приложения устраняют уязвимости Kaspersky Endpoint Security, добавляют новые функции или улучшают существующие.

В процессе обновления базы и модули приложения на вашем компьютере сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы и модули приложения отличаются от актуальной версии, на компьютер устанавливается недостающая часть обновлений.

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

Информация о текущем состоянии баз Kaspersky Endpoint Security отображается в главном окне приложения или в подсказке при наведении курсора на значок приложения в области уведомлений.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении задачи обновления, записывается в отчет Kaspersky Endpoint Security.

Если приложение работает в режиме Легкого агента, обновление баз и модулей приложения имеет особенности.

Параметры обновления баз и модулей приложения

Параметр	Описание
Расписание обновления баз	**Автоматически**. Режим запуска задачи обновления, при котором приложение Kaspersky Endpoint Security проверяет наличие пакета обновлений в источнике обновлений с определенной периодичностью. Частота проверки наличия пакета обновлений увеличивается во время вирусных эпидемий и сокращается при их отсутствии. Обнаружив свежий пакет обновлений, приложение Kaspersky Endpoint Security скачивает его и устанавливает обновления на компьютер. **Вручную**. Этот режим запуска задачи обновления позволяет вам запускать задачу обновления вручную. **По расписанию**. Режим запуска задачи обновления, при котором приложение Kaspersky Endpoint Security выполняет задачу обновления по сформированному вами расписанию. Если выбран этот режим запуска задачи обновления, вы также можете запускать задачу обновления приложения Kaspersky Endpoint Security вручную.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Endpoint Security запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.
Источники обновлений	*Источник обновлений* – это ресурс, содержащий обновления баз и модулей приложения Kaspersky Endpoint Security. Источником обновлений могут быть сервер Kaspersky Security Center, серверы обновлений "Лаборатории Касперского", сетевая или локальная папка. Если серверы обновлений "Лаборатории Касперского" недоступны, Kaspersky Endpoint Security может использовать альтернативные домены для получения обновлений баз и модулей приложения. Подробнее см. в базе знаний Службы технической поддержки. По умолчанию список источников обновлений содержит сервер Kaspersky Security Center и серверы обновлений "Лаборатории Касперского". Вы можете добавлять в список другие источники обновлений. В качестве источников обновлений можно указывать HTTP- или FTP-серверы, папки общего доступа. Kaspersky Endpoint Security не поддерживает загрузку обновлений с HTTPS-серверов, если это не серверы обновлений "Лаборатории Касперского". Если в качестве источников обновлений выбрано несколько ресурсов, в процессе обновления Kaspersky Endpoint Security обращается к ним строго по списку и выполняет задачу обновления, используя пакет обновлений первого доступного источника обновлений. По умолчанию Kaspersky Endpoint Security использует сервер Kaspersky Security Center в качестве первого источника обновлений. Это позволяет сократить расход трафика при обновлении. Если к компьютеру не применена политика, в параметрах локальной задачи *Обновление баз и модулей приложения* выбраны серверы "Лаборатории Касперского" в качестве первого источника обновления, так как у приложения может отсутствовать доступ к серверу Kaspersky Security Center. Если приложение работает в режиме Легкого агента, в качестве источника обновлений выбрана папка на SVM.
Запускать обновление баз с правами	По умолчанию задача обновления приложения Kaspersky Endpoint Security запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление приложения Kaspersky Endpoint Security может производиться из источника обновления, к которому у пользователя нет прав доступа (например, из папки общего доступа, содержащей пакет обновлений) или для которого не настроено использование аутентификации на прокси-сервере. Вы можете указать пользователя, обладающего этими правами, в параметрах приложения и запускать задачу обновления приложения Kaspersky Endpoint Security от имени этого пользователя.

Параметр	Описание
Загружать обновления модулей приложения	Загрузка обновлений модулей приложения с обновлениями баз приложения. Если флажок установлен, то Kaspersky Endpoint Security уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи обновления включает обновления модулей приложения в пакет обновлений. При этом применение обновлений модулей приложения определяется следующими параметрами: • **Устанавливать критические и одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает критические обновления автоматически, а остальные обновления модулей приложения – после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center. • **Устанавливать только одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center. Этот вариант выбран по умолчанию. Если флажок не установлен, то Kaspersky Endpoint Security не уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи обновления не включает обновления модулей приложения в пакет обновлений. Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения, то приложение устанавливает обновление после согласия с положениями Лицензионного соглашения. По умолчанию флажок установлен.
Копировать обновления в папку	Если флажок установлен, то Kaspersky Endpoint Security копирует пакет обновлений в папку общего доступа, указанную под флажком. Тогда остальные компьютеры локальной сети организации смогут получать пакет обновлений из папки общего доступа. Это позволяет уменьшить интернет-трафик, так как пакет обновлений загружается только один раз. По умолчанию задана следующая папка: `C:\ProgramData\Kaspersky Lab\KES.14.3\Update distribution\`.
Прокси-сервер для обновлений *(доступен только в интерфейсе Kaspersky Endpoint Security)*	Параметры прокси-сервера для доступа пользователей клиентских компьютеров в интернет для обновления баз и модулей приложения. Для автоматической настройки прокси-сервера Kaspersky Endpoint Security использует протокол WPAD (Web Proxy Auto-Discovery Protocol). В случае если по этому протоколу не удается определить IP-адрес прокси-сервера, Kaspersky Endpoint Security использует адрес прокси-сервера, указанный в параметрах браузера Microsoft Internet Explorer.
Не использовать прокси-сервер для локальных адресов *(доступен только в интерфейсе Kaspersky Endpoint Security)*	Если флажок установлен, то при обновлении Kaspersky Endpoint Security из папки общего доступа прокси-сервер не используется.

Удаленный доступ

Данная функция находится на этапе бета-тестирования и доступна только участникам программы бета-тестирования решений "Лаборатории Касперского". Работа функции может быть нестабильной.

В Kaspersky Endpoint Security 14.3 добавлен компонент VPN-агент, который обеспечивает защищенное подключение к корпоративной сети через общедоступные сети. Для этого Kaspersky Endpoint Security использует инфраструктуру Kaspersky NGFW.

Kaspersky Endpoint Security в составе Kaspersky NGWF выполняет следующие функции:

- Установление защищенного соединения с удаленным сервером по протоколу WireGuard.
- Аутентификация пользователя с помощью сертификата на токене.

- Поддержка функции раздельного туннелирования (англ. split tunneling). Функция позволяет модифицировать таблицу маршрутизации компьютера пользователя при установлении VPN-соединения в соответствии с параметрами, заданными администратором на удаленном сервере.

- Централизованное управление сетевыми параметрами и политиками безопасности на компьютере пользователя в Kaspersky Security Center.

Управление Защитой доступа сети выполняется в политике Kaspersky Endpoint Security и политике Kaspersky NGFW. Для работы с политиками Kaspersky NGFW требуется установить плагин Kaspersky NGFW, который входит в комплект поставки.

Параметры Удаленного доступа

Параметр	Описание
Пользовательские удаленные серверы	• **Разрешить пользователям добавлять пользовательские серверы**. Пользователь может вручную настроить параметры подключения к удаленному серверу в интерфейсе приложения. • **Запретить пользователям добавлять пользовательские серверы**. Приложение позволяет выбрать только предустановленные серверы для установления VPN-соединения.
Время ожидания (сек.)	Максимальное время ожидания ответа от удаленного сервера. Если в течение заданного периода установить соединение с удаленным сервером не удалось, приложение отображает сообщение об ошибке.
Предустановленные удаленные серверы	Удаленные серверы, которые будут доступны пользователю в интерфейсе приложения. Таким образом, пользователю не нужно вводить адрес удаленного сервера вручную. Пользователь не может изменить адрес предустановленного сервера, заданный в политике. Приложение выполняет подключение к предустановленному серверу автоматически. Администратор может добавить несколько серверов для повышения отказоустойчивости. Если установить соединение с одним сервером не удалось, пользователь может попробовать подключиться к другому серверу.

Приложение 2. Группы доверия приложений

Все приложения, запускаемые на компьютере, Kaspersky Endpoint Security распределяет на группы доверия. Приложения распределяются на группы доверия в зависимости от степени угрозы, которую эти приложения могут представлять для операционной системы.

Существуют следующие группы доверия:

- **Доверенные**. В группу входят приложения, для которых выполняется одно или более следующих условий:

  - Приложения обладают цифровой подписью доверенных производителей.

  - О приложениях есть записи в базе доверенных приложений Kaspersky Security Network.

  - Пользователь поместил приложение в группу *Доверенные*.

  Запрещенных операций для таких приложений нет.

- **Слабые ограничения**. В группу входят приложения, для которых выполняются следующие условия:

  - Приложения не обладают цифровой подписью доверенных производителей.

  - О приложениях нет записей в базе доверенных приложений Kaspersky Security Network.

  - Пользователь поместил приложение в группу *Слабые ограничения*.

  Такие приложения имеют минимальные ограничения на работу с ресурсами операционной системы.

- **Сильные ограничения**. В группу входят приложения, для которых выполняются следующие условия:
  - Приложения не обладают цифровой подписью доверенных производителей.
  - О приложениях нет записей в базе доверенных приложений Kaspersky Security Network.
  - Пользователь поместил приложение в группу *Сильные ограничения*.

  Такие приложения имеют значительные ограничения на работу с ресурсами операционной системы.
- **Недоверенные**. В группу входят приложения, для которых выполняются следующие условия:
  - Приложения не обладают цифровой подписью доверенных производителей.
  - О приложениях нет записей в базе доверенных приложений Kaspersky Security Network.
  - Пользователь поместил приложение в группу *Недоверенные*.

  Для таких приложений запрещены все операции.

Приложение 3. Расширения файлов для быстрой проверки съемных дисков

com – исполняемый файл приложения размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив;

sys – системный файл Microsoft Windows;

prg – текст приложения dBase™, Clipper или Microsoft Visual FoxPro®, приложение пакета WAVmaker;

bin – бинарный файл;

bat – файл пакетного задания;

cmd – командный файл Microsoft Windows NT (аналогичен bat-файлу для DOS), OS/2;

dpl – упакованная библиотека Borland Delphi;

dll – библиотека динамической загрузки;

scr – файл-заставка экрана Microsoft Windows;

cpl – модуль панели управления (control panel) в Microsoft Windows;

ocx – объект Microsoft OLE (Object Linking and Embedding);

tsp – приложение, работающее в режиме разделения времени;

drv – драйвер некоторого устройства;

vxd – драйвер виртуального устройства Microsoft Windows;

pif – файл с информацией о приложении;

lnk – файл-ссылка в Microsoft Windows;

reg – файл регистрации ключей системного реестра Microsoft Windows;

ini – файл конфигурации, который содержит данные настроек для Microsoft Windows, Windows NT и некоторых приложений;

cla – класс Java;

vbs – скрипт Visual Basic®;

vbe – видеорасширение BIOS;

js, jse – исходный текст JavaScript;

htm – гипертекстовый документ;

htt – гипертекстовая заготовка Microsoft Windows;

hta – гипертекстовое приложение для Microsoft Internet Explorer®;

asp – скрипт Active Server Pages;

chm – скомпилированный HTML-файл;

pht – HTML-файл со встроенными скриптами PHP;

php – скрипт, встраиваемый в HTML-файлы;

wsh – файл Microsoft Windows Script Host;

wsf – скрипт Microsoft Windows;

the – файл заставки для рабочего стола Microsoft Windows 95;

hlp – файл справки формата Win Help;

msg – сообщение электронной почты Microsoft Mail;

plg – сообщение электронной почты;

mbx – сохраненное сообщение электронной почты Microsoft Office Outlook;

doc* – документы Microsoft Office Word, такие как: doc – документ Microsoft Office Word, docx – документ Microsoft Office Word 2007 с поддержкой языка XML, docm – документ Microsoft Office Word 2007 с поддержкой макросов;

dot* – шаблоны документа Microsoft Office Word, такие как: dot – шаблон документа Microsoft Office Word, dotx – шаблон документа Microsoft Office Word 2007, dotm – шаблон документа Microsoft Office Word 2007 с поддержкой макросов;

fpm – приложение баз данных, стартовый файл Microsoft Visual FoxPro;

rtf – документ в формате Rich Text Format;

shs – фрагмент Windows Shell Scrap Object Handler;

dwg – база данных чертежей AutoCAD®;

msi – пакет Microsoft Windows Installer;

otm – VBA-проект для Microsoft Office Outlook;

pdf – документ Adobe Acrobat;

swf – объект пакета Shockwave® Flash;

jpg, jpeg – файл графического формата хранения сжатых изображений;

emf – файл формата Enhanced Metafile;

ico – файл значка объекта;

ov? – исполняемые файлы Microsoft Office Word;

xl* – документы и файлы Microsoft Office Excel, такие как: xla – расширение Microsoft Office Excel, xlc – диаграмма, xlt – шаблон документа, xlsx – рабочая книга Microsoft Office Excel 2007, xltm – рабочая книга Microsoft Office Excel 2007 с поддержкой макросов, xlsb – рабочая книга Microsoft Office Excel 2007 в бинарном (не XML) формате, xltx – шаблон Microsoft Office Excel 2007, xlsm – шаблон Microsoft Office Excel 2007 с поддержкой макросов, xlam – надстройка Microsoft Office Excel 2007 с поддержкой макросов;

pp* – документы и файлы Microsoft Office PowerPoint®, такие как: pps – слайд Microsoft Office PowerPoint, ppt – презентация, pptx – презентация Microsoft Office PowerPoint 2007, pptm – презентация Microsoft Office PowerPoint 2007 с поддержкой макросов, potx – шаблон презентации Microsoft Office PowerPoint 2007, potm – шаблон презентации Microsoft Office PowerPoint 2007 с поддержкой макросов, ppsx – слайд-шоу Microsoft Office PowerPoint 2007, ppsm – слайд-шоу Microsoft Office PowerPoint 2007 с поддержкой макросов, ppam – надстройка Microsoft Office PowerPoint 2007 с поддержкой макросов;

md* – документы и файлы Microsoft Office Access®, такие как: mda – рабочая группа Microsoft Office Access, mdb – база данных;

sldx – слайд Microsoft Office PowerPoint 2007;

sldm – слайд Microsoft Office PowerPoint 2007 с поддержкой макросов;

thmx – тема Microsoft Office 2007.

Приложение 4. Типы файлов для фильтра вложений Защиты от почтовых угроз

Следует помнить, что фактический формат файла может не совпадать с форматом, указанным в расширении файла.

Если вы включили фильтрацию вложений в сообщениях электронной почты, то в результате фильтрации компонент Защита от почтовых угроз может переименовывать или удалять файлы следующих расширений:

com – исполняемый файл приложения размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив;

sys – системный файл Microsoft Windows;

prg – текст приложения dBase™, Clipper или Microsoft Visual FoxPro®, приложение пакета WAVmaker;

bin – бинарный файл;

bat – файл пакетного задания;

cmd – командный файл Microsoft Windows NT (аналогичен bat-файлу для DOS), OS/2;

dpl – упакованная библиотека Borland Delphi;

dll – библиотека динамической загрузки;

scr – файл-заставка экрана Microsoft Windows;

cpl – модуль панели управления (control panel) в Microsoft Windows;

ocx – объект Microsoft OLE (Object Linking and Embedding);

tsp – приложение, работающее в режиме разделения времени;

drv – драйвер некоторого устройства;

vxd – драйвер виртуального устройства Microsoft Windows;

pif – файл с информацией о приложении;

lnk – файл-ссылка в Microsoft Windows;

reg – файл регистрации ключей системного реестра Microsoft Windows;

ini – файл конфигурации, который содержит данные настроек для Microsoft Windows, Windows NT и некоторых приложений;

cla – класс Java;

vbs – скрипт Visual Basic®;

vbe – видеорасширение BIOS;

js, jse – исходный текст JavaScript;

htm – гипертекстовый документ;

htt – гипертекстовая заготовка Microsoft Windows;

hta – гипертекстовое приложение для Microsoft Internet Explorer®;

asp – скрипт Active Server Pages;

chm – скомпилированный HTML-файл;

pht – HTML-файл со встроенными скриптами PHP;

php – скрипт, встраиваемый в HTML-файлы;

wsh – файл Microsoft Windows Script Host;

wsf – скрипт Microsoft Windows;

the – файл заставки для рабочего стола Microsoft Windows 95;

hlp – файл справки формата Win Help;

msg – сообщение электронной почты Microsoft Mail;

plg – сообщение электронной почты;

mbx – сохраненное сообщение электронной почты Microsoft Office Outlook;

doc* – документы Microsoft Office Word, такие как: doc – документ Microsoft Office Word, docx – документ Microsoft Office Word 2007 с поддержкой языка XML, docm – документ Microsoft Office Word 2007 с поддержкой макросов;

dot* – шаблоны документа Microsoft Office Word, такие как: dot – шаблон документа Microsoft Office Word, dotx – шаблон документа Microsoft Office Word 2007, dotm – шаблон документа Microsoft Office Word 2007 с поддержкой макросов;

fpm – приложение баз данных, стартовый файл Microsoft Visual FoxPro;

rtf – документ в формате Rich Text Format;

shs – фрагмент Windows Shell Scrap Object Handler;

dwg – база данных чертежей AutoCAD®;

msi – пакет Microsoft Windows Installer;

otm – VBA-проект для Microsoft Office Outlook;

pdf – документ Adobe Acrobat;

swf – объект пакета Shockwave® Flash;

jpg, jpeg – файл графического формата хранения сжатых изображений;

emf – файл формата Enhanced Metafile;

ico – файл значка объекта;

ov? – исполняемые файлы Microsoft Office Word;

xl* – документы и файлы Microsoft Office Excel, такие как: xla – расширение Microsoft Office Excel, xlc – диаграмма, xlt – шаблон документа, xlsx – рабочая книга Microsoft Office Excel 2007, xltm – рабочая книга Microsoft Office Excel 2007 с поддержкой макросов, xlsb – рабочая книга Microsoft Office Excel 2007 в бинарном (не XML) формате, xltx – шаблон Microsoft Office Excel 2007, xlsm – шаблон Microsoft Office Excel 2007 с поддержкой макросов, xlam – надстройка Microsoft Office Excel 2007 с поддержкой макросов;

pp* – документы и файлы Microsoft Office PowerPoint®, такие как: pps – слайд Microsoft Office PowerPoint, ppt – презентация, pptx – презентация Microsoft Office PowerPoint 2007, pptm – презентация Microsoft Office PowerPoint 2007 с поддержкой макросов, potx – шаблон презентации Microsoft Office PowerPoint 2007, potm – шаблон презентации Microsoft Office PowerPoint 2007 с поддержкой макросов, ppsx – слайд-шоу Microsoft Office PowerPoint 2007, ppsm – слайд-шоу Microsoft Office PowerPoint 2007 с поддержкой макросов, ppam – надстройка Microsoft Office PowerPoint 2007 с поддержкой макросов;

md* – документы и файлы Microsoft Office Access®, такие как: mda – рабочая группа Microsoft Office Access, mdb – база данных;

sldx – слайд Microsoft Office PowerPoint 2007;

sldm – слайд Microsoft Office PowerPoint 2007 с поддержкой макросов;

thmx – тема Microsoft Office 2007.

Приложение 5. Сетевые параметры для взаимодействия с внешними службами

Kaspersky Endpoint Security и Kaspersky Security Center используют защищенный канал связи с TLS (Transport Layer Security) для работы с внешними службами "Лаборатории Касперского".

Приложение Kaspersky Endpoint Security использует следующие сетевые параметры для взаимодействия с внешними службами.

Сетевые параметры

Адрес	Описание
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Протокол: `HTTPS` Порт: `443`	Активация приложения.

Адрес	Описание

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Протокол: `HTTPS`
Порт: `443`
	Обновление баз и модулей приложения.

`downloads.upd.kaspersky.com` Протокол: `HTTPS` Порт: `443`	• Обновление баз и модулей приложения. • Проверка доступа к серверам "Лаборатории Касперского". При сбоях доступа к серверам через системный DNS приложение будет использовать публичный DNS. Это нужно для обновления антивирусных баз и поддержки уровня безопасности компьютера. Приложение Kaspersky Endpoint Security будет использовать следующие публичные DNS в порядке их обхода: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Запросы приложения могут содержать адреса доменов и внешний IP-адрес пользователя, так как приложение устанавливает с DNS-сервером TCP/UDP-соединение. Эти данные нужны, например, для проверки сертификата веб-ресурса при обращении по HTTPS. Если приложение Kaspersky Endpoint Security использует публичный DNS-сервер, правила обработки данных регламентируются Политикой конфиденциальности этого сервиса. Если требуется запретить приложению Kaspersky Endpoint Security использовать публичный DNS-сервер, обратитесь в Службу технической поддержки за приватным патчем.
`touch.kaspersky.com` Протокол: `HTTP`	• Получение доверенного времени для проверки срока действия сертификата (TLS-соединение). • Предупреждение о запрете доступа к веб-ресурсу в браузере при работе Защиты от веб-угроз.

Адрес	Описание

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Протокол: `HTTP`
Порт: `80`
	Обновление баз и модулей приложения.

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Протокол: `HTTPS`
Порт: `443`
	Использование Kaspersky Security Network.

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Протокол: `KSN`
Порт: `443`, `1443`
	Использование Kaspersky Security Network.

`click.kaspersky.com`
 	
`redirect.kaspersky.com`
Протокол: `HTTPS`
Порт: `443`
	Переход по ссылкам из интерфейса.

Параметры, использующиеся для шифрования

Адрес	Описание

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Протокол: `HTTP`
Порт: `80`
	Инфраструктура открытых ключей (англ. Public Key Infrastructure, PKI).

Приложение 6. События приложения

Информация о работе каждого компонента Kaspersky Endpoint Security, о событиях шифрования данных, о выполнении каждой задачи поиска вредоносного ПО, задачи обновления и задачи проверки целостности, а также о работе приложения в целом сохраняется в журнале событий Kaspersky Security Center и журнале событий Windows.

Kaspersky Endpoint Security формирует события следующих типов: общие и специфические события. Специфические события создает только приложение Kaspersky Endpoint Security для Windows. Специфические события имеют простой идентификатор, например, `000000cb`. Специфические события содержат следующие обязательные параметры:

- `GNRL_EA_DESCRIPTION` – содержание события.
- `GNRL_EA_ID` – служебный идентификатор события.
- `GNRL_EA_SEVERITY` – статус события. `1` – *Информационное сообщение*, `2` – *Предупреждение*, `3` – *Отказ функционирования*, `4` – *Критическое*.
- `EVENT_TYPE_DISPLAY_NAME` – заголовок события.
- `TASK_DISPLAY_NAME` – название компонента приложения, который инициировал событие.

Общие события, кроме Kaspersky Endpoint Security для Windows, могут создавать и другие приложения "Лаборатории Касперского" (например, Kaspersky Security для Windows Server). Общие события имеют более сложный идентификатор, например, `GNRL_EV_VIRUS_FOUND`. Общие события кроме обязательных параметров содержат еще дополнительные параметры.

Сколько времени события хранятся на сервере

Критическое

Срок действия лицензии истек

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	`201`
Идентификатор события Kaspersky Security Center	`GNRL_EV_LICENSE_EXPIRATION`
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Срок действия лицензии почти истек

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	`203`

Идентификатор события Kaspersky Security Center	000000cb
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Базы повреждены или отсутствуют

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	206
Идентификатор события Kaspersky Security Center	000000ce
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Базы сильно устарели

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	207
Идентификатор события Kaspersky Security Center	000000cf
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Автозапуск приложения выключен

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	209
Идентификатор события Kaspersky Security Center	000000d1
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка активации

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	229
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружена активная угроза. Требуется запуск процедуры лечения активного заражения

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	231
Идентификатор события Kaspersky Security Center	000000e7

Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Серверы KSN недоступны

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	2023
Идентификатор события Kaspersky Security Center	000007e7
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Недостаточно места в хранилище карантина

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	343
Идентификатор события Kaspersky Security Center	00000157
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект не восстановлен из карантина

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	346
Идентификатор события Kaspersky Security Center	0000015a
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект не удален из карантина

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	348
Идентификатор события Kaspersky Security Center	0000015c
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Приложение установило соединение с сайтом с недоверенным сертификатом

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	57
Идентификатор события Kaspersky Security Center	00000039

Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Возникла ошибка проверки зашифрованного соединения. Домен добавлен в список исключений

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	`60`
Идентификатор события Kaspersky Security Center	`0000003c`
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружен вредоносный объект (локальные базы)

Статус	!
Компонент	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз AMSI-защита Предотвращение вторжений Анализ поведения Защита от шифрования Защита от эксплойтов Поиск вредоносного ПО
Идентификатор события Windows	`302`
Идентификатор события Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Параметры события	• `GNRL_EA_PARAM_1` – хеш объекта (SHA256). • `GNRL_EA_PARAM_2` – название объекта. При обнаружении внешнего шифрования папок общего доступа приложение показывает путь к целевому файлу. • `GNRL_EA_PARAM_5` – название угрозы по классификации "Лаборатории Касперского", например, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` – имя сессионного пользователя. • `GNRL_EA_PARAM_8` – тип угрозы (`type`). • `GNRL_EA_PARAM_9` – дополнительная информация об обнаружении объекта: Компонент приложения (`engine`). Технология обнаружения угроз (`method`). Угроза обнаружена с помощью Kaspersky Private Security Network (`blacklist`): `true` или `false`. Версия EDR. Идентификатор угрозы в EDR. Хеш объекта MD5.
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружен вредоносный объект (KSN)

Статус	!
Компонент	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз AMSI-защита Предотвращение вторжений Анализ поведения Защита от шифрования Защита от эксплойтов Поиск вредоносного ПО
Идентификатор события Windows	302
Идентификатор события Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_BY_KSN
Параметры события	• GNRL_EA_PARAM_1 – хеш объекта (SHA256). • GNRL_EA_PARAM_2 – название объекта. • GNRL_EA_PARAM_5 – название угрозы по классификации "Лаборатории Касперского", например, EICAR-Test-File. • GNRL_EA_PARAM_7 – имя сессионного пользователя. • GNRL_EA_PARAM_8 – тип угрозы (type). • GNRL_EA_PARAM_9 – дополнительная информация об обнаружении объекта: Компонент приложения (engine). Технология обнаружения угроз (method). Угроза обнаружена с помощью Kaspersky Private Security Network (blacklist): true или false. Версия EDR. Идентификатор угрозы в EDR. Хеш объекта MD5.
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Лечение невозможно

Статус	!
Компонент	Защита от файловых угроз Защита от почтовых угроз Предотвращение вторжений Анализ поведения Защита от шифрования Поиск вредоносного ПО
Идентификатор события Windows	312
Идентификатор события Kaspersky Security Center	GNRL_EV_OBJECT_NOTCURED
Параметры события	• GNRL_EA_PARAM_1 – хеш объекта (SHA256). • GNRL_EA_PARAM_2 – название объекта. • GNRL_EA_PARAM_5 – название угрозы по классификации "Лаборатории Касперского", например, EICAR-Test-File. • GNRL_EA_PARAM_7 – имя сессионного пользователя. • GNRL_EA_PARAM_8 – тип угрозы (type). • GNRL_EA_PARAM_9 – дополнительная информация об обнаружении объекта: Компонент приложения (engine). Технология обнаружения угроз (method). Угроза обнаружена с помощью Kaspersky Private Security Network (blacklist): true или false. Версия EDR. Идентификатор угрозы в EDR. Хеш объекта MD5.
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Невозможно удалить

Статус	!
Компонент	Защита от файловых угроз Предотвращение вторжений Анализ поведения Защита от шифрования Поиск вредоносного ПО
Идентификатор события Windows	313
Идентификатор события Kaspersky Security Center	00000139
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка обработки

Статус	!
Компонент	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз Предотвращение вторжений AMSI-защита Поиск вредоносного ПО
Идентификатор события Windows	317
Идентификатор события Kaspersky Security Center	0000013d
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Процесс завершен

Статус	!
Компонент	Защита от файловых угроз Предотвращение вторжений Анализ поведения Поиск вредоносного ПО
Идентификатор события Windows	452
Идентификатор события Kaspersky Security Center	000001c4
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Невозможно завершить процесс

Статус	!
Компонент	Защита от файловых угроз Предотвращение вторжений Анализ поведения Поиск вредоносного ПО
Идентификатор события Windows	453
Идентификатор события Kaspersky Security Center	000001c5
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Заблокирована опасная ссылка

Статус	!
Компонент	Защита от веб-угроз
Идентификатор события Windows	362
Идентификатор события Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
Параметры события	• GNRL_EA_PARAM_2 – путь к объекту. • GNRL_EA_PARAM_5 – название угрозы по классификации "Лаборатории Касперского". • GNRL_EA_PARAM_7 – имя сессионного пользователя. • GNRL_EA_PARAM_8 – тип угрозы (type). • GNRL_EA_PARAM_9 – дополнительная информация об обнаружении объекта: Компонент приложения (engine). Технология обнаружения угроз (method). Угроза обнаружена с помощью Локального KSN (blacklist): true или false.
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Открыта опасная ссылка

Статус	!
Компонент	Защита от веб-угроз
Идентификатор события Windows	363
Идентификатор события Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_REPORTED
Параметры события	• GNRL_EA_PARAM_2 – путь к объекту. • GNRL_EA_PARAM_5 – название угрозы по классификации "Лаборатории Касперского". • GNRL_EA_PARAM_7 – имя сессионного пользователя. • GNRL_EA_PARAM_8 – тип угрозы (type). • GNRL_EA_PARAM_9 – дополнительная информация об обнаружении объекта: Компонент приложения (engine). Технология обнаружения угроз (method). Угроза обнаружена с помощью Локального KSN (blacklist): true или false.
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружена ранее открытая опасная ссылка

Статус	!
Компонент	Защита от веб-угроз
Идентификатор события Windows	1201
Идентификатор события Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_PASSED
Параметры события	• GNRL_EA_PARAM_2 – путь к объекту. • GNRL_EA_PARAM_5 – название угрозы по классификации "Лаборатории Касперского". • GNRL_EA_PARAM_7 – имя сессионного пользователя. • GNRL_EA_PARAM_8 – тип угрозы (type). • GNRL_EA_PARAM_9 – дополнительная информация об обнаружении объекта: Компонент приложения (engine). Технология обнаружения угроз (method). Угроза обнаружена с помощью Локального KSN (blacklist): true или false.

Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Действие процесса заблокировано

Статус	!
Компонент	Адаптивный контроль аномалий
Идентификатор события Windows	`2200`
Идентификатор события Kaspersky Security Center	`GNRL_EV_ADSEC_DETECT`
Параметры события	• `GNRL_EA_PARAM_1` – название правила Адаптивного контроля аномалий. • `GNRL_EA_PARAM_2` – идентификатор эвристического правила. • `GNRL_EA_PARAM_3` – имя сессионного пользователя. • `GNRL_EA_PARAM_4` – исходный процесс. • `GNRL_EA_PARAM_5` – исходный объект. • `GNRL_EA_PARAM_6` – целевой процесс. • `GNRL_EA_PARAM_7` – целевой объект. • `GNRL_EA_PARAM_8` – дополнительная информация об обнаружении объекта: Контрольные суммы исходного процесса / объекта и целевого процесса / объекта. Блокирование процесса (`verdict_type`): `true` или `false`. Идентификатор безопасности пользователя (SID).
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Клавиатура не авторизована

Статус	!
Компонент	Защита от атак BadUSB
Идентификатор события Windows	`2051`
Идентификатор события Kaspersky Security Center	`00000803`
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

AMSI-запрос заблокирован

Статус	!
Компонент	AMSI-защита
Идентификатор события Windows	`2200`
Идентификатор события Kaspersky Security Center	`00000898`
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сетевая активность запрещена

Статус	!
Компонент	Сетевой экран
Идентификатор события Windows	`602`
Идентификатор события Kaspersky Security Center	`00000329`

Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружена сетевая атака

Статус	ⓘ
Компонент	Защита от сетевых угроз
Идентификатор события Windows	651
Идентификатор события Kaspersky Security Center	GNRL_EV_ATTACK_DETECTED
Параметры события	• GNRL_EA_PARAM_1 – название атаки. • GNRL_EA_PARAM_2 – протокол. • GNRL_EA_PARAM_3 – IP-адрес компьютера, с которого осуществляется сетевая атака. IP-адрес указан в порядке байтов хоста. Например, 2886729929 для 172.16.0.201. • GNRL_EA_PARAM_4 – номер порта. • GNRL_EA_PARAM_5 – IPv6-адрес, например, 12B012B012B012B012B012B012B012B0. • GNRL_EA_PARAM_6 – IP-адрес компьютера, на который осуществляется сетевая атака. IP-адрес указан в порядке байтов хоста. Например, 2886729929 для 172.16.0.201.
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запуск приложения запрещен

Статус	ⓘ
Компонент	Контроль приложений
Идентификатор события Windows	702
Идентификатор события Kaspersky Security Center	GNRL_EV_APPLICATION_LAUNCH_DENIED
Параметры события	• GNRL_EA_PARAM_2 – имя сессионного пользователя. • GNRL_EA_PARAM_3 – идентификатор категории, созданной вручную. • GNRL_EA_PARAM_4 – идентификатор категории приложений. • GNRL_EA_PARAM_5 – информация о цифровой подписи приложения. • GNRL_EA_PARAM_6 – имя исполняемого файла приложения (например, chrome.exe). • GNRL_EA_PARAM_7 – путь к исполняемому файлу. • GNRL_EA_PARAM_8 – хеш объекта (SHA256). • GNRL_EA_PARAM_9 – версия приложения, которую пользователь пытается запустить.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запрещенный процесс был запущен до старта Kaspersky Endpoint Security для Windows

Статус	ⓘ
Компонент	Контроль приложений
Идентификатор события Windows	710
Идентификатор события Kaspersky Security Center	000002c6
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Доступ запрещен (локальные базы)

Статус	!
Компонент	Веб-Контроль
Идентификатор события Windows	752
Идентификатор события Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Параметры события	• GNRL_EA_PARAM_1 – URL-адрес. • GNRL_EA_PARAM_2 – имя сессионного пользователя. • GNRL_EA_PARAM_3 – название правила Веб-Контроля.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Доступ запрещен (KSN)

Статус	!
Компонент	Веб-Контроль
Идентификатор события Windows	752
Идентификатор события Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Параметры события	• GNRL_EA_PARAM_1 – URL-адрес. • GNRL_EA_PARAM_2 – имя сессионного пользователя. • GNRL_EA_PARAM_3 – название правила Веб-Контроля.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Операция с устройством запрещена

Статус	!
Компонент	Контроль устройств
Идентификатор события Windows	802
Идентификатор события Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Параметры события	• GNRL_EA_PARAM_1 – идентификатор устройства (англ. Hardware ID, HWID). • GNRL_EA_PARAM_2 – имя сессионного пользователя.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сетевое соединение заблокировано

Статус	!
Компонент	Контроль устройств
Идентификатор события Windows	809
Идентификатор события Kaspersky Security Center	00000329
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Операция с устройством запрещена до запуска Kaspersky Endpoint Security для Windows

Статус	!
Компонент	Контроль устройств
Идентификатор события Windows	816
Идентификатор события Kaspersky Security Center	00000330
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Подключение устройства заблокировано до запуска Kaspersky Endpoint Security для Windows

Статус	!
Компонент	Контроль устройств
Идентификатор события Windows	817
Идентификатор события Kaspersky Security Center	00000331
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка обновления компонента

Статус	!
Компонент	Обновление
Идентификатор события Windows	1011
Идентификатор события Kaspersky Security Center	000003f3
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка копирования обновлений компонента

Статус	!
Компонент	Обновление
Идентификатор события Windows	1012
Идентификатор события Kaspersky Security Center	000003f4
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Локальная ошибка обновления

Статус	!
Компонент	Обновление
Идентификатор события Windows	1014
Идентификатор события Kaspersky Security Center	000003f6
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Сетевая ошибка обновления

Статус	!
Компонент	Обновление
Идентификатор события Windows	1015
Идентификатор события Kaspersky Security Center	000003f7
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Невозможен запуск двух задач одновременно

Статус	!
Компонент	Обновление
Идентификатор события Windows	1017
Идентификатор события Kaspersky Security Center	000003f9
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка проверки баз и модулей приложения

Статус	!
Компонент	Обновление
Идентификатор события Windows	1018
Идентификатор события Kaspersky Security Center	000003fa
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка взаимодействия с Kaspersky Security Center

Статус	!
Компонент	Обновление
Идентификатор события Windows	1019
Идентификатор события Kaspersky Security Center	000003fb
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обновлены не все компоненты

Статус	!
Компонент	Обновление
Идентификатор события Windows	1021
Идентификатор события Kaspersky Security Center	000003fd
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обновление завершено успешно, а копирование обновлений завершено с ошибкой

Статус	!
Компонент	Обновление
Идентификатор события Windows	1023
Идентификатор события Kaspersky Security Center	000003ff
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Внутренняя ошибка задачи

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	101
Идентификатор события Kaspersky Security Center	00000065
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Ошибка установки патча

Статус	!
Компонент	Обновление
Идентификатор события Windows	2153
Идентификатор события Kaspersky Security Center	00000869
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка отката патча

Статус	!
Компонент	Обновление
Идентификатор события Windows	2156
Идентификатор события Kaspersky Security Center	0000086c
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка применения правил шифрования / расшифровки файлов

Статус	!
Компонент	Шифрование данных
Идентификатор события Windows	904
Идентификатор события Kaspersky Security Center	00000388
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка шифрования / расшифровки файла

Статус	!
Компонент	Шифрование данных
Идентификатор события Windows	912
Идентификатор события Kaspersky Security Center	GNRL_EV_ENCRYPTION_ERROR
Параметры события	• GNRL_EA_PARAM_1 – путь к файлу. • GNRL_EA_PARAM_2 – причина ошибки. • GNRL_EA_PARAM_3 – тип устройства.
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Заблокирован доступ к файлу

Статус	!
Компонент	Шифрование данных
Идентификатор события Windows	940
Идентификатор события Kaspersky Security Center	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
Параметры события	• GNRL_EA_PARAM_1 – целевой объект. • GNRL_EA_PARAM_2 – имя сессионного пользователя. • GNRL_EA_PARAM_3 – имя исполняемого файла приложения (например, chrome.exe), которое пытается получить доступ к файлу.
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Ошибка активации портативного режима

Статус	!
Компонент	Шифрование данных
Идентификатор события Windows	951
Идентификатор события Kaspersky Security Center	000003b7
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка деактивации портативного режима

Статус	!
Компонент	Шифрование данных
Идентификатор события Windows	953
Идентификатор события Kaspersky Security Center	000003b9
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка создания зашифрованного архива

Статус	!
Компонент	Шифрование данных
Идентификатор события Windows	931
Идентификатор события Kaspersky Security Center	000003a3
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка шифрования / расшифровки устройства

Статус	!
Компонент	Шифрование данных
Идентификатор события Windows	1305
Идентификатор события Kaspersky Security Center	00000519
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Не удалось загрузить модуль шифрования

Статус	!
Компонент	Шифрование данных
Идентификатор события Windows	1311
Идентификатор события Kaspersky Security Center	0000051f
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Задача управления учетными записями Агента аутентификации завершилась ошибкой

Статус	!
Компонент	Шифрование данных
Идентификатор события Windows	1340
Идентификатор события Kaspersky Security Center	0000053c
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Политика не может быть применена

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	1312
Идентификатор события Kaspersky Security Center	00000520
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обновление функциональности шифрования завершено с ошибкой

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1342
Идентификатор события Kaspersky Security Center	0000053e
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Откат обновления функциональности шифрования завершен с ошибкой (более подробная информация доступна в онлайн-справке для Kaspersky Endpoint Security для Windows)

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1344
Идентификатор события Kaspersky Security Center	00000540
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сервер Kaspersky Anti Targeted Attack Platform недоступен

Статус	ⓘ
Компонент	Endpoint Sensor
Идентификатор события Windows	2100
Идентификатор события Kaspersky Security Center	00000834
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка удаления объекта

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2252
Идентификатор события Kaspersky Security Center	000008cc
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект не помещен на карантин (Sandbox)

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2603
Идентификатор события Kaspersky Security Center	00000a2b
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Возникла внутренняя ошибка

Статус	!
Компонент	Sandbox
Идентификатор события Windows	2607
Идентификатор события Kaspersky Security Center	00000a2f
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сертификат сервера Sandbox недействителен

Статус	!
Компонент	Sandbox
Идентификатор события Windows	2613
Идентификатор события Kaspersky Security Center	00000a35
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Узел Sandbox недоступен

Статус	!
Компонент	Sandbox
Идентификатор события Windows	2614
Идентификатор события Kaspersky Security Center	00000a36
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обработка объекта в Sandbox завершилась с ошибкой

Статус	!
Компонент	Sandbox
Идентификатор события Windows	2617
Идентификатор события Kaspersky Security Center	00000a39
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Превышена допустимая нагрузка на Sandbox

Статус	!
Компонент	Sandbox
Идентификатор события Windows	2618
Идентификатор события Kaspersky Security Center	00000a3a
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

IOC обнаружен

Статус	ⓘ
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2651
Идентификатор события Kaspersky Security Center	00000a5b
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Возникла ошибка при проверке лицензии Sandbox

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2620
Идентификатор события Kaspersky Security Center	00000a3c
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка отправки задачи проверки в Sandbox пользователем

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2623
Идентификатор события Kaspersky Security Center	00000a3e
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка создания задачи Sandbox

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2621
Идентификатор события Kaspersky Security Center	00000a3d
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запрещен запуск объекта

Статус	ⓘ
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2553
Идентификатор события Kaspersky Security Center	000009f9
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запрещен запуск процесса

Статус	!
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2551
Идентификатор события Kaspersky Security Center	000009f7
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запрещено выполнение скрипта

Статус	!
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2559
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект не помещен на карантин (Endpoint Detection and Response)

Статус	!
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2556
Идентификатор события Kaspersky Security Center	000009fc
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запуск процесса не заблокирован

Статус	!
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2561
Идентификатор события Kaspersky Security Center	00000a01
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект не заблокирован

Статус	!
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2562
Идентификатор события Kaspersky Security Center	00000a02
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Выполнение скрипта не заблокировано

Статус	!
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2563
Идентификатор события Kaspersky Security Center	00000a03
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка изменения состава компонентов приложения

Статус	!
Компонент	Системный аудит
Идентификатор события Windows	1401
Идентификатор события Kaspersky Security Center	00000579
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружена возможная попытка взлома пароля с помощью подбора

Статус	!
Компонент	Анализ журналов
Идентификатор события Windows	2800
Идентификатор события Kaspersky Security Center	00000af0
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружены признаки компрометации журналов Windows

Статус	!
Компонент	Анализ журналов
Идентификатор события Windows	2801
Идентификатор события Kaspersky Security Center	00000af1
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружена подозрительная активность со стороны новой установленной службы

Статус	!
Компонент	Анализ журналов
Идентификатор события Windows	2802
Идентификатор события Kaspersky Security Center	00000af2
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружена подозрительная аутентификация с явным указанием учетных данных

Статус	!
Компонент	Анализ журналов
Идентификатор события Windows	2803
Идентификатор события Kaspersky Security Center	00000af3
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружены признаки атаки Kerberos forged PAC (MS14-068)

Статус	!
Компонент	Анализ журналов
Идентификатор события Windows	2804
Идентификатор события Kaspersky Security Center	00000af4
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружены подозрительные изменения привилегированной группы Администраторы

Статус	!
Компонент	Анализ журналов
Идентификатор события Windows	2805
Идентификатор события Kaspersky Security Center	00000af5
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружена подозрительная активность во время сетевого сеанса входа

Статус	!
Компонент	Анализ журналов
Идентификатор события Windows	2806
Идентификатор события Kaspersky Security Center	00000af6
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сработало правило Анализа журналов

Статус	!
Компонент	Анализ журналов
Идентификатор события Windows	2807
Идентификатор события Kaspersky Security Center	00000af7
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Подозрительное событие повторяется слишком часто. Запущено формирование агрегированных событий

Статус	!
Компонент	Анализ журналов
Идентификатор события Windows	2808
Идентификатор события Kaspersky Security Center	00000af8
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Отчет о подозрительном событии за период агрегации

Статус	!
Компонент	Анализ журналов
Идентификатор события Windows	2809
Идентификатор события Kaspersky Security Center	00000af9
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка подключения к серверу EDR Expert

Статус	!
Компонент	Endpoint Detection and Response Expert (on-premises)
Идентификатор события Windows	2850
Идентификатор события Kaspersky Security Center	00000b22
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат сервера EDR Expert

Статус	!
Компонент	Endpoint Detection and Response Expert (on-premises)
Идентификатор события Windows	2851
Идентификатор события Kaspersky Security Center	00000b23
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат агента на сервере EDR Expert

Статус	!
Компонент	Endpoint Detection and Response Expert (on-premises)
Идентификатор события Windows	2852
Идентификатор события Kaspersky Security Center	00000b24
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка подключения к серверу реагирования EDR Expert

Статус	!
Компонент	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Идентификатор события Windows	2858
Идентификатор события Kaspersky Security Center	00000b22
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат сервера реагирования EDR Expert

Статус	!
Компонент	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Идентификатор события Windows	2859
Идентификатор события Kaspersky Security Center	00000b23
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат агента на сервере реагирования EDR Expert

Статус	!
Компонент	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Идентификатор события Windows	2860
Идентификатор события Kaspersky Security Center	00000b24
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка подключения к серверу сбора телеметрии EDR Expert

Статус	!
Компонент	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Идентификатор события Windows	2854
Идентификатор события Kaspersky Security Center	00000b22
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат сервера сбора телеметрии EDR Expert

Статус	!
Компонент	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Идентификатор события Windows	2855
Идентификатор события Kaspersky Security Center	00000b23

Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат агента на сервере сбора телеметрии EDR Expert

Статус	ⓘ
Компонент	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Идентификатор события Windows	2856
Идентификатор события Kaspersky Security Center	00000b24
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка подключения к серверу NDR

Статус	ⓘ
Компонент	Network Detection and Response (KATA)
Идентификатор события Windows	3080
Идентификатор события Kaspersky Security Center	00000c08
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат сервера NDR

Статус	ⓘ
Компонент	Network Detection and Response (KATA)
Идентификатор события Windows	3081
Идентификатор события Kaspersky Security Center	00000c09
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат агента на сервере NDR

Статус	ⓘ
Компонент	Network Detection and Response (KATA)
Идентификатор события Windows	3082
Идентификатор события Kaspersky Security Center	00000c0a
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ваше устройство подключено к недоверенному Серверу администрирования. Обратитесь к администратору

Статус	ⓘ
Компонент	Защита подключения к Серверу администрирования
Идентификатор события Windows	3301

Идентификатор события Kaspersky Security Center	00000ce5
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружено изменение файла или папки

Статус	ⓘ / ⚠ / ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2950
Идентификатор события Kaspersky Security Center	00000b86
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Объект изменяется слишком часто. Запущено формирование агрегированных событий

Статус	ⓘ / ⚠ / ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2955
Идентификатор события Kaspersky Security Center	00000b8b
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Отчет об изменениях объекта за период агрегации

Статус	ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2953
Идентификатор события Kaspersky Security Center	00000b89
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Статус	ⓘ / ⚠ / ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2956
Идентификатор события Kaspersky Security Center	00000b8c
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Обнаружено изменение реестра

Статус	/ /
Компонент	Контроль целостности системы
Идентификатор события Windows	2951
Идентификатор события Kaspersky Security Center	00000b87
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки.*

Обнаружено подключение / отключение устройства

Статус	/ /
Компонент	Контроль целостности системы
Идентификатор события Windows	2952
Идентификатор события Kaspersky Security Center	00000b88
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки.*

Область мониторинга содержит некорректные объекты

Статус	/ /
Компонент	Контроль целостности системы
Идентификатор события Windows	2903
Идентификатор события Kaspersky Security Center	00000b89
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки.*

Попыток выполнения запрещенных действий с объектом слишком много. Запущено формирование агрегированных событий

Статус	
Компонент	Контроль целостности системы
Идентификатор события Windows	2963
Идентификатор события Kaspersky Security Center	00000b93

Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запрещено действие с файлами из области мониторинга

Статус	ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2959
Идентификатор события Kaspersky Security Center	00000b8f
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Изменение реестра заблокировано

Статус	ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2960
Идентификатор события Kaspersky Security Center	00000b90
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Ошибка обработки

Статус	ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2954
Идентификатор события Kaspersky Security Center	00000b8a
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Контроль целостности системы: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)

Статус	ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2964
Идентификатор события Kaspersky Security Center	00000b94
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Контроль приложений: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)

Статус	!
Компонент	Контроль приложений
Идентификатор события Windows	711
Идентификатор события Kaspersky Security Center	000002c7
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Контроль устройств: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)

Статус	!
Компонент	Контроль устройств
Идентификатор события Windows	810
Идентификатор события Kaspersky Security Center	0000032a
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Веб-Контроль: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)

Статус	!
Компонент	Веб-Контроль
Идентификатор события Windows	757
Идентификатор события Kaspersky Security Center	000002f5
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Адаптивный контроль аномалий: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)

Статус	!
Компонент	Адаптивный контроль аномалий
Идентификатор события Windows	504
Идентификатор события Kaspersky Security Center	000001f8
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Анализ журналов: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)

Статус	!
Компонент	Анализ журналов
Идентификатор события Windows	2810

Идентификатор события Kaspersky Security Center	00000afa
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

SVM недоступна

Статус	!
Компонент	Легкий агент
Идентификатор события Windows	3151
Идентификатор события Kaspersky Security Center	00000c4f
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружен вредоносный объект. Требуется запуск процедуры лечения активного заражения на шаблоне виртуальной машины

Статус	!
Компонент	Легкий агент
Идентификатор события Windows	3182
Идентификатор события Kaspersky Security Center	00000c6e
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Заблокировано сетевое соединение по устаревшему протоколу

Статус	!
Компонент	Защита
Идентификатор события Windows	75
Идентификатор события Kaspersky Security Center	0000004b
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка подключения к серверу KUMA

Статус	!
Компонент	Интеграция с KUMA
Идентификатор события Windows	2854
Идентификатор события Kaspersky Security Center	00000b26
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат сервера KUMA

Статус	!
Компонент	Интеграция с KUMA
Идентификатор события Windows	2855

Идентификатор события Kaspersky Security Center	00000b27
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат агента на сервере KUMA

Статус	!
Компонент	Интеграция с KUMA
Идентификатор события Windows	2856
Идентификатор события Kaspersky Security Center	00000b28
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка подключения к серверу SIEM

Статус	!
Компонент	Интеграция с KUMA
Идентификатор события Windows	3250
Идентификатор события Kaspersky Security Center	00000cb2
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат сервера SIEM

Статус	!
Компонент	Интеграция с KUMA
Идентификатор события Windows	3251
Идентификатор события Kaspersky Security Center	00000cb3
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный сертификат агента на сервере SIEM

Статус	!
Компонент	Интеграция с KUMA
Идентификатор события Windows	3252
Идентификатор события Kaspersky Security Center	00000cb4
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Отказ функционирования

Не удалось выполнить задачу

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	212
Идентификатор события Kaspersky Security Center	000000d4
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка в настройках задачи. Настройки задачи не применены

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	707
Идентификатор события Kaspersky Security Center	000002c3
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Защищенное соединение с удаленным сервером разорвано

Статус	ⓘ
Компонент	Удаленный доступ
Идентификатор события Windows	4302
Идентификатор события Kaspersky Security Center	000010cf
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Предупреждение

Обнаружено некорректное завершение предыдущей сессии работы приложения

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	237
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Срок действия лицензии скоро истекает

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	204
Идентификатор события Kaspersky Security Center	000000cc

Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Базы устарели

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	208
Идентификатор события Kaspersky Security Center	000000d0
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Автоматическое обновление выключено

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	210
Идентификатор события Kaspersky Security Center	000000d2
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Самозащита приложения выключена

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	211
Идентификатор события Kaspersky Security Center	000000d3
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Компоненты защиты выключены

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	214
Идентификатор события Kaspersky Security Center	000000d6
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Компьютер работает в безопасном режиме

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	215
Идентификатор события Kaspersky Security Center	000000d7

Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Есть необработанные файлы

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	216
Идентификатор события Kaspersky Security Center	000000d8
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Применена групповая политика

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	219
Идентификатор события Kaspersky Security Center	000000db
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Задача остановлена

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	222
Идентификатор события Kaspersky Security Center	000000de
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для завершения обновления необходимо перезапустить приложение

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	224
Идентификатор события Kaspersky Security Center	0000057b
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Необходима перезагрузка компьютера

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	225
Идентификатор события Kaspersky Security Center	000000e1

Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Установлены не все компоненты приложения, которые позволяет использовать лицензия

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	226
Идентификатор события Kaspersky Security Center	000000e2
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запущена процедура лечения активного заражения

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	232
Идентификатор события Kaspersky Security Center	000000e8
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Процедура лечения активного заражения завершена

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	233
Идентификатор события Kaspersky Security Center	000000e9
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Некорректный резервный ключ

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	230
Идентификатор события Kaspersky Security Center	000000e6
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Подписка скоро истекает

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	240
Идентификатор события Kaspersky Security Center	000000f0

Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запрещено

Статус	⚠
Компонент	Анализ поведения Защита от шифрования Защита от эксплойтов Защита от веб-угроз
Идентификатор события Windows	`331`
Идентификатор события Kaspersky Security Center	`GNRL_EV_OBJECT_BLOCKED`
Параметры события	• `GNRL_EA_PARAM_1` – хеш объекта (SHA256). • `GNRL_EA_PARAM_2` – название объекта. При обнаружении внешнего шифрования папок общего доступа приложение показывает путь к целевому файлу. • `GNRL_EA_PARAM_5` – название угрозы по классификации "Лаборатории Касперского", например, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` – имя сессионного пользователя. • `GNRL_EA_PARAM_8` – тип угрозы (`type`). • `GNRL_EA_PARAM_9` – дополнительная информация об обнаружении объекта: Компонент приложения (`engine`). Технология обнаружения угроз (`method`). Угроза обнаружена с помощью Kaspersky Private Security Network (`blacklist`): `true` или `false`. Версия EDR. Идентификатор угрозы в EDR. Хеш объекта MD5.
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Настройки операционной системы не позволяют контролировать доступ к сетям Wi-Fi

Статус	⚠
Компонент	Контроль устройств
Идентификатор события Windows	`249`
Идентификатор события Kaspersky Security Center	`000000f9`
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Объект не восстановлен из резервного хранилища

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	`336`
Идентификатор события Kaspersky Security Center	`00000150`
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Обнаружена подозрительная сетевая активность

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	2001
Идентификатор события Kaspersky Security Center	000007d1
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Защищенное соединение разорвано

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	250
Идентификатор события Kaspersky Security Center	000007d3
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Участие в KSN выключено

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	2021
Идентификатор события Kaspersky Security Center	000007e5
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обработка приложением некоторых функций ОС выключена

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	245
Идентификатор события Kaspersky Security Center	000000f5
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

В хранилище карантина скоро закончится место

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	344
Идентификатор события Kaspersky Security Center	00000158
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сетевое соединение заблокировано

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	809
Идентификатор события Kaspersky Security Center	00000abe
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Невозможно создать резервную копию объекта

Статус	⚠
Компонент	Защита от файловых угроз Анализ поведения Защита от шифрования Предотвращение вторжений Поиск вредоносного ПО
Идентификатор события Windows	310
Идентификатор события Kaspersky Security Center	00000136
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект не обработан

Статус	⚠
Компонент	Защита от файловых угроз Защита от почтовых угроз Предотвращение вторжений AMSI-защита Поиск вредоносного ПО
Идентификатор события Windows	314
Идентификатор события Kaspersky Security Center	0000013a
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект зашифрован

Статус	⚠
Компонент	Предотвращение вторжений
Идентификатор события Windows	320
Идентификатор события Kaspersky Security Center	00000140
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Объект поврежден

Статус	⚠
Компонент	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз AMSI-защита Предотвращение вторжений Поиск вредоносного ПО

Идентификатор события Windows	321
Идентификатор события Kaspersky Security Center	00000141
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Обнаружено легальное приложение, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или данным пользователя (локальные базы)

Статус	⚠
Компонент	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз Предотвращение вторжений AMSI-защита Анализ поведения Защита от шифрования Защита от шифрования Поиск вредоносного ПО
Идентификатор события Windows	303
Идентификатор события Kaspersky Security Center	GNRL_EV_VIRUS_FOUND
Параметры события	• GNRL_EA_PARAM_1 – хеш объекта (SHA256). • GNRL_EA_PARAM_2 – название объекта. • GNRL_EA_PARAM_5 – название угрозы по классификации "Лаборатории Касперского", например, EICAR-Test-File. • GNRL_EA_PARAM_7 – имя сессионного пользователя. • GNRL_EA_PARAM_8 – тип угрозы (type).
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружено легальное приложение, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или данным пользователя (KSN)

Статус	⚠
Компонент	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз Предотвращение вторжений AMSI-защита Анализ поведения Защита от шифрования Защита от шифрования Поиск вредоносного ПО
Идентификатор события Windows	303
Идентификатор события Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_BY_KSN
Параметры события	• GNRL_EA_PARAM_1 – хеш объекта (SHA256). • GNRL_EA_PARAM_2 – название объекта. • GNRL_EA_PARAM_5 – название угрозы по классификации "Лаборатории Касперского", например, EICAR-Test-File. • GNRL_EA_PARAM_7 – имя сессионного пользователя. • GNRL_EA_PARAM_8 – тип угрозы (type).
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект удален

Статус	⚠
Компонент	Защита от файловых угроз Защита от почтовых угроз Предотвращение вторжений Защита от эксплойтов Анализ поведения Защита от шифрования Поиск вредоносного ПО
Идентификатор события Windows	`307`
Идентификатор события Kaspersky Security Center	`GNRL_EV_OBJECT_DELETED`
Параметры события	• `GNRL_EA_PARAM_1` – хеш объекта (SHA256). • `GNRL_EA_PARAM_2` – название объекта. • `GNRL_EA_PARAM_5` – название угрозы по классификации "Лаборатории Касперского", например, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` – имя сессионного пользователя. • `GNRL_EA_PARAM_8` – тип угрозы (`type`). • `GNRL_EA_PARAM_9` – дополнительная информация об обнаружении объекта: Компонент приложения (`engine`). Технология обнаружения угроз (`method`). Угроза обнаружена с помощью Kaspersky Private Security Network (`blacklist`): `true` или `false`. Версия EDR. Идентификатор угрозы в EDR. Хеш объекта MD5.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект вылечен

Статус	⚠
Компонент	Защита от файловых угроз Защита от почтовых угроз Предотвращение вторжений Поиск вредоносного ПО
Идентификатор события Windows	`306`
Идентификатор события Kaspersky Security Center	`GNRL_EV_OBJECT_CURED`
Параметры события	• `GNRL_EA_PARAM_1` – хеш объекта (SHA256). • `GNRL_EA_PARAM_2` – название объекта. • `GNRL_EA_PARAM_5` – название угрозы по классификации "Лаборатории Касперского", например, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` – имя сессионного пользователя. • `GNRL_EA_PARAM_8` – тип угрозы (`type`). • `GNRL_EA_PARAM_9` – дополнительная информация об обнаружении объекта: Компонент приложения (`engine`). Технология обнаружения угроз (`method`). Угроза обнаружена с помощью Kaspersky Private Security Network (`blacklist`): `true` или `false`. Версия EDR. Идентификатор угрозы в EDR. Хеш объекта MD5.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект будет вылечен при перезагрузке

Статус	⚠
Компонент	Предотвращение вторжений Защита от файловых угроз Поиск вредоносного ПО
Идентификатор события Windows	324
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Объект будет удален при перезагрузке

Статус	⚠
Компонент	Анализ поведения Защита от шифрования Защита от эксплойтов Предотвращение вторжений Защита от файловых угроз Поиск вредоносного ПО
Идентификатор события Windows	323
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Объект удален в соответствии с настройками

Статус	⚠
Компонент	Защита от почтовых угроз
Идентификатор события Windows	342
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Откат выполнен

Статус	⚠
Компонент	Защита от файловых угроз Анализ поведения Защита от шифрования Защита от эксплойтов Поиск вредоносного ПО
Идентификатор события Windows	455
Идентификатор события Kaspersky Security Center	000001c7
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка при удалении предыдущей версии приложения

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	246
Идентификатор события Kaspersky Security Center	000000f6
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Загрузка объекта запрещена

Статус	⚠
Компонент	Защита от веб-угроз
Идентификатор события Windows	341
Идентификатор события Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
Параметры события	• GNRL_EA_PARAM_1 – хеш объекта (SHA256). • GNRL_EA_PARAM_2 – название объекта. • GNRL_EA_PARAM_5 – название угрозы по классификации "Лаборатории Касперского", например, EICAR-Test-File. • GNRL_EA_PARAM_7 – имя сессионного пользователя. • GNRL_EA_PARAM_8 – тип угрозы (type). • GNRL_EA_PARAM_9 – дополнительная информация об обнаружении объекта: Компонент приложения (engine). Технология обнаружения угроз (method). Угроза обнаружена с помощью Kaspersky Private Security Network (blacklist): true или false. Версия EDR. Идентификатор угрозы в EDR. Хеш объекта MD5.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ошибка авторизации клавиатуры

Статус	⚠
Компонент	Защита от атак BadUSB
Идентификатор события Windows	2052
Идентификатор события Kaspersky Security Center	00000804
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Результат проверки объекта передан стороннему приложению

Статус	⚠
Компонент	AMSI-защита
Идентификатор события Windows	1512

Идентификатор события Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
Параметры события	• GNRL_EA_PARAM_1 – хеш объекта (SHA256). • GNRL_EA_PARAM_2 – название объекта. • GNRL_EA_PARAM_5 – название угрозы по классификации "Лаборатории Касперского", например, EICAR-Test-File. • GNRL_EA_PARAM_7 – имя сессионного пользователя. • GNRL_EA_PARAM_8 – тип угрозы (type). • GNRL_EA_PARAM_9 – дополнительная информация об обнаружении объекта: Компонент приложения (engine). Технология обнаружения угроз (method). Угроза обнаружена с помощью Kaspersky Private Security Network (blacklist): true или false. Версия EDR. Идентификатор угрозы в EDR. Хеш объекта MD5.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Настройки задачи успешно применены

Статус	⚠
Компонент	Контроль приложений
Идентификатор события Windows	708
Идентификатор события Kaspersky Security Center	000002c4
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Предупреждение о нежелательном содержимом (локальные базы)

Статус	⚠
Компонент	Веб-Контроль
Идентификатор события Windows	708
Идентификатор события Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Параметры события	• GNRL_EA_PARAM_1 – URL-адрес. • GNRL_EA_PARAM_2 – имя сессионного пользователя. • GNRL_EA_PARAM_3 – название правила Веб-Контроля.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Предупреждение о нежелательном содержимом (KSN)

Статус	⚠
Компонент	Веб-Контроль
Идентификатор события Windows	708
Идентификатор события Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Параметры события	• GNRL_EA_PARAM_1 – URL-адрес. • GNRL_EA_PARAM_2 – имя сессионного пользователя. • GNRL_EA_PARAM_3 – название правила Веб-Контроля.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Осуществлен доступ к нежелательному содержимому после предупреждения

Статус	⚠
Компонент	Веб-Контроль
Идентификатор события Windows	754
Идентификатор события Kaspersky Security Center	000002f2
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Активирован временный доступ к устройству

Статус	⚠
Компонент	Контроль устройств
Идентификатор события Windows	803
Идентификатор события Kaspersky Security Center	000002f2
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Операция отменена пользователем

Статус	⚠
Компонент	Обновление
Идентификатор события Windows	1016
Идентификатор события Kaspersky Security Center	000003f8
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Пользователь отказался от политики шифрования

Статус	⚠
Компонент	Шифрование данных
Идентификатор события Windows	1306
Идентификатор события Kaspersky Security Center	0000051a
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Прервано применение правил шифрования / расшифровки файлов

Статус	⚠
Компонент	Шифрование данных
Идентификатор события Windows	903
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Операция шифрования / расшифровки файла прервана

Статус	⚠
Компонент	Шифрование данных
Идентификатор события Windows	914
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Приостановка шифрования / расшифровки устройства

Статус	⚠
Компонент	Шифрование данных
Идентификатор события Windows	1303
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Не удалось установить или обновить драйверы для компонента Шифрование диска Kaspersky в образе среды восстановления Windows

Статус	⚠
Компонент	Шифрование данных
Идентификатор события Windows	1345
Идентификатор события Kaspersky Security Center	00000541
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Неуспешная проверка подписи модуля

Статус	⚠
Компонент	Проверка целостности системы
Идентификатор события Windows	2002
Идентификатор события Kaspersky Security Center	000007d2
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запуск приложения был заблокирован

Статус	⚠
Компонент	Endpoint Sensor
Идентификатор события Windows	2105
Идентификатор события Kaspersky Security Center	00000839
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Открытие документа было заблокировано

Статус	⚠
Компонент	Endpoint Sensor
Идентификатор события Windows	2106
Идентификатор события Kaspersky Security Center	0000083a
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Процесс завершен администратором сервера Kaspersky Anti Targeted Attack Platform

Статус	⚠
Компонент	Endpoint Sensor
Идентификатор события Windows	2112
Идентификатор события Kaspersky Security Center	00000840
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Работа приложения завершена администратором сервера Kaspersky Anti Targeted Attack Platform

Статус	⚠
Компонент	Endpoint Sensor
Идентификатор события Windows	2113
Идентификатор события Kaspersky Security Center	00000841
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Файл или стрим удален администратором сервера Kaspersky Anti Targeted Attack Platform

Статус	⚠
Компонент	Endpoint Sensor
Идентификатор события Windows	2111
Идентификатор события Kaspersky Security Center	0000083f
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Файл восстановлен из карантина сервера Kaspersky Anti Targeted Attack Platform администратором

Статус	⚠
Компонент	Endpoint Sensor
Идентификатор события Windows	2110
Идентификатор события Kaspersky Security Center	0000083e
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Файл помещен на карантин сервера Kaspersky Anti Targeted Attack Platform администратором

Статус	⚠
Компонент	Endpoint Sensor
Идентификатор события Windows	2109
Идентификатор события Kaspersky Security Center	0000083d
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сетевая активность приложений сторонних производителей заблокирована

Статус	⚠
Компонент	Endpoint Sensor
Идентификатор события Windows	2107
Идентификатор события Kaspersky Security Center	0000083b
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сетевая активность приложений сторонних производителей разблокирована

Статус	⚠
Компонент	Endpoint Sensor
Идентификатор события Windows	2108
Идентификатор события Kaspersky Security Center	0000083c
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект будет удален после перезагрузки (Sandbox)

Статус	⚠
Компонент	Sandbox
Идентификатор события Windows	2605
Идентификатор события Kaspersky Security Center	00000a2d
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Суммарный размер задач проверки превысил максимальное значение

Статус	⚠
Компонент	Sandbox
Идентификатор события Windows	2612
Идентификатор события Kaspersky Security Center	00000a34
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запуск объекта разрешен, событие записано в отчет

Статус	⚠
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2553
Идентификатор события Kaspersky Security Center	000009fa
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запуск процесса разрешен, событие записано в отчет

Статус	⚠
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2554
Идентификатор события Kaspersky Security Center	000009f8
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект будет удален после перезагрузки (Endpoint Detection and Response)

Статус	⚠
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2558
Идентификатор события Kaspersky Security Center	000009fe
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сетевая изоляция

Статус	⚠
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2700
Идентификатор события Kaspersky Security Center	00000a8c
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Завершение сетевой изоляции

Статус	⚠
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2701
Идентификатор события Kaspersky Security Center	00000a8d
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для завершения задачи требуется перезагрузка

Статус	⚠
Компонент	Системный аудит
Идентификатор события Windows	225
Идентификатор события Kaspersky Security Center	0000057b
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Установлено соединение с сайтом с недоверенным сертификатом по решению пользователя

Статус	⚠
Компонент	Network Detection and Response (KATA)
Идентификатор события Windows	70
Идентификатор события Kaspersky Security Center	00000046
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Сообщение администратору о запрете запуска приложения

Статус	⚠
Компонент	Контроль приложений
Идентификатор события Windows	503
Идентификатор события Kaspersky Security Center	GNRL_EV_AC_USER_REQUEST
Параметры события	• GNRL_EA_DESCRIPTION – сообщение пользователя. • GNRL_EA_PARAM_2 – имя сессионного пользователя. • GNRL_EA_PARAM_6 – имя исполняемого файла приложения (например, chrome.exe). • GNRL_EA_PARAM_7 – путь к исполняемому файлу. • GNRL_EA_PARAM_8 – хеш объекта (SHA256). • GNRL_EA_PARAM_9 – версия приложения, которую пользователь пытается запустить.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сообщение администратору о запрете доступа к устройству

Статус	⚠
Компонент	Контроль устройств
Идентификатор события Windows	804
Идентификатор события Kaspersky Security Center	GNRL_EV_DC_USER_REQUEST
Параметры события	• c_er_descr – сообщение пользователя. • GNRL_EA_PARAM_1 – идентификатор устройства (англ. Hardware ID, HWID). • GNRL_EA_PARAM_2 – имя сессионного пользователя.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сообщение администратору о запрете доступа к веб-странице

Статус	⚠
Компонент	Веб-Контроль
Идентификатор события Windows	755
Идентификатор события Kaspersky Security Center	GNRL_EV_WC_USER_REQUEST
Параметры события	• GNRL_EA_DESCRIPTION – сообщение пользователя. • GNRL_EA_PARAM_1 – URL-адрес. • GNRL_EA_PARAM_2 – имя сессионного пользователя.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Подключение устройства заблокировано

Статус	⚠
Компонент	Контроль устройств
Идентификатор события Windows	807
Идентификатор события Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Параметры события	• GNRL_EA_PARAM_1 – идентификатор устройства (англ. Hardware ID, HWID). • GNRL_EA_PARAM_2 – имя сессионного пользователя.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сообщение администратору о запрете действия приложения

Статус	⚠
Компонент	Адаптивный контроль аномалий
Идентификатор события Windows	503
Идентификатор события Kaspersky Security Center	GNRL_EV_ADSEC_USER_REQUEST
Параметры события	• GNRL_EA_DESCRIPTION – сообщение пользователя. • GNRL_EA_PARAM_1 – название правила Адаптивного контроля аномалий. • GNRL_EA_PARAM_2 – идентификатор эвристического правила. • GNRL_EA_PARAM_3 – имя сессионного пользователя. • GNRL_EA_PARAM_4 – исходный процесс. • GNRL_EA_PARAM_5 – исходный объект. • GNRL_EA_PARAM_6 – целевой процесс. • GNRL_EA_PARAM_7 – целевой объект. • GNRL_EA_PARAM_8 – дополнительная информация об обнаружении объекта: Хеш-суммы исходного процесса / объекта и целевого процесса / объекта. Блокирование процесса (verdict_type): true или false. Идентификатор безопасности пользователя (SID).
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запуск клиентского приложения облачной службы запрещен

Статус	⚠
Компонент	Cloud Discovery
Идентификатор события Windows	2212

Идентификатор события Kaspersky Security Center	000008a4
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Доступ к облачной службе запрещен

Статус	⚠
Компонент	Cloud Discovery
Идентификатор события Windows	2213
Идентификатор события Kaspersky Security Center	000008a5
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружено изменение файла или папки

Статус	ⓘ / ⚠ / !
Компонент	Контроль целостности системы
Идентификатор события Windows	2950
Идентификатор события Kaspersky Security Center	00000b86
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки.*

Объект изменяется слишком часто. Запущено формирование агрегированных событий

Статус	ⓘ / ⚠ / !
Компонент	Контроль целостности системы
Идентификатор события Windows	2955
Идентификатор события Kaspersky Security Center	00000b8b
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Отчет об изменениях объекта за период агрегации

Статус	ⓘ / ⚠ / !
Компонент	Контроль целостности системы
Идентификатор события Windows	2956
Идентификатор события Kaspersky Security Center	00000b8c
Журнал событий Windows (по умолчанию)	–

Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Обнаружено изменение реестра

Статус	ⓘ / ⚠ / !
Компонент	Контроль целостности системы
Идентификатор события Windows	2951
Идентификатор события Kaspersky Security Center	00000b87
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Обнаружено подключение / отключение устройства

Статус	ⓘ / ⚠ / !
Компонент	Контроль целостности системы
Идентификатор события Windows	2952
Идентификатор события Kaspersky Security Center	00000b88
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Область мониторинга содержит некорректные объекты

Статус	ⓘ / ⚠ / !
Компонент	Контроль целостности системы
Идентификатор события Windows	2903
Идентификатор события Kaspersky Security Center	00000b89
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Запрещенное действие разрешено в тестовом режиме

Статус	⚠
Компонент	Контроль целостности системы
Идентификатор события Windows	2961
Идентификатор события Kaspersky Security Center	00000b91
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Не удается подключиться к Серверу интеграции более 30 минут. Проверьте состояние Сервера интеграции и настройки сети

Статус	⚠
Компонент	Легкий агент
Идентификатор события Windows	3102
Идентификатор события Kaspersky Security Center	00000c1e
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Не удается подключиться к Серверу интеграции более 6 часов. Проверьте состояние Сервера интеграции и настройки сети

Статус	⚠
Компонент	Легкий агент
Идентификатор события Windows	3103
Идентификатор события Kaspersky Security Center	00000c1f
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Не удается подключиться к Серверу интеграции. Проверьте состояние Сервера интеграции и настройки сети

Статус	⚠
Компонент	Легкий агент
Идентификатор события Windows	3101
Идентификатор события Kaspersky Security Center	00000c1d
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Требуется обновить шаблон виртуальных машин

Статус	⚠
Компонент	Легкий агент
Идентификатор события Windows	3181
Идентификатор события Kaspersky Security Center	00000c6d
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Действие лицензии Standard прекращено. Приложение используется по лицензии Enterprise

Статус	⚠
Компонент	Легкий агент
Идентификатор события Windows	3171
Идентификатор события Kaspersky Security Center	00000c64
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Не удалось установить защищенное соединение с удаленным сервером

Статус	⚠
Компонент	Удаленный доступ
Идентификатор события Windows	4303
Идентификатор события Kaspersky Security Center	000010d0
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Статус	⚠
Компонент	Мониторинг файловых операций
Идентификатор события Windows	2901
Идентификатор события Kaspersky Security Center	00000b55
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Статус	⚠
Компонент	Мониторинг файловых операций
Идентификатор события Windows	2900
Идентификатор события Kaspersky Security Center	00000b54
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Информационное сообщение

Приложение запущено

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	235
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Приложение остановлено

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	236
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Самозащита ограничила доступ к защищаемому ресурсу

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	213
Идентификатор события Kaspersky Security Center	000000d5
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Отчет очищен

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	217
Идентификатор события Kaspersky Security Center	000000d9
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Групповая политика деактивирована

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	220
Идентификатор события Kaspersky Security Center	000000dc
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Изменены настройки приложения

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	218
Идентификатор события Kaspersky Security Center	000000da
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Задача запущена

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	221
Идентификатор события Kaspersky Security Center	000000dd
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Задача завершена

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	223
Идентификатор события Kaspersky Security Center	000000df
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Все компоненты приложения, которые позволяет использовать лицензия, установлены и работают в нормальном режиме

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	227
Идентификатор события Kaspersky Security Center	000000e3
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Параметры подписки были изменены

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	238
Идентификатор события Kaspersky Security Center	000000ee
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Подписка была продлена

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	239
Идентификатор события Kaspersky Security Center	000000ef
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект восстановлен из резервного хранилища

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	335
Идентификатор события Kaspersky Security Center	0000014f
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ввод имени пользователя и пароля

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	2000
Идентификатор события Kaspersky Security Center	000007d0
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Участие в KSN включено

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	2020
Идентификатор события Kaspersky Security Center	000007e4
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Серверы KSN доступны

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	2022
Идентификатор события Kaspersky Security Center	000007e6
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Приложение работает и обрабатывает данные в соответствии с местным законодательством и использует локальную инфраструктуру

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	2024
Идентификатор события Kaspersky Security Center	000007e8
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект восстановлен из карантина

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	345
Идентификатор события Kaspersky Security Center	00000159
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект удален из карантина

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	347
Идентификатор события Kaspersky Security Center	0000015b
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Создана резервная копия объекта

Статус	ⓘ
Компонент	Защита от файловых угроз Защита от почтовых угроз Анализ поведения Защита от шифрования Предотвращение вторжений Sandbox Поиск вредоносного ПО
Идентификатор события Windows	308
Идентификатор события Kaspersky Security Center	00000134
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект перезаписан вылеченной ранее копией

Статус	ⓘ
Компонент	Защита от файловых угроз Предотвращение вторжений Поиск вредоносного ПО
Идентификатор события Windows	327
Идентификатор события Kaspersky Security Center	00000147
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Обнаружен защищенный паролем архив

Статус	ⓘ
Компонент	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз AMSI-защита Предотвращение вторжений Поиск вредоносного ПО

Идентификатор события Windows	322
Идентификатор события Kaspersky Security Center	GNRL_EV_PASSWD_ARCHIVE_FOUND
Параметры события	• GNRL_EA_PARAM_2 – имя объекта. • GNRL_EA_PARAM_3 – дата создания объекта (необязательный). • GNRL_EA_PARAM_7 – имя сессионного пользователя. • GNRL_EA_PARAM_9 – дополнительная информация об обнаружении объекта: Компонент приложения (engine). Технология обнаружения угроз (method). Угроза обнаружена с помощью Локального KSN (blacklist): true или false.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Информация об обнаруженном объекте

Статус	ⓘ
Компонент	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз AMSI-защита Предотвращение вторжений Поиск вредоносного ПО
Идентификатор события Windows	332
Идентификатор события Kaspersky Security Center	0000014c
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект находится в списке разрешенных в Kaspersky Private Security Network

Статус	ⓘ
Компонент	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз AMSI-защита Предотвращение вторжений Поиск вредоносного ПО
Идентификатор события Windows	340
Идентификатор события Kaspersky Security Center	00000154
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект переименован

Статус	ⓘ
Компонент	Защита от почтовых угроз Защита от эксплойтов Анализ поведения Защита от шифрования Поиск вредоносного ПО
Идентификатор события Windows	329
Идентификатор события Kaspersky Security Center	00000149
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект обработан

Статус	ⓘ
Компонент	Предотвращение вторжений Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз Поиск вредоносного ПО
Идентификатор события Windows	301
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Объект пропущен

Статус	ⓘ
Компонент	Предотвращение вторжений Защита от файловых угроз AMSI-защита Поиск вредоносного ПО
Идентификатор события Windows	315
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Обнаружен архив

Статус	ⓘ
Компонент	Предотвращение вторжений Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз AMSI-защита Поиск вредоносного ПО
Идентификатор события Windows	318
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Обнаружен упакованный объект

Статус	ⓘ
Компонент	Предотвращение вторжений Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз AMSI-защита Поиск вредоносного ПО
Идентификатор события Windows	319
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Ссылка обработана

Статус	ⓘ
Компонент	Защита от веб-угроз
Идентификатор события Windows	361
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Запуск приложения разрешен

Статус	ⓘ
Компонент	Контроль приложений
Идентификатор события Windows	701
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Выбран источник обновлений

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	1001
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Выбран прокси-сервер

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	1002
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Ссылка находится в списке разрешенных в Kaspersky Private Security Network

Статус	ⓘ
Компонент	Защита от веб-угроз
Идентификатор события Windows	370
Идентификатор события Kaspersky Security Center	00000172
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Приложение помещено в группу доверенных приложений

Статус	ⓘ
Компонент	Предотвращение вторжений
Идентификатор события Windows	401
Идентификатор события Kaspersky Security Center	00000191
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Приложение помещено в группу с ограничениями

Статус	ⓘ
Компонент	Предотвращение вторжений
Идентификатор события Windows	402
Идентификатор события Kaspersky Security Center	00000192
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сработал компонент Предотвращение вторжений

Статус	ⓘ
Компонент	Предотвращение вторжений
Идентификатор события Windows	403
Идентификатор события Kaspersky Security Center	00000193
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Файл восстановлен

Статус	ⓘ
Компонент	Анализ поведения Защита от шифрования Защита от эксплойтов Предотвращение вторжений
Идентификатор события Windows	457
Идентификатор события Kaspersky Security Center	000001c9
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Значение реестра восстановлено

Статус	ⓘ
Компонент	Анализ поведения Защита от эксплойтов
Идентификатор события Windows	458
Идентификатор события Kaspersky Security Center	000001ca
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Значение реестра удалено

Статус	ⓘ
Компонент	Анализ поведения Защита от эксплойтов
Идентификатор события Windows	459
Идентификатор события Kaspersky Security Center	000001cb
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Действие процесса пропущено

Статус	ⓘ
Компонент	Адаптивный контроль аномалий
Идентификатор события Windows	2201
Идентификатор события Kaspersky Security Center	GNRL_EV_ADSEC_DETECT
Параметры события	• GNRL_EA_PARAM_1 – название правила Адаптивного контроля аномалий. • GNRL_EA_PARAM_2 – идентификатор эвристического правила. • GNRL_EA_PARAM_3 – имя сессионного пользователя. • GNRL_EA_PARAM_4 – исходный процесс. • GNRL_EA_PARAM_5 – исходный объект. • GNRL_EA_PARAM_6 – целевой процесс. • GNRL_EA_PARAM_7 – целевой объект. • GNRL_EA_PARAM_8 – дополнительная информация об обнаружении объекта: Хеш-суммы исходного процесса / объекта и целевого процесса / объекта. Блокирование процесса (verdict_type): true или false. Идентификатор безопасности пользователя (SID).
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Клавиатура авторизована

Статус	ⓘ
Компонент	Защита от атак BadUSB
Идентификатор события Windows	2050
Идентификатор события Kaspersky Security Center	00000802
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сетевая активность разрешена

Статус	ⓘ
Компонент	Сетевой экран
Идентификатор события Windows	601
Идентификатор события Kaspersky Security Center	00000259
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Запуск приложения запрещен в тестовом режиме

Статус	
Компонент	Контроль приложений
Идентификатор события Windows	703
Идентификатор события Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Параметры события	• GNRL_EA_PARAM_2 – имя сессионного пользователя. • GNRL_EA_PARAM_3 – идентификатор категории, созданной вручную. • GNRL_EA_PARAM_4 – идентификатор безопасности учетной записи (англ. SID, Security Identifier). • GNRL_EA_PARAM_5 – информация о цифровой подписи приложения. • GNRL_EA_PARAM_6 – имя исполняемого файла приложения (например, chrome.exe). • GNRL_EA_PARAM_7 – путь к исполняемому файлу. • GNRL_EA_PARAM_8 – хеш объекта (SHA256). • GNRL_EA_PARAM_9 – версия приложения, которую пользователь пытается запустить.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запуск приложения разрешен в тестовом режиме

Статус	
Компонент	Контроль приложений
Идентификатор события Windows	704
Идентификатор события Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Параметры события	• GNRL_EA_PARAM_2 – имя сессионного пользователя. • GNRL_EA_PARAM_3 – идентификатор категории, созданной вручную. • GNRL_EA_PARAM_4 – идентификатор безопасности учетной записи (англ. SID, Security Identifier). • GNRL_EA_PARAM_5 – информация о цифровой подписи приложения.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Открыта разрешенная страница

Статус	
Компонент	Веб-Контроль
Идентификатор события Windows	751
Идентификатор события Kaspersky Security Center	000002f4
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Операция с устройством разрешена

Статус	
Компонент	Контроль устройств
Идентификатор события Windows	801
Идентификатор события Kaspersky Security Center	00000321

Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Выполнена операция с файлом

Статус	
Компонент	Контроль устройств
Идентификатор события Windows	`808`
Идентификатор события Kaspersky Security Center	`GNRL_EV_USB_FILE_OPERATION`
Параметры события	• `GNRL_EA_PARAM_1` – операция с файлом (запись или удаление). • `GNRL_EA_PARAM_2` – путь к файлу. • `GNRL_EA_PARAM_3` – название устройства. • `GNRL_EA_PARAM_4` – имя сессионного пользователя. • `GNRL_EA_PARAM_5` – идентификатор устройства (англ. Hardware ID, HWID).
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Нет доступных обновлений

Статус	
Компонент	Обновление
Идентификатор события Windows	`1020`
Идентификатор события Kaspersky Security Center	`000003fc`
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Копирование обновлений успешно завершено

Статус	
Компонент	Обновление
Идентификатор события Windows	`1022`
Идентификатор события Kaspersky Security Center	`000003fe`
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Загрузка файла

Статус	
Компонент	Обновление
Идентификатор события Windows	`1003`
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Файл загружен

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	1004
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Файл установлен

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	1005
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Файл обновлен

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	1006
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Выполнен откат файла из-за ошибки обновления

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	1007
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Обновление файлов

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	1008
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Копирование обновлений

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	1009
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Откат файлов

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	1010
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Формирование списка файлов для загрузки

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	1013
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Загрузка патчей

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	2150
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Установка патча

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	2151
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Патч установлен

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	2152
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Откат патча

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	2154
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Откат патча выполнен

Статус	ⓘ
Компонент	Обновление
Идентификатор события Windows	2155
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Началось применение правил шифрования / расшифровки файлов

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	901
Идентификатор события Kaspersky Security Center	00000385
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Завершено применение правил шифрования / расшифровки файлов

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	902
Идентификатор события Kaspersky Security Center	00000386
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Продолжено применение правил шифрования / расшифровки файлов

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	905
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Запущена операция шифрования / расшифровки файла

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	910
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Завершена операция шифрования / расшифровки файла

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	911
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Шифрование файла не выполнено, так как файл является исключением

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	913
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Активирован портативный режим

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	950
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Деактивирован портативный режим

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	952
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Запущена операция шифрования / расшифровки устройства

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1301
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Завершена операция шифрования / расшифровки устройства

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1302
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Возобновление шифрования / расшифровки устройства

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1304
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Устройство не зашифровано

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1307
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Процесс шифрования / расшифровки устройства переведен в активный режим

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1308
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Процесс шифрования / расшифровки устройства переведен в пассивный режим

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1309
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Загружен модуль шифрования

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1310
Идентификатор события Kaspersky Security Center	0000051e
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Создана новая учетная запись Агента аутентификации

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1330
Идентификатор события Kaspersky Security Center	00000532
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Удалена учетная запись Агента аутентификации

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1331
Идентификатор события Kaspersky Security Center	00000533
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Изменен пароль для учетной записи Агента аутентификации

Статус	
Компонент	Шифрование данных
Идентификатор события Windows	1332
Идентификатор события Kaspersky Security Center	00000534
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Успешная аутентификация в Агенте аутентификации

Статус	
Компонент	Шифрование данных
Идентификатор события Windows	1333
Идентификатор события Kaspersky Security Center	00000535
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Аутентификация в Агенте аутентификации завершилась с ошибкой

Статус	
Компонент	Шифрование данных
Идентификатор события Windows	1334
Идентификатор события Kaspersky Security Center	00000536
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Получен доступ к жесткому диску с помощью процедуры запроса доступа к зашифрованным устройствам

Статус	
Компонент	Шифрование данных
Идентификатор события Windows	1335
Идентификатор события Kaspersky Security Center	00000537
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Попытка получения доступа к жесткому диску с помощью процедуры запроса доступа к зашифрованным устройствам завершилась с ошибкой

Статус	
Компонент	Шифрование данных
Идентификатор события Windows	1336
Идентификатор события Kaspersky Security Center	00000538
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Учетная запись не добавлена. Такая учетная запись уже существует

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1337
Идентификатор события Kaspersky Security Center	00000539
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Учетная запись не изменена. Такая учетная запись не существует

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1338
Идентификатор события Kaspersky Security Center	0000053a
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Учетная запись не удалена. Такая учетная запись не существует

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1339
Идентификатор события Kaspersky Security Center	0000053b
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Обновление функциональности шифрования завершено успешно

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1341
Идентификатор события Kaspersky Security Center	0000053d
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Откат обновления функциональности шифрования завершен успешно

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1343
Идентификатор события Kaspersky Security Center	0000053f
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Не удалось удалить драйверы для компонента Шифрование диска Kaspersky из образа среды восстановления Windows

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1346
Идентификатор события Kaspersky Security Center	00000542
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ключ восстановления для BitLocker изменен

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1370
Идентификатор события Kaspersky Security Center	0000055a
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Пароль / PIN-код для BitLocker изменен

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1371
Идентификатор события Kaspersky Security Center	0000055b
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ключ восстановления BitLocker был сохранен на съемный диск

Статус	ⓘ
Компонент	Шифрование данных
Идентификатор события Windows	1372
Идентификатор события Kaspersky Security Center	0000055c
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Задачи с сервера Kaspersky Anti Targeted Attack Platform не обрабатываются

Статус	ⓘ
Компонент	Endpoint Sensor
Идентификатор события Windows	2103
Идентификатор события Kaspersky Security Center	00000837
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Компонент Endpoint Sensor подключен к серверу

Статус	ⓘ
Компонент	Endpoint Sensor
Идентификатор события Windows	2101
Идентификатор события Kaspersky Security Center	00000835
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Связь с сервером Kaspersky Anti Targeted Attack Platform восстановлена

Статус	ⓘ
Компонент	Endpoint Sensor
Идентификатор события Windows	2102
Идентификатор события Kaspersky Security Center	00000836
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Задачи с сервера Kaspersky Anti Targeted Attack Platform обрабатываются

Статус	ⓘ
Компонент	Endpoint Sensor
Идентификатор события Windows	2104
Идентификатор события Kaspersky Security Center	00000838
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект удален

Статус	ⓘ
Компонент	Удаление данных
Идентификатор события Windows	2251
Идентификатор события Kaspersky Security Center	000008cb
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	–

Статистика задачи удаления

Статус	ⓘ
Компонент	Endpoint Detection and Response Expert (on-premises)
Идентификатор события Windows	2853
Идентификатор события Kaspersky Security Center	00000b25
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Статус	ⓘ
Компонент	Удаление данных

Идентификатор события Windows	2253
Идентификатор события Kaspersky Security Center	000008cd
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект помещен на карантин (Sandbox)

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2602
Идентификатор события Kaspersky Security Center	00000a2a
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект удален (Sandbox)

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2604
Идентификатор события Kaspersky Security Center	00000a2c
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Запущен поиск IOC

Статус	ⓘ
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2652
Идентификатор события Kaspersky Security Center	00000a5c
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Завершен поиск IOC

Статус	ⓘ
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2653
Идентификатор события Kaspersky Security Center	00000a5d
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект помещен на карантин (Endpoint Detection and Response)

Статус	ⓘ
Компонент	Endpoint Detection and Response

Идентификатор события Windows	2555
Идентификатор события Kaspersky Security Center	000009fb
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект удален (Endpoint Detection and Response)

Статус	ⓘ
Компонент	Endpoint Detection and Response
Идентификатор события Windows	2557
Идентификатор события Kaspersky Security Center	000009fd
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Состав компонентов приложения успешно изменен

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	1402
Идентификатор события Kaspersky Security Center	0000057a
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2606
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2609
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2610
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2616
Идентификатор события Kaspersky Security Center	–
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	–

Сервер администрирования, к которому подключено ваше устройство, стал доверенным

Статус	ⓘ
Компонент	Защита подключения к Серверу администрирования
Идентификатор события Windows	3300
Идентификатор события Kaspersky Security Center	00000ce4
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Ваше устройство подключено к новому доверенному Серверу администрирования

Статус	ⓘ
Компонент	Защита подключения к Серверу администрирования
Идентификатор события Windows	3302
Идентификатор события Kaspersky Security Center	00000ce6
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сервер администрирования, к которому подключено ваше устройство, перестал быть доверенным

Статус	ⓘ
Компонент	Защита подключения к Серверу администрирования
Идентификатор события Windows	3303
Идентификатор события Kaspersky Security Center	00000ce7
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Асинхронное обнаружение Sandbox

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2619
Идентификатор события Kaspersky Security Center	GNRL_EV_APP_INCIDENT_OCCURED
Параметры события	• GNRL_EA_PARAM_1 – параметры компонента Sandbox. • GNRL_EA_PARAM_2 – путь к объекту. • GNRL_EA_PARAM_3 – идентификатор инцидента. • GNRL_EA_PARAM_4 – хеш объекта (SHA256).
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Задача проверки успешно отправлена в Sandbox пользователем

Статус	ⓘ
Компонент	Sandbox
Идентификатор события Windows	2622
Идентификатор события Kaspersky Security Center	00000a3e
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Устройство подключено

Статус	ⓘ
Компонент	Контроль устройств
Идентификатор события Windows	805
Идентификатор события Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUGGED
Параметры события	• GNRL_EA_PARAM_1 – идентификатор устройства (англ. Hardware ID, HWID). • GNRL_EA_PARAM_2 – имя сессионного пользователя.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Устройство отключено

Статус	ⓘ
Компонент	Контроль устройств
Идентификатор события Windows	806
Идентификатор события Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
Параметры события	• GNRL_EA_PARAM_1 – идентификатор устройства (англ. Hardware ID, HWID). • GNRL_EA_PARAM_2 – имя сессионного пользователя.
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Успешное подключение к серверу EDR Expert

Статус	ⓘ
Компонент	Endpoint Detection and Response Expert (on-premises)
Идентификатор события Windows	2853
Идентификатор события Kaspersky Security Center	00000b25
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Успешное подключение к серверу реагирования EDR Expert

Статус	ⓘ
Компонент	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Идентификатор события Windows	2853

Идентификатор события Kaspersky Security Center	00000b25
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Успешное подключение к серверу сбора телеметрии EDR Expert

Статус	ⓘ
Компонент	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Идентификатор события Windows	2857
Идентификатор события Kaspersky Security Center	00000b26
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Успешное подключение к серверу NDR

Статус	ⓘ
Компонент	Network Detection and Response (KATA)
Идентификатор события Windows	3083
Идентификатор события Kaspersky Security Center	00000c0b
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запуск клиентского приложения облачной службы разрешен

Статус	ⓘ
Компонент	Cloud Discovery
Идентификатор события Windows	2210
Идентификатор события Kaspersky Security Center	000008a2
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Доступ к облачной службе разрешен

Статус	ⓘ
Компонент	Cloud Discovery
Идентификатор события Windows	2211
Идентификатор события Kaspersky Security Center	000008a3
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Получен доступ к защищаемой области

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	2004

Идентификатор события Kaspersky Security Center	000007d4
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружено изменение файла или папки

Статус	ⓘ / ⚠ / ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2950
Идентификатор события Kaspersky Security Center	00000b86
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Объект изменяется слишком часто. Запущено формирование агрегированных событий

Статус	ⓘ / ⚠ / ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2955
Идентификатор события Kaspersky Security Center	00000b8b
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Отчет об изменениях объекта за период агрегации

Статус	ⓘ / ⚠ / ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2956
Идентификатор события Kaspersky Security Center	00000b8c
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Обнаружено изменение реестра

Статус	ⓘ / ⚠ / ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2951
Идентификатор события Kaspersky Security Center	00000b87
Журнал событий Windows (по умолчанию)	–

Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Обнаружено подключение / отключение устройства

Статус	ⓘ / ⚠ / !
Компонент	Контроль целостности системы
Идентификатор события Windows	2952
Идентификатор события Kaspersky Security Center	00000b88
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Область мониторинга содержит некорректные объекты

Статус	ⓘ / ⚠ / !
Компонент	Контроль целостности системы
Идентификатор события Windows	2903
Идентификатор события Kaspersky Security Center	00000b89
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Снимок состояния системы создан

Статус	ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2957
Идентификатор события Kaspersky Security Center	00000b8d
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Снимок состояния системы обновлен

Статус	ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2958
Идентификатор события Kaspersky Security Center	00000b8e

Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Действие выполнено доверенным пользователем

Статус	ⓘ
Компонент	Контроль целостности системы
Идентификатор события Windows	2962
Идентификатор события Kaspersky Security Center	00000b92
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Для настройки времени хранения этого события следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки*.

Соединение с SVM установлено

Статус	ⓘ
Компонент	Легкий агент
Идентификатор события Windows	3152
Идентификатор события Kaspersky Security Center	00000c50
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Создан новый временный пароль

Статус	ⓘ
Компонент	Системный аудит
Идентификатор события Windows	265
Идентификатор события Kaspersky Security Center	00000109
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Подключено к Серверу интеграции

Статус	ⓘ
Компонент	Легкий агент
Идентификатор события Windows	3105
Идентификатор события Kaspersky Security Center	00000c21
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Восстанавливаем подключение к Серверу интеграции

Статус	ⓘ
Компонент	Легкий агент
Идентификатор события Windows	3104
Идентификатор события Kaspersky Security Center	00000c20
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Успешное подключение к серверу KUMA

Статус	ⓘ
Компонент	Интеграция с KUMA
Идентификатор события Windows	2857
Идентификатор события Kaspersky Security Center	00000b29
Журнал событий Windows (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Установка защищенного соединения с удаленным сервером

Статус	ⓘ
Компонент	Удаленный доступ
Идентификатор события Windows	4304
Идентификатор события Kaspersky Security Center	000010cc
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Защищенное соединение с удаленным сервером установлено

Статус	ⓘ
Компонент	Удаленный доступ
Идентификатор события Windows	4300
Идентификатор события Kaspersky Security Center	000010ce
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Защищенное соединение с удаленным сервером закрыто

Статус	ⓘ
Компонент	Удаленный доступ
Идентификатор события Windows	4301
Идентификатор события Kaspersky Security Center	000010cd
Журнал событий Windows (по умолчанию)	✓
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Приложение 7. Поддерживаемые расширения файлов для Запрета запуска объектов

Kaspersky Endpoint Security поддерживает запрет открытия файлов офисного формата через определенные приложения. Информация о поддерживаемых расширениях имен файлов и приложений приведена в следующей таблице.

Поддерживаемые расширения файлов для Запрета запуска объектов

Имя приложения	Исполняемый файл	Расширение имени файла
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm

Имя приложения	Исполняемый файл	Расширение имени файла
Adobe Acrobat	acrord32.exe	pdf
Foxit PDF Reader	FoxitReader.exe	
STDU Viewer	STDUViewerApp.exe	
Microsoft Edge	MicrosoftEdge.exe	
Google Chrome	chrome.exe	
Mozilla Firefox	firefox.exe	
Яндекс.Браузер	browser.exe	
Tor Browser	tor.exe	

Приложение 8. Поддерживаемые интерпретаторы скриптов для Запрета запуска объектов

Запрет запуска объектов поддерживает следующие интерпретаторы скриптов:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe

- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Запрет запуска объектов поддерживает работу с Java-приложениями в среде выполнения Java (процессы java.exe и javaw.exe).

Приложение 9. Область поиска IOC в реестре (RegistryItem)

При добавлении типа данных **Реестр Windows - RegistryItem** в область поиска IOC, Kaspersky Endpoint Security по умолчанию анализирует следующие разделы реестра:

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders
```

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Приложение 10. Требования к IOC-файлам

При создании задач поиска IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- Приложение поддерживает IOC-файлы с расширением ioc и xml открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.
- После загрузки IOC-файлов вы можете вручную изменять содержание файлов во встроенном редакторе прямо в свойствах задачи. Kaspersky Endpoint Security поддерживает изменение содержания IOC-файлов, которые соответствуют стандарту OpenIOC версии 1.1. Изменить содержание IOC-файлов, соответствующих стандарту OpenIOC версии 1.0, невозможно.

- Если при создании задачи *Поиск IOC* из командной строки вы загрузите IOC-файлы, часть из которых не поддерживается, то при запуске задачи приложение будет использовать только поддерживаемые IOC-файлы. Если при создании задачи *Поиск IOC* из командной строки все загруженные вами IOC-файлы не поддерживаются, то задача может быть запущена, но в результате выполнения задачи не будут обнаружены индикаторы компрометации. Загрузить IOC-файлы, которые не поддерживаются, в Web Console или Cloud Console невозможно.

- Семантические ошибки и неподдерживаемые IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов приложение фиксирует отсутствие совпадения.

- Идентификаторы всех IOC-файлов, которые используются в одной задаче поиска IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.

- Размер одного IOC-файла не должен превышать 2 МБ. Использование файлов большего размера приводит к завершению задач поиска IOC с ошибкой. Суммарный размер всех добавляемых файлов в IOC-коллекции не должен превышать 10 МБ. Если размер всех файлов превышает 10 МБ, вам нужно разделить IOC-коллекцию и создать несколько задач *Поиск IOC*.

- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи *Поиск IOC*.

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC.

ЗАГРУЗИТЬ ФАЙЛ IOC_TERMS.XLSX

Особенности и ограничения поддержки стандарта OpenIOC приложением приведены в следующей таблице.

Особенности и ограничения поддержки стандарта OpenIOC версий 1.0 и 1.1.

Поддерживаемые условия	OpenIOC 1.0:
	
	`is`
	`isnot` (как исключение из множества)
	`contains`
	`containsnot` (как исключение из множества)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	Для терминов Email/* поддерживаются только условия `contains` и `is`. Для корректной работы ретроспективного поиска IOC при использовании условия `is` адрес электронной почты в IOC-файлах необходимо указывать в формате `"name@example.org" <SMTP:name@example.org>`. При работе задачи *Поиск IOC* в обычном режиме достаточно указать адрес электронной почты в формате `name@example.org`.

Поддерживаемые атрибуты условий	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Поддерживаемые операторы	`AND` `OR`

Поддерживаемые типы данных	`"date"`: дата (применимые условия: `is`, `greater-than`, `less-than`) `"int"`: целое число (применимые условия: `is`, `greater-than`, `less-than`) `"string"`: строка (применимые условия: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: продолжительность в секундах (применимые условия: `is`, `greater-than`, `less-than`)

Особенности интерпретации типов данных	Типы данных `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` интерпретируются как строка (string).
	
	Приложение поддерживает интерпретацию параметра `Content` для типов данных `int` и `date`, заданного в виде промежутков:
	
	OpenIOC 1.0:
	С использованием оператора `TO` в поле `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	С помощью условий `greater-than` и `less-than`
	С использованием оператора `TO` в поле `Content`
	Приложение поддерживает интерпретацию типов данных `date` и `duration`, если индикаторы заданы в формате `ISO 8601, Zulu time zone, UTC`.

Приложение 11. API для реагирования на угрозы EDR

В Kaspersky Endpoint Security для Windows 12.9 добавлена поддержка действий по реагированию на угрозы EDR (EDR responses) с помощью Kaspersky Security Center OpenAPI. То есть вы можете вызывать методы OpenAPI для автоматизации реагирования на угрозы EDR с помощью Python. Вы можете вызывать эти методы при взаимодействии с SIEM-решениями. SIEM-решение от "Лаборатории Касперского" – *Kaspersky Unified Monitoring and Analysis Platform* – поддерживает OpenAPI для реагирования на угрозы EDR начиная с версии 3.4.1. В справке KUMA приведены примеры скриптов.

Для выполнения действий по реагированию на угрозы EDR вам нужно создать запрос и отправить его с помощью KSC Open API (`AddIncident`). После обработки запроса в консоли Kaspersky Security Center будет создана специальная задача.

Для создания задач при реагировании на угрозы EDR вам нужно установить фоновое соединение между Сервером администрирования и Kaspersky Security Center Web Console. Служба фонового соединения доступна в Kaspersky Security Center Windows 14.2 и выше и Kaspersky Security Center Linux 15.2 и выше. Другие консоли, включая консоли решений Detection and Response от "Лаборатории Касперского", не поддерживаются.

Для реагирования на угрозы EDR необходимо задать основные параметры запроса, например, с помощью JSON:

- `task` – тип задачи (см. ниже).
- `targetHost` – идентификатор компьютера, на котором нужно запустить скрипт. Обязательный аргумент. Скрипт получает этот аргумент из события.
- `responseEventIncidentArea` – название приложения, которое инициировало запуск скрипта (например, `KUMA`). Этот параметр будет добавлен в название создаваемой задачи.

Для настройки параметров реагирования на угрозы EDR вам нужно в параметре `"KLINCDT_BODY": json.dumps(data)` задать параметры задачи в JSON. В результате в консоли Kaspersky Security Center приложение создает задачу `[Response][KUMA] <task type> - <Date> <Time> - <ID>`.

Подключение к Kaspersky Security Center OpenAPI

При реагировании на угрозы EDR приложение создает в консоли Kaspersky Security Center специальные задачи. Для создания этих задач нужно установить соединение между компьютером и Kaspersky Security Center. Для этого в запросе необходимо указать параметры подключения к Kaspersky Security Center.

В Kaspersky XDR версии 2.1 изменился способ авторизации запросов. Kaspersky XDR использует PAT-токены вместо авторизации по имени пользователя и паролю. Поэтому в Kaspersky XDR запустить скрипты невозможно. Подробнее об авторизации запросов см. в справке Kaspersky XDR.

Параметры подключения к Kaspersky Security Center

Параметр	Тип	Описание
`kscHost`	`string`	Адрес Сервера администрирования Kaspersky Security Center. Обязательный параметр.
`kscPort`	`int`	Порт подключения к Серверу администрирования. Обязательный параметр.
`kscCert`	`string`	Путь к файлу сертификата для подключения к Серверу администрирования Kaspersky Security Center. По умолчанию параметр имеет значение `False`.
`kscUser`	`string`	Имя учетной записи пользователя. Обязательный параметр.
`kscPassword`	`string`	Пароль учетной записи пользователя. Обязательный параметр.

Пример

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

Так как учетные данные пользователя не защищены, для работы со скриптами необходимо выделить отдельного пользователя, который выполняет только эти действия.

Получение файла – getFile

Параметры задачи Получение файла

Параметр	Тип	Описание
md5hash	string	MD5-хеш файла, который вам нужно получить.
sha256hash	string	SHA256-хеш файла, который вам нужно получить.
path	string	Путь к файлу, который вам нужно получить.

Пример

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Удаление файла – deleteFile

Параметры задачи Удаление файла

Параметр	Тип	Описание
md5hash	string	MD5-хеш файла, который вам нужно удалить.
sha256hash	string	SHA256-хеш файла, который вам нужно удалить.
path	string	Путь к файлу, который вам нужно удалить.
searchInSubfolders?	boolean	Поиск файла, который вам нужно удалить, в подпапках.

Пример

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

Помещение файла на карантин – quarantineFile

Параметры задачи Помещение файла на карантин

Параметр	Тип	Описание
`md5hash`	`string`	MD5-хеш файла, который вам нужно поместить на карантин.
`sha256hash`	`string`	SHA256-хеш файла, который вам нужно поместить на карантин.
`path`	`string`	Путь к файлу, который вам нужно поместить на карантин.

Пример

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Поиск IOC – iocScan

Параметры задачи Поиск IOC

Параметр	Тип	Описание
`ioc`	`string`	Путь к ZIP-архиву с IOC-файлом, по которому требуется выполнять поиск.
`isolateHost`	`boolean`	Изоляция компьютера от сети при обнаружении индикатора компрометации для предотвращения распространения угрозы.
`scanCriticalAreas`	`boolean`	Запуск задачи *Проверка важных областей* при обнаружении индикатора компрометации.
`quarantineObject`	`boolean`	Удаление вредоносного объекта при обнаружении индикатора компрометации. Перед удалением объекта Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин.

Пример

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

Запуск процесса – startProcess

Параметры задачи Запуск процесса

Параметр	Тип	Описание
executablePath	string	Путь к исполняемому файлу для запуска процесса.
arguments?	string	Дополнительные аргументы для запуска процесса.
workingFolder?	string	Путь к рабочей папке процесса.

Пример

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

Завершение процесса – terminateProcess

Параметры задачи Завершение процесса

Параметр	Тип	Описание
md5hash	string	MD5-хеш файла, процесс которого вам нужно завершить.
sha256hash	string	SHA256-хеш файла, процесс которого вам нужно завершить.
path	string	Путь к файлу, процесс которого вам нужно завершить.
caseSensitive	boolean	Режим учета регистра при поиске файла.

Пример

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Сетевая изоляция компьютера – isolateHost

Параметры Сетевой изоляции компьютера

Параметр	Тип	Описание
`action`	`string`	Режим работы Сетевой изоляции.

Пример

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Запрет запуска объектов – preventExecution

Параметры Запрета запуска объектов

Параметр	Тип	Описание
`hash`	`string`	MD5-хеш файла, запуск которого вы хотите запретить.
`path`	`string`	Путь к файлу, запуск которого вы хотите запретить.
`caseSensitive`	`boolean`	Режим учета регистра при поиске файла.

Пример

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Поиск вредоносного ПО – onDemandScan

Параметры задачи Поиск вредоносного ПО

Параметр	Тип	Описание
`path`	`string`	Список файлов и папок для выборочной проверки через пробел
`recursive`	`boolean`	Режим рекурсивной проверки.

Параметр	Тип	Описание
type	number	Область проверки.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Пример

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

Приложение 12. Учетные записи пользователей в правилах компонентов приложения

Для настройки работы некоторых компонентов приложения нужно добавить специальные правила. Например, для Веб-Контроля нужно добавить правило со списком веб-адресов, доступ к которым приложение будет блокировать. Также в правилах компонентов приложения вы можете настроить расписание работы компонента или выбрать пользователей, для которых приложение будет применять это правило.

Правила необходимо добавлять для настройки следующих компонентов приложения:

- Контроль приложений;
- Веб-Контроль;
- Контроль устройств;
- Анализ журналов;
- Адаптивный контроль аномалий;
- Контроль целостности системы.

В Kaspersky Endpoint Security для Windows 12.5 добавлена возможность выбирать пользователей не только из Active Directory, но и из списка пользователей в Kaspersky Security Center или вы можете ввести данные локальной учетной записи вручную. Таким образом, вы можете добавить пользователей следующими способами:

- Active Directory (рекомендуется).
- Список пользователей в Kaspersky Security Center.
- Локальная учетная запись.

Для корректного добавления пользователей из всех источников необходимо обновить плагин управления и приложение Kaspersky Endpoint Security до версии 12.5 или выше.

Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно. Подробнее о рисках безопасности локальных учетных записей см. в Базе знаний Microsoft. Вы сами несете ответственность за обеспечение безопасности компьютера при использовании локальных учетных записей, в частности, за контроль и ограничение доступа к параметрам Kaspersky Endpoint Security.

Для идентификации пользователей приложение использует SID пользователя (Security Identifier). При использовании учетных записей из Active Directory или списка пользователей в Kaspersky Security Center приложение определяет SID на Сервере администрирования. Таким образом, приложение не оказывает дополнительную нагрузку на компьютер для идентификации пользователя. Если вы добавили в правило приложения более 1000 локальных учетных записей, то для идентификации пользователя приложение обращается к контроллеру домена. Таким образом, возрастает нагрузка на компьютер. Для оптимизации нагрузки на компьютер рекомендуется использовать учетные записи из Active Directory или списка пользователей в Kaspersky Security Center.

Для идентификации учетных записей, добавленных вручную в формате `<username>` или `<hostname>\<username>`, приложение использует NetBIOS-имена. NetBIOS-имя имеет ограничение в 16 байт (15 символов). Если имя компьютера содержит более 15 символов, приложение не может идентифицировать пользователя. Далее приложение выключает правило и формирует ошибку, например, *Веб-Контроль: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)*. Для работы правила вам нужно вручную сократить длину имени компьютера. Вы можете добавлять учетные записи из Active Directory или Kaspersky Security Center. В этом случае приложение сокращает имя компьютера автоматически.

Kaspersky Endpoint Security также поддерживает в правилах встроенные учетные записи пользователей и групп (например, группа "Все"). Из-за особенностей определения SID пользователя приложение позволяет использовать встроенные учетные записи, добавленные только из Active Directory или списка пользователей в Kaspersky Security Center. Правила, в которых встроенная учетная запись добавлена локально, не работают.

Юридическая информация

Предоставление данных

Этот раздел содержит информацию о данных, которые приложение Kaspersky Endpoint Security может сохранять на устройстве и передавать в автоматическом режиме в "Лабораторию Касперского" в ходе своей работы.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Предоставление данных в рамках Лицензионного соглашения

Если для активации Kaspersky Endpoint Security применяется код активации, с целью проверки правомерности использования приложения вы соглашаетесь периодически передавать в автоматическом режиме в "Лабораторию Касперского" следующую информацию:

- тип, версию и локализацию Kaspersky Endpoint Security;
- версии установленных обновлений Kaspersky Endpoint Security;
- идентификатор компьютера и идентификатор установки Kaspersky Endpoint Security на компьютере;
- серийный номер и идентификатор активного ключа;
- тип, версию и разрядность операционной системы, название виртуальной среды, если приложение Kaspersky Endpoint Security установлено в виртуальной среде;
- уникальный идентификатор запроса к службам Правообладателя;
- идентификаторы компонентов Kaspersky Endpoint Security, активных на момент предоставления информации.

"Лаборатория Касперского" может также использовать эту информацию для формирования статистической информации о распространении и использовании программного обеспечения "Лаборатории Касперского".

Используя код активации, вы соглашаетесь на автоматическую передачу данных, перечисленных выше. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", для активации Kaspersky Endpoint Security следует использовать файл ключа.

Принимая условия Лицензионного соглашения, вы соглашаетесь передавать в автоматическом режиме следующую информацию:

- При обновлении Kaspersky Endpoint Security:
  - версию Kaspersky Endpoint Security;
  - идентификатор Kaspersky Endpoint Security;

- активный ключ;
- уникальный идентификатор запуска задачи обновления;
- уникальный идентификатор установки Kaspersky Endpoint Security.

- При переходе по ссылкам из интерфейса Kaspersky Endpoint Security:
  - версию Kaspersky Endpoint Security;
  - версию операционной системы;
  - дату активации Kaspersky Endpoint Security;
  - дату окончания действия лицензии;
  - дату создания ключа;
  - дату установки Kaspersky Endpoint Security;
  - идентификатор Kaspersky Endpoint Security;
  - идентификатор обнаруженной уязвимости операционной системы;
  - идентификатор последнего установленного обновления для Kaspersky Endpoint Security;
  - хеш обнаруженного файла, представляющего угрозу, и название этого объекта по классификации "Лаборатории Касперского";
  - категорию ошибки активации Kaspersky Endpoint Security;
  - код ошибки активации Kaspersky Endpoint Security;
  - количество дней до истечения срока годности ключа;
  - количество дней, прошедших с момента добавления ключа;
  - количество дней, прошедших с момента окончания срока действия лицензии;
  - количество компьютеров, на которые распространяется действующая лицензия;
  - активный ключ;
  - срок действия лицензии Kaspersky Endpoint Security;
  - текущий статус лицензии;
  - тип действующей лицензии;
  - тип приложения;
  - уникальный идентификатор запуска задачи обновления;

- уникальный идентификатор установки Kaspersky Endpoint Security на компьютере;
- язык интерфейса Kaspersky Endpoint Security.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Более подробную информацию о получении, обработке, хранении и уничтожении информации об использовании приложения после принятия Лицензионного соглашения и согласия с Положением о Kaspersky Security Network вы можете узнать, прочитав тексты этих документов, а также на веб-сайте "Лаборатории Касперского". Файлы license.txt и ksn_<ID языка>.txt с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки приложения.

Предоставление данных при использовании Kaspersky Security Network

Набор данных, которые Kaspersky Endpoint Security передает в "Лабораторию Касперского", зависят от типа лицензии и параметров использования Kaspersky Security Network.

Использование KSN по лицензии не более чем на 4 компьютера

Принимая Положение о Kaspersky Security Network, вы соглашаетесь передавать в автоматическом режиме следующую информацию:

- информацию об обновлении конфигурации KSN: идентификатор действующей конфигурации, идентификатор полученной конфигурации, код ошибки обновления конфигурации;
- информацию о проверяемых файлах и URL-адресах: контрольные суммы проверяемого файла (MD5, SHA2-256, SHA1) и паттернов файла (MD5), размер паттерна, тип обнаруженной угрозы и ее название согласно классификации Правообладателя, идентификатор антивирусных баз, URL-адрес, по которому запрашивается репутация, а также URL-адрес страницы, с которой осуществлен переход на проверяемый URL-адрес, идентификатор протокола соединения и номер используемого порта;
- идентификатор задачи проверки, в которой обнаружена угроза;
- информацию об используемых цифровых сертификатах, необходимую для проверки их подлинности: контрольные суммы (SHA256) сертификата, которым подписан проверяемый объект, и открытого ключа сертификата;
- идентификатор компонента ПО, выполняющего сканирование;
- идентификаторы антивирусных баз и записей в антивирусных базах;

- информацию об активации ПО на Компьютере: подписанный заголовок тикета от службы активации (идентификатор регионального центра активации, контрольную сумму кода активации, контрольную сумму тикета, дату создания тикета, уникальный идентификатор тикета, версию тикета, статус лицензии, дату и время начала / окончания действия тикета, уникальный идентификатор лицензии, версию лицензии), идентификатор сертификата, которым подписан заголовок тикета, контрольную сумму (MD5) файла ключа;

- информацию о ПО Правообладателя: полную версию, тип, версию используемого протокола соединения с сервисами "Лаборатории Касперского".

Использование KSN по лицензии на 5 компьютеров и более

Принимая Положение о Kaspersky Security Network, вы соглашаетесь передавать в автоматическом режиме следующую информацию:

Если флажок **Kaspersky Security Network** установлен, а флажок **Включить расширенный режим KSN** снят, приложение передает следующую информацию:

- информацию об обновлении конфигурации KSN: идентификатор действующей конфигурации, идентификатор полученной конфигурации, код ошибки обновления конфигурации;

- информацию о проверяемых файлах и URL-адресах: контрольные суммы проверяемого файла (MD5, SHA2-256, SHA1) и паттернов файла (MD5), размер паттерна, тип обнаруженной угрозы и ее название согласно классификации Правообладателя, идентификатор антивирусных баз, URL-адрес, по которому запрашивается репутация, а также URL-адрес страницы, с которой осуществлен переход на проверяемый URL-адрес, идентификатор протокола соединения и номер используемого порта;

- идентификатор задачи проверки, в которой обнаружена угроза;

- информацию об используемых цифровых сертификатах, необходимую для проверки их подлинности: контрольные суммы (SHA256) сертификата, которым подписан проверяемый объект, и открытого ключа сертификата;

- идентификатор компонента ПО, выполняющего сканирование;

- идентификаторы антивирусных баз и записей в антивирусных базах;

- информацию об активации ПО на Компьютере: подписанный заголовок тикета от службы активации (идентификатор регионального центра активации, контрольную сумму кода активации, контрольную сумму тикета, дату создания тикета, уникальный идентификатор тикета, версию тикета, статус лицензии, дату и время начала / окончания действия тикета, уникальный идентификатор лицензии, версию лицензии), идентификатор сертификата, которым подписан заголовок тикета, контрольную сумму (MD5) файла ключа;

- информацию о ПО Правообладателя: полную версию, тип, версию используемого протокола соединения с сервисами "Лаборатории Касперского".

Если в дополнение к флажку **Kaspersky Security Network** установлен флажок **Включить расширенный режим KSN**, приложение дополнительно к перечисленному выше передает следующую информацию:

- информацию о результатах категоризации запрашиваемых веб-ресурсов, которая содержит проверяемый URL-адрес и IP-адрес хоста, версию компонента ПО, выполнившего категоризацию, способ категоризации и набор категорий, определенных для веб-ресурса;

- информацию об установленном на Компьютере программном обеспечении: название программного обеспечения и его производителей, используемые ключи реестра и их значения, информацию о файлах компонентов установленного программного обеспечения (контрольные суммы (MD5, SHA2-256, SHA1), имя, путь к файлу на Компьютере, размер, версию и цифровую подпись);

- информацию о состоянии антивирусной защиты Компьютера: версии, даты и время выпуска используемых антивирусных баз, идентификатор задачи и идентификатор ПО, выполняющего сканирование;

- информацию о загружаемых Пользователем файлах: URL- и IP-адреса, откуда была выполнена загрузка, и URL-адрес страницы, с которой был выполнен переход на страницу загрузки файла, идентификатор протокола загрузки и номер порта соединения, признак вредоносности адресов, атрибуты и размер файла и его контрольные суммы (MD5, SHA2-256, SHA1), информацию о процессе, загрузившем файл (контрольные суммы (MD5, SHA2-256, SHA1), дата и время создания и линковки, признак нахождения в автозапуске, атрибуты, имена упаковщиков, информация о подписи, признак исполняемого файла, идентификатор формата, тип учетной записи, от имени которой был запущен процесс), информацию о файле процесса (имя, путь к файлу и размер), имя файла, путь к файлу на Компьютере, цифровая подпись файла и информация о выполнении подписи, URL-адрес, на котором произошло обнаружение, номер скрипта на странице, оказавшегося подозрительным или вредоносным;

- информацию о запускаемых приложениях и их модулях: данные о запущенных процессах в системе (идентификатор процесса в системе (PID), имя процесса, данные об учетной записи, от которой запущен процесс, приложению и команде, запустившей процесс, а также признак доверенности приложения или процесса, полный путь к файлам процесса и их контрольные суммы (MD5, SHA2-256, SHA1), командная строка запуска, уровень целостности процесса, описание продукта, к которому относится процесс (название продукта и данные об издателе), а также данные об используемых цифровых сертификатах и информацию, необходимую для проверки их подлинности, или данные об отсутствии цифровой подписи файла), также информацию о загружаемых в процессы модулях (имя, размер, тип, дата создания, атрибуты, контрольные суммы (MD5, SHA2-256, SHA1), путь), информация заголовка PE-файлов, названия упаковщика (если файл был упакован);

- информацию обо всех потенциально вредоносных объектах и действиях: название детектируемого объекта и полный путь к объекту на Компьютере, контрольные суммы обрабатываемых файлов (MD5, SHA2-256, SHA1), дата и время обнаружения, названия и размер обрабатываемых файлов и пути к ним, код шаблона пути, признак исполняемого файла, признак, является ли объект контейнером, названия упаковщика (если файл был упакован), код типа файла, идентификатор формата файла, идентификаторы антивирусных баз и записей в антивирусных базах, на основании которых было вынесено решение ПО, признак потенциально вредоносного объекта, название обнаруженной угрозы согласно классификации Правообладателя, степень опасности, статус и способ обнаружения, причина включения в анализируемый контекст и порядковый номер файла в контексте, контрольные суммы (MD5, SHA2-256, SHA1), имя и атрибуты исполняемого файла приложения, через которое прошло зараженное сообщение или ссылка, IP-адреса (IPv4 и IPv6) хоста заблокированного объекта, энтропия файла, признак нахождения файла в автозапуске, время первого обнаружения файла в системе, количество запусков файла с момента последней отправки статистик, тип компилятора, информация о названии, контрольных суммах (MD5, SHA2-256, SHA1) и размере почтового клиента, через который был получен вредоносный объект, идентификатор задачи ПО, которое выполнило проверку, признак проверки репутации или подписи файла, результаты статического анализа содержимого объекта, паттерны объекта, размер паттерна в байтах, технические характеристики по применяемым технологиям детектирования;

- информацию о проверенных объектах: присвоенную группу доверия, в которую помещен и/или из которой перемещен файл, причина, по которой файл помещен в данную категорию, идентификатор категории, информация об источнике категорий и версии базы категорий, признак наличия у файла доверенного сертификата, название производителя файла, версия файла, имя и версия приложения, частью которого является файл;

- информацию об обнаруженных уязвимостях: идентификатор уязвимости в базе уязвимостей, класс опасности уязвимости;

- информацию о выполнении эмуляции исполняемого файла: размер файла и его контрольные суммы (MD5, SHA2-256, SHA1), версия компонента эмуляции, глубина эмуляции, вектор характеристик логических блоков и функций внутри логических блоков, полученный в ходе эмуляции, данные из структуры PE-заголовка исполняемого файла;

- информацию о сетевых атаках: IP-адреса атакующего компьютера (IPv4 и IPv6), номер порта Компьютера, на который была направлена сетевая атака, идентификатор протокола IP-пакета, в котором зафиксирована атака, цель атаки (название организации, веб-сайт), флаг реакции на атаку, весовой уровень атаки, значение уровня доверия;

- информацию об атаках, связанных с подменой сетевых ресурсов, DNS- и IP-адреса (IPv4 или IPv6) посещаемых веб-сайтов;

- DNS- и IP-адреса (IPv4 или IPv6) запрашиваемого веб-ресурса, информацию о файле и веб-клиенте, обращающемся к веб-ресурсу: название, размер, контрольные суммы (MD5, SHA2-256, SHA1) файла, полный путь к нему и код шаблона пути, результат проверки его цифровой подписи и его статус в KSN;

- информацию о выполнении отката деятельности вредоносного приложения: данные о файле, активность которого откатывается (имя файла, полный путь к нему, его размер и контрольные суммы (MD5, SHA2-256, SHA1)), данные об успешных и неуспешных действиях по удалению, переименованию и копированию файлов и восстановлению значений в реестре (имена ключей реестра и их значения), информация о системных файлах, измененных вредоносным приложением, до и после выполнения отката;

- информацию об исключениях для правил компонента Адаптивный контроль аномалий: идентификатор и статус сработавшего правила, действие ПО при срабатывании правила, тип учетной записи, от имени которой процесс или поток выполняет подозрительные действия, информацию о процессе, выполнившем подозрительные действия, и о процессе, в отношении которого были выполнены подозрительные действия (идентификатор скрипта или имя файла процесса, полный путь к файлу процесса, код шаблона пути, контрольные суммы (MD5, SHA2-256, SHA1) файла процесса), информацию об объекте, от имени которого были выполнены подозрительные действия, и об объекте, в отношении которого были выполнены подозрительные действия (название ключа реестра или имя файла, полный путь к файлу, код шаблона пути и контрольные суммы (MD5, SHA2-256, SHA1) файла);

- информацию о загружаемых ПО модулях: название, размер и контрольные суммы (MD5, SHA2-256, SHA1) файла модуля, полный путь к нему и код шаблона пути, параметры цифровой подписи файла модуля, дата и время создания подписи, название субъекта и организации, подписавших файл модуля, идентификатор процесса, в который был загружен модуль, название поставщика модуля, порядковый номер модуля в очереди загрузки;

- информацию о качестве работы ПО с сервисами KSN: дату и время начала и окончания периода формирования статистики, информацию о качестве запросов и соединения с каждым из используемых сервисов KSN (идентификатор сервиса KSN, количество успешных запросов, количество запросов с ответами из кеша, количество неуспешных запросов (сетевые проблемы, выключен KSN в параметрах ПО, неправильная маршрутизация), распределение по времени успешных запросов, распределение по времени отмененных запросов, распределение по времени запросов, превысивших ограничение на время ожидания, количество подключений к KSN, взятых из кеша, количество успешных подключений к KSN, количество неуспешных подключений к KSN, количество успешных транзакций, количество неуспешных транзакций, распределение по времени успешных подключений к KSN, распределение по времени неуспешных подключений к KSN, распределение по времени успешных транзакций, распределение по времени неуспешных транзакций);

- в случае обнаружения потенциально вредоносного объекта предоставляется информация о данных в памяти процессов: элементы иерархии системных объектов (ObjectManager), данные памяти UEFI BIOS, названия ключей реестра и их значения;

- информацию о событиях в системных журналах: время события, название журнала, в котором обнаружено событие, тип и категория события, название источника события и его описание;

- информацию о сетевых соединениях: версия и контрольные суммы (MD5, SHA2-256, SHA1) файла процесса, открывшего порт, путь к файлу процесса и его цифровая подпись, локальный и удаленный IP-адреса, номера локального и удаленного портов соединения, состояние соединения, время открытия порта;

- информацию о дате установки и активации ПО на Компьютере: идентификатор партнера, у которого приобретена лицензия, серийный номер лицензии, подписанный заголовок тикета от службы активации (идентификатор регионального центра активации, контрольную сумму кода активации, контрольную сумму тикета, дату создания тикета, уникальный идентификатор тикета, версию тикета, статус лицензии, дату и время начала / окончания действия тикета, уникальный идентификатор лицензии, версию лицензии), идентификатор сертификата, которым подписан заголовок тикета, контрольную сумму (MD5) файла ключа, уникальный идентификатор установки ПО на Компьютере, тип и идентификатор обновляемого приложения, идентификатор задачи обновления;

- информацию о наборе всех установленных обновлений, а также о наборе последних установленных и/или удаленных обновлений, тип события, служащего причиной отправки информации об обновлениях, период времени, прошедший после установки последнего обновления, информацию о загруженных в момент предоставления информации антивирусных базах;

- информацию о работе ПО на Компьютере: данные по использованию процессора (CPU), данные по использованию памяти (Private Bytes, Non-Paged Pool, Paged Pool), количество активных потоков в процессе ПО и потоков в состоянии ожидания, длительность работы ПО до возникновения ошибки, признак работы ПО в интерактивном режиме;

- количество дампов ПО и дампов системы (BSOD) с момента установки ПО и с момента последнего обновления, идентификатор и версия модуля ПО, в котором произошел сбой, стек памяти в продуктовом процессе и информация об антивирусных базах в момент сбоя;

- данные о дампе системы (BSOD): признак возникновения BSOD на Компьютере, имя драйвера, вызвавшего BSOD, адрес и стек памяти в драйвере, признак длительности сессии ОС до возникновения BSOD, стек памяти падения драйвера, тип сохраненного дампа памяти, признак того, что сессия работы ОС до BSOD длилась более 10 минут, уникальный идентификатор дампа, дата и время возникновения BSOD;

- данные об ошибках или проблемах с производительностью, возникших в работе компонентов ПО: идентификатор состояния ПО, тип, код и причина ошибки, а также время ее возникновения, идентификаторы компонента, модуля и процесса продукта, в котором возникла ошибка, идентификатор задачи или категории обновления, при выполнении которой возникла ошибка, логи драйверов, используемых ПО (код ошибки, имя модуля, имя исходного файла и строка, где произошла ошибка);

- данные об обновлениях антивирусных баз и компонент ПО: имена, даты и время индексных файлов, загруженных в результате последнего обновления и загружаемых в текущем обновлении;

- информацию об аварийных завершениях работы ПО: дату и время создания дампа, его тип, тип события, вызвавшего аварийное завершение работы ПО (непредвиденное отключение питания, падение приложения стороннего правообладателя), дату и время непредвиденного отключения питания;

- информацию о совместимости драйверов ПО с аппаратным и программным обеспечением: информацию о свойствах ОС, накладывающих ограничения на функциональность компонентов ПО (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), тип встроенного ПО загрузки (UEFI, BIOS), признак наличия доверенного платформенного модуля (Trusted Platform Module, TPM), версия спецификации TPM, информацию об установленном на компьютере центральном процессоре (CPU), режим и параметры работы Code Integrity и Device Guard, режим работы драйверов и причина использования текущего режима, версию драйверов ПО, статус поддержки драйверами программных и аппаратных средств виртуализации Компьютера;

- информацию о сторонних приложениях, вызвавших ошибку: их название, версию и локализацию, код ошибки и информацию о ней из системного журнала приложений, адрес возникновения ошибки и стек памяти стороннего приложения, признак возникновения ошибки в компоненте ПО, длительность работы стороннего приложения до возникновения ошибки, контрольные суммы (MD5, SHA2-256, SHA1) образа процесса приложения, в котором произошла ошибка, путь к этому образу процесса приложения и код шаблона пути, информацию из системного журнала ОС с описанием ошибки, связанной с приложением, информацию о модуле приложения, в котором произошла ошибка (идентификатор ошибки, адрес ошибки как смещение в модуле, имя и версию модуля, идентификатор падения приложения в плагине Правообладателя и стек памяти такого падения, время работы приложения до сбоя);

- версию компонента обновления ПО, количество аварийных завершений работы компонента обновления ПО при выполнении задач обновления за время работы компонента, идентификатор типа задачи обновления, количество неуспешных завершений задач обновления компонента обновления ПО;

- информацию о работе компонентов мониторинга системы: полные версии компонентов, дату и время запуска компонентов, код события, которое переполнило очередь событий, и количество таких событий, общее количество переполнений очереди событий, информация о файле процесса-инициатора события (название файла и путь к нему на Компьютере, код шаблона пути, контрольные суммы (MD5, SHA2-256, SHA1) процесса, связанного с файлом, версия файла), идентификатор выполненного перехвата события, полная версия фильтра перехвата, идентификатор типа перехваченного события, размер очереди событий и количество событий между первым событием в очереди и текущим событием, количество просроченных событий в очереди, информация о процессе-инициаторе текущего события (название файла процесса и путь к нему на Компьютере, код шаблона пути, контрольные суммы (MD5, SHA2-256, SHA1) процесса), время обработки события, максимально допустимое время обработки событий, значение вероятности отправки данных, информацию о событиях ОС, время обработки которых ПО превысило ограничение на время ожидания (дата и время получения события, количество повторных инициализаций антивирусных баз, дату и время последней повторной инициализации антивирусных баз после их обновления, время задержки обработки события каждым компонентом мониторинга системы, количество ожидающих событий, количество обработанных событий, количество задержанных событий текущего типа, суммарное время задержки событий текущего типа, суммарное время задержки всех событий);

- информацию от инструмента трассировки событий Windows (Event Tracing for Windows, ETW) при проблемах с производительностью ПО, поставщики событий SysConfig / SysConfigEx / WinSATAssessment от Microsoft: данные о компьютере (модель, производитель, форм-фактор корпуса, версия), данные о метриках производительности Windows (данные WinSAT-оценки, индекс производительности Windows), имя домена, данные о физических и логических процессорах (количество физических и логических процессоров, производитель, модель, степпинг, количество ядер, тактовая частота, идентификатор процессора (CPUID), характеристики кеша, характеристики логического процессора, признаки поддержки режимов и инструкций), данные о модулях оперативной памяти (тип, форм-фактор, производитель, модель, объем, гранулярность выделения памяти), данные о сетевых интерфейсах (IP- и MAC-адреса, название, описание, конфигурация сетевых интерфейсов, распределение числа и объема сетевых пакетов по типам, скорость сетевого обмена, распределение числа сетевых ошибок по типам), конфигурацию IDE-контроллера, IP-адреса DNS-серверов, данные о видеокарте (модель, описание, производитель, совместимость, объем видеопамяти, разрешение экрана, количество бит на пиксель, версия BIOS), данные о подключенных самонастраиваемых (Plug-and-Play) устройствах (название, описание, идентификатор устройства [PnP, ACPI], данные о дисках и накопителях (количество дисков или флеш-накопителей, производитель, модель, объем диска, число цилиндров, число дорожек на цилиндр, число секторов на дорожку, объем сектора, характеристики кеша, порядковый номер, число разделов, конфигурация контролера SCSI), данные о логических дисках (порядковый номер, объем раздела, объем тома, буква тома, тип раздела, тип файловой системы, количество кластеров, размер кластера, число секторов в кластере, число занятых и свободных кластеров, буква загрузочного тома, адрес-смещение раздела относительно начала диска), данные о BIOS материнской платы (производитель, дата выпуска, версия), данные о материнской плате (производитель, модель, тип), данные о физической памяти (общий и свободный объем), данные о службах операционной системы (имя, описание, статус, тег, данные о процессах [имя и идентификатор PID]), параметры энергопотребления компьютера, конфигурацию контролера прерываний, пути к системным папкам Windows (Windows и System32), данные об ОС (версия, сборка, дата выпуска, название, тип, дата установки), размер файла подкачки, данные о мониторах (количество, производитель, разрешение экрана, разрешающая способность, тип), данные о драйвере видеокарты (производитель, дата выпуска, версия);

- информацию от ETW, поставщики событий EventTrace / EventMetadata от Microsoft: данные о последовательности системных событий (тип, время, дата, часовой пояс), метаданные о файле с результатами трассировки (имя, структура, параметры трассировки, распределение числа операций трассировки по типам), данные об ОС (название, тип, версия, сборка, дата выпуска, время старта);

- информацию от ETW, поставщики событий Process / Microsoft-Windows-Kernel-Process / Microsoft-Windows-Kernel-Processor-Power от Microsoft: данные о запускаемых и завершаемых процессах (имя, идентификатор PID, параметры старта, командная строка, код возврата, параметры управления питанием, время запуска и завершения, тип маркера доступа, идентификатор безопасности SID, идентификатор сеанса SessionID, число установленных дескрипторов), данные об изменении приоритетов потоков (идентификатор потока TID, приоритет, время), данные о дисковых операциях процесса (тип, время, объем, число), история изменения структуры и объема используемой процессом памяти;

- информацию от ETW, поставщики событий StackWalk / Perfinfo от Microsoft: данные счетчиков производительности (производительность отдельных участков кода, последовательность вызовов функций, идентификатор процесса PID, идентификатор потока TID, адреса и атрибуты обработчиков прерываний ISR и отложенных вызовов процедур DPC);

- информацию от ETW, поставщик событий KernelTraceControl-ImageID от Microsoft: данные об исполняемых файлах и динамических библиотеках (имя, размер образа, полный путь), данные о PDB-файлах (имя, идентификатор), данные ресурса VERSIONINFO исполняемого файла (название, описание, производитель, локализация, версия и идентификатор приложения, версия и идентификатор файла);

- информацию от ETW, поставщики событий FileIo / DiskIo / Image / Windows-Kernel-Disk от Microsoft: данные о файловых и дисковых операциях (тип, объем, время начала, время завершения, длительность, статус завершения, идентификатор процесса PID, идентификатор потока TID, адреса вызовов функций драйвера, пакет запроса ввода-вывода (I/O Request Packet, IRP), атрибуты файлового объекта Windows), данные о файлах, участвующих в файловых и дисковых операциях (имя, версия, размер, полный путь, атрибуты, смещение, контрольная сумма образа, опции открытия и доступа);

- информацию от ETW, поставщик событий PageFault от Microsoft: данные об ошибках доступа к страницам памяти (адрес, время, объем, идентификатор процесса PID, идентификатор потока TID, атрибуты файлового объекта Windows, параметры выделения памяти);

- информацию от ETW, поставщик событий Thread от Microsoft: данные о создании / завершении потоков, данные о запущенных потоках (идентификатор процесса PID, идентификатор потока TID, размер стека, приоритеты и распределение ресурсов CPU, ресурсов ввода-вывода, страниц памяти между потоками, адрес стека, адрес начальной функции, адрес блока окружения потока (Thread Environment Block, TEB), тег службы Windows);

- информацию от ETW, поставщик событий Microsoft-Windows-Kernel-Memory от Microsoft: данные об операциях управления памятью (статус завершения, время, количество, идентификатор процесса PID), структура распределения памяти (тип, объем, идентификатор сеанса SessionID, идентификатор процесса PID);

- информацию о работе ПО при появлении проблем с производительностью: идентификатор установки ПО, тип и значение снижения производительности, данные о последовательности внутренних событий ПО (время, часовой пояс, тип, статус завершения, идентификатор компонента ПО, идентификатор сценария работы ПО, идентификатор потока TID, идентификатор процесса PID, адреса вызовов функций), данные о проверяемых сетевых соединениях (URL, направление соединения, размер сетевого пакета), данные о PDB-файлах (имя, идентификатор, размер образа исполняемого файла), данные о проверяемых файлах (имя, полный путь, контрольная сумма), параметры мониторинга производительности ПО;

- информацию о неуспешной последней перезагрузке ОС: количество неуспешных перезагрузок с момента установки ОС, данные о дампе системы (код и параметры ошибки, имя, версия и контрольная сумма (CRC32) модуля, вызвавшего ошибку в работе ОС, адрес ошибки как смещение в модуле, контрольные суммы (MD5, SHA2-256, SHA1) дампа системы);

- информацию для проверки подлинности сертификатов, которыми подписаны файлы: отпечаток сертификата, алгоритм вычисления контрольной суммы, публичный ключ и серийный номер сертификата, имя эмитента сертификата, результат проверки сертификата и идентификатор базы сертификатов;

- информацию о процессе, выполняющем атаку на самозащиту ПО: имя и размер файла процесса, его контрольные суммы (MD5, SHA2-256, SHA1), полный путь к нему и код шаблона пути, даты и время создания и компоновки файла процесса, код типа файла процесса, признак исполняемого файла, атрибуты файла процесса, информацию о сертификате, которым подписан файл процесса, тип учетной записи, от имени которой процесс или поток выполняет подозрительные действия, идентификатор операций, которые осуществлялись для доступа к процессу, тип ресурса, с которым выполняется операция (процесс, файл, объект реестра, поиск окна с помощью функции FindWindow), имя ресурса, с которым выполняется операция, признак успешности выполнения операции, статус файла процесса и его подписи в KSN;

- информацию о ПО Правообладателя: полную версию, тип, локализацию и статус работы используемого ПО, версии установленных компонентов ПО и статус их работы, данные об установленных обновлениях ПО, а также значение фильтра TARGET, версию используемого протокола соединения с сервисами Правообладателя;

- информацию об установленном на Компьютере аппаратном обеспечении: тип, название, модель, версию прошивки, характеристики встроенных и подключенных устройств, уникальный идентификатор Компьютера, на котором установлено ПО;

- информацию о версии установленной на Компьютере операционной системы (ОС) и установленных пакетов обновлений, разрядность, редакцию и параметры режима работы ОС, версию и контрольные суммы (MD5, SHA2-256, SHA1) файла ядра ОС, дату и время запуска ОС;

- исполняемые и неисполняемые файлы целиком или частично;

- участки оперативной памяти Компьютера;

- сектора, участвующие в процессе загрузки операционной системы;
- пакеты данных сетевого трафика;
- веб-страницы и электронные письма, содержащие подозрительные и вредоносные объекты;
- описание классов и экземпляров классов WMI хранилища;
- отчеты об активностях приложений:
  - имя, размер и версия отправляемого файла, его описание и контрольные суммы (MD5, SHA2-256, SHA1), идентификатор формата, название его производителя, название продукта, к которому относится файл, полный путь к файлу на Компьютере и код шаблона пути, дата и время создания и модификации файла;
  - даты и время начала и окончания срока действия сертификата, если отправляемый файл имеет ЭЦП, дата и время подписания, имя эмитента сертификата, информация о владельце сертификата, отпечаток и открытый ключ сертификата и алгоритмы их вычисления, серийный номер сертификата;
  - имя учетной записи, от которой запущен процесс;
  - контрольные суммы (MD5, SHA2-256, SHA1) имени Компьютера, на котором запущен процесс;
  - заголовки окон процесса;
  - идентификатор антивирусных баз, название обнаруженной угрозы согласно классификации Правообладателя;
  - информацию об установленной в ПО лицензии, идентификатор лицензии, ее тип и дата истечения;
  - локальное время Компьютера в момент предоставления информации;
  - имена и пути к файлам, к которым получал доступ процесс;
  - имена ключей реестра и их значения, к которым получал доступ процесс;
  - URL- и IP-адреса, к которым обращался процесс;
  - URL- и IP-адреса, с которых был получен запускаемый файл.

Предоставление данных при использовании решений Detection and Response

На компьютерах с установленным приложением Kaspersky Endpoint Security хранятся данные, подготовленные для автоматической отправки на серверы решений Kaspersky Endpoint Detection and Response, Kaspersky Sandbox и Kaspersky Anti Targeted Attack Platform. Файлы хранятся на компьютерах в открытом незашифрованном виде.

Конкретный состав данных зависит от решения, в составе которого используется Kaspersky Endpoint Security.

Все данные, которые приложение хранит локально на компьютере, будут удалены с компьютера при удалении Kaspersky Endpoint Security.

Данные о результатах выполнения задачи Поиск IOC (стандартная задача)

Kaspersky Endpoint Security автоматически передает данные о результатах выполнения задач *Поиск IOC* в Kaspersky Security Center.

Данные в результатах выполнения задач *Поиск IOC* могут содержать следующую информацию:

- IP-адрес из ARP-таблицы.
- Физический адрес из ARP-таблицы.
- Тип и имя записи DNS.
- IP-адрес защищаемого компьютера.
- Физический адрес (MAC) защищаемого компьютера.
- Идентификатор записи в журнале событий.
- Имя источника данных в журнале.
- Имя журнала.
- Время события.
- MD5 и SHA256-хеши файла.
- Полное имя файла (включая путь).
- Размер файла.
- Удаленные IP-адрес и порт, с которыми было установлено соединение в момент проверки.
- IP-адрес локального адаптера.
- Порт, открытый на локальном адаптере.
- Протокол в виде числа (в соответствии со стандартом IANA).
- Имя процесса.
- Аргументы процесса.

- Путь к файлу процесса.
- Windows идентификатор процесса (PID).
- Windows идентификатор родительского процесса (PID).
- Имя учетной записи пользователя, запустившего процесс.
- Дата и время запуска процесса.
- Имя службы.
- Описание службы.
- Путь и имя DLL-службы (для svchost).
- Путь и имя исполняемого файла службы.
- Windows идентификатор службы (PID).
- Тип службы (например, драйвер ядра или адаптер).
- Статус службы.
- Режим запуска службы.
- Имя учетной записи пользователя.
- Наименование тома.
- Буква тома.
- Тип тома.
- Значение реестра Windows.
- Значение куста реестра.
- Путь к ключу реестра (без куста и без имени значения).
- Параметр реестра.
- Система (окружение).
- Имя и версия операционной системы, установленной на компьютере.
- Сетевое имя защищаемого компьютера.
- Домен или группа, к которому принадлежит защищаемый компьютер.
- Имя браузера.
- Версия браузера.
- Время последнего обращения к веб-ресурсу.

- URL из HTTP-запроса.
- Имя учетной записи, под которой выполнен HTTP-запрос.
- Имя файла процесса, выполнившего HTTP-запрос.
- Полный путь к файлу процесса, выполнившего HTTP-запрос.
- Windows идентификатор (PID) процесса, выполнившего HTTP-запрос.
- HTTP referer (URL источника HTTP-запроса).
- URI ресурса, запрошенного по протоколу HTTP.
- Информация о HTTP агенте пользователя (приложении, выполнившем HTTP-запрос).
- Время выполнения HTTP-запроса.
- Уникальный идентификатор процесса, выполнившего HTTP-запрос.

Данные для построения цепочки развития угрозы

Данные для построения цепочки развития угрозы по умолчанию хранятся семь дней. Эти данные автоматически передаются в Kaspersky Security Center.

Данные для построения цепочки развития угрозы могут содержать следующую информацию:

- Дата и время инцидента.
- Имя обнаружения.
- Режим проверки.
- Статус последнего действия, связанного с обнаружением.
- Причина неудачной обработки обнаружения.
- Тип обнаруженного объекта.
- Имя обнаруженного объекта.
- Статус угрозы после обработки объекта.
- Причина неудачного выполнения действий над объектом.
- Действия, выполняемые для отката вредоносных действий.
- Об обрабатываемом объекте:
  - Уникальный идентификатор процесса.
  - Уникальный идентификатор родительского процесса.

- Уникальный идентификатор файла процесса.
- Идентификатор процесса Windows (PID).
- Командная строка процесса.
- Имя учетной записи пользователя, запустившего процесс.
- Код сеанса входа в систему, в котором запущен процесс.
- Тип сеанса, в котором запущен процесс.
- Уровень целостности обрабатываемого процесса.
- Принадлежность учетной записи пользователя, запустившего процесс, к привилегированным локальным и доменным группам.
- Идентификатор обрабатываемого объекта.
- Полное имя обрабатываемого объекта.
- Идентификатор защищаемого устройства.
- Полное имя объекта (имя локального файла или веб-адрес загружаемого файла).
- MD5 и SHA256-хеши обрабатываемого объекта.
- Тип обрабатываемого объекта.
- Дата создания обрабатываемого объекта.
- Дата последнего изменения обрабатываемого объекта.
- Размер обрабатываемого объекта.
- Атрибуты обрабатываемого объекта.
- Организация, подписавшая обрабатываемый объект.
- Результат проверки цифрового сертификата обрабатываемого объекта.
- Идентификатор безопасности (SID) обрабатываемого объекта.
- Идентификатор часового пояса обрабатываемого объекта.
- Веб-адрес загрузки обрабатываемого объекта (только для файла на диске).
- Название приложения, загрузившего файл.
- MD5 и SHA256-хеши приложения, загрузившего файл.
- Название приложения, последний раз изменившего файл.
- MD5 и SHA256-хеши приложения, последний раз изменившего файл.

- Количество запусков обрабатываемого объекта.
- Дата и время первого запуска обрабатываемого объекта.
- Уникальный идентификатор файла.
- Полное имя файла (имя локального файла или веб-адрес загружаемого файла).
- Путь к обрабатываемой переменной реестра Windows.
- Имя обрабатываемой переменной реестра Windows.
- Значение обрабатываемой переменной реестра Windows.
- Тип обрабатываемой переменной реестра Windows.
- Показатель принадлежности обрабатываемого ключа реестра к точке автозапуска.
- Веб-адрес обрабатываемого веб-запроса.
- Источник ссылок обрабатываемого веб-запроса.
- Агент пользователя обрабатываемого веб-запроса.
- Тип обрабатываемого веб-запроса (`GET` или `POST`).
- Локальный IP-порт для обрабатываемого веб-запроса.
- Удаленный IP-порт для обрабатываемого веб-запроса.
- Направление соединения (входящее или исходящее) обрабатываемого веб-запроса.
- Идентификатор процесса, в который произошло внедрение вредоносного кода.

Kaspersky Sandbox

Все данные, которые приложение хранит локально на компьютере, будут удалены с компьютера при удалении Kaspersky Endpoint Security.

Служебные данные

Kaspersky Endpoint Security хранит следующие данные, обрабатываемые при автоматическом реагировании:

- Обрабатываемые файлы и данные, передаваемые пользователем в ходе настройки параметров встроенного агента Kaspersky Endpoint Security:
  - Файлы на карантине.
  - Открытый ключ сертификата для интеграции с Kaspersky Sandbox.

- Кеш встроенного агента Kaspersky Endpoint Security:
  - Время записи результата проверки в кеш.
  - MD5-хеш задачи проверки.
  - Идентификатор задачи проверки.
  - Результат проверки объекта.
- Очередь запросов на проверку объекта:
  - Идентификатор объекта в очереди.
  - Время помещения объекта в очередь.
  - Статус обработки объекта в очереди.
  - Идентификатор пользовательской сессии в операционной системе, в которой создана задача на проверку объекта.
  - Системный идентификатор (SID) пользователя операционной системы, под учетной записью которого создана задача.
  - MD5-хеш задачи проверки объекта.
- Информация о задачах, для которых встроенный агент Kaspersky Endpoint Security ожидает результат проверки от Kaspersky Sandbox:
  - Время получения задачи на проверку объекта.
  - Статус обработки объекта.
  - Идентификатор пользовательской сессии в операционной системе, в которой создана задача на проверку объекта.
  - Идентификатор задачи на проверку объекта.
  - MD5-хеш задачи проверки объекта.
  - Системный идентификатор (SID) пользователя операционной системы, под учетной записью которого создана задача.
  - XML-схема автоматически созданного IOC.
  - MD5 и SHA256-хеши проверяемого объекта.
  - Ошибки обработки.
  - Имена объектов, для которых создана задача.
  - Результат проверки объекта.

Данные из запросов к Kaspersky Sandbox

Следующие данные из запросов от встроенного агента Kaspersky Endpoint Security к Kaspersky Sandbox хранятся локально на компьютере:

- MD5-хеш задачи проверки.
- Идентификатор задачи проверки.
- Проверяемый объект и все связанные с ним файлы.

Данные о результатах выполнения задачи Поиск IOC (автономная задача)

Kaspersky Endpoint Security автоматически передает данные о результатах выполнения задач *Поиск IOC* в Kaspersky Security Center.

Данные в результатах выполнения задач *Поиск IOC* могут содержать следующую информацию:

- IP-адрес из ARP-таблицы.
- Физический адрес из ARP-таблицы.
- Тип и имя записи DNS.
- IP-адрес защищаемого компьютера.
- Физический адрес (MAC) защищаемого компьютера.
- Идентификатор записи в журнале событий.
- Имя источника данных в журнале.
- Имя журнала.
- Время события.
- MD5 и SHA256-хеши файла.
- Полное имя файла (включая путь).
- Размер файла.
- Удаленные IP-адрес и порт, с которыми было установлено соединение в момент проверки.
- IP-адрес локального адаптера.
- Порт, открытый на локальном адаптере.
- Протокол в виде числа (в соответствии со стандартом IANA).

- Имя процесса.
- Аргументы процесса.
- Путь к файлу процесса.
- Windows идентификатор процесса (PID).
- Windows идентификатор родительского процесса (PID).
- Имя учетной записи пользователя, запустившего процесс.
- Дата и время запуска процесса.
- Имя службы.
- Описание службы.
- Путь и имя DLL-службы (для svchost).
- Путь и имя исполняемого файла службы.
- Windows идентификатор службы (PID).
- Тип службы (например, драйвер ядра или адаптер).
- Статус службы.
- Режим запуска службы.
- Имя учетной записи пользователя.
- Наименование тома.
- Буква тома.
- Тип тома.
- Значение реестра Windows.
- Значение куста реестра.
- Путь к ключу реестра (без куста и без имени значения).
- Параметр реестра.
- Система (окружение).
- Имя и версия операционной системы, установленной на компьютере.
- Сетевое имя защищаемого компьютера.
- Домен или группа, к которому принадлежит защищаемый компьютер.
- Имя браузера.

- Версия браузера.
- Время последнего обращения к веб-ресурсу.
- URL из HTTP-запроса.
- Имя учетной записи, под которой выполнен HTTP-запрос.
- Имя файла процесса, выполнившего HTTP-запрос.
- Полный путь к файлу процесса, выполнившего HTTP-запрос.
- Windows идентификатор (PID) процесса, выполнившего HTTP-запрос.
- HTTP referer (URL источника HTTP-запроса).
- URI ресурса, запрошенного по протоколу HTTP.
- Информация о HTTP агенте пользователя (приложении, выполнившем HTTP-запрос).
- Время выполнения HTTP-запроса.
- Уникальный идентификатор процесса, выполнившего HTTP-запрос.

Kaspersky Endpoint Detection and Response Expert (on-premises)

Все данные, которые приложение хранит локально на компьютере, будут удалены с компьютера при удалении Kaspersky Endpoint Security.

Служебные данные

Встроенный агент Kaspersky Endpoint Security хранит локально следующие данные:

- Данные, необходимые для интеграции с компонентом EDR Expert (on-premises):
  - Адрес и порт для подключения к серверу KATA Central Node.
  - Адрес и порт для подключения к серверу передачи телеметрии.
  - Адрес и порт для подключения к серверу реагирования.
  - Информация о сертификатах для интеграции с KATA Central Node.
  - Информация о сертификатах для интеграции с сервером передачи телеметрии.
  - Информация о сертификатах для интеграции с сервером реагирования.
- Файлы на карантине.

Данные из передаваемых событий телеметрии

- **Данные телеметрии.**
  - Данные о файлах:
    - Уникальный идентификатор файла.
    - Тип файла.
    - Полный путь к файлу.
    - Размер файла.
    - Атрибуты файла.
    - Идентификатор зоны.
    - Дата и время создания файла.
    - Дата и время последнего изменения файла.
    - Исходное имя файла.
    - Имя приложения.
    - Версия приложения.
    - Производитель приложения.
    - Описание файла.
    - Версия файла.
    - MD5 и SHA256-хеши объекта.
    - Результат проверки подписи файла.
    - Имя издателя сертификата.
    - Имя владельца сертификата.
    - Серийный номер сертификата.
  - Данные об AMSI проверке:
    - Уникальный идентификатор процесса, инициировавшего активность.
    - Тип содержимого объекта, которое передается в AMSI.
    - Содержимое объекта, которое передается в AMSI.

    - Имя объекта.
    - MD5 и SHA256-хеши объекта.
- Данные о блокировке приложений:
    - Уникальный идентификатор процесса, инициировавшего блокировку приложения.
    - Уникальный идентификатор родительского процесса.
    - Уникальный системный идентификатор процесса.
    - Команда, используемая для запуска процесса.
    - Идентификатор сеанса входа.
    - Уровень целостности процесса.
    - Статус процесса.
    - Уникальный идентификатор файла процесса.
    - Командная строка процесса.
    - Список уникальных идентификаторов интерпретируемых файлов.
- Данные о блокировке открытии файлов:
    - Уникальный идентификатор процесса, инициировавшего открытие файла.
    - Уникальный идентификатор файла.
- Данные о загрузке драйверов:
    - Уникальный идентификатор загруженного драйвера.
- Данные о событиях:
    - Уникальный идентификатор события.
    - Дата и время события.
- Данные об изменении файлов:
    - Уникальный идентификатор процесса, инициировавшего изменение файла.
    - Уникальный идентификатор файла.
    - Тип операции изменения.
    - Флаг, указывающий, что файл помечен к удалению после перезагрузки.
    - Уникальный идентификатор модифицированного файла.
    - Уникальный идентификатор файла до изменения.

    - Набор битовых флагов, которые определяют как файл был открыт.
    - Данные об операциях над списком контроля доступа.
    - Данные о смене владельца файла или его исходной группы.
- Данные о сессии входа:
    - Идентификатор сессии входа.
    - Имя пользователя, который осуществил вход.
    - Тип аккаунта пользователя.
    - Тип сессии.
- Данные о сетевых соединениях:
    - Уникальный идентификатор процесса, инициировавшего соединение.
    - Локальный IP-адрес, через который инициировано соединение.
    - Удаленный IP-адрес конечной точки соединения.
    - Направление соединения.
    - Протокол передачи данных.
    - HTTP метод.
    - Путь без имени хоста.
    - Имя хоста.
    - Динамическое состояние процесса в момент соединения.
    - Флаг, указывающий, что соединение открыто на уровне сырого сокета.
    - Версия TLS, использованная в сеансе соединения.
    - Имя TLS сервера.
    - MD5 и SHA1-хеши сертификата TLS сервера.
    - Список Subject Alternative Names (SAN) сертификата.
    - Имя издателя TLS сертификата.
    - Серийный номер сертификата.
    - Используемый шифровальный набор.
    - Начало и окончание действие сертификата.

    - JA3 отпечаток клиентского TLS клиента.
    - JA3S отпечаток сервера.
- Данные при прослушивании сетевого порта:
    - Уникальный идентификатор процесса, инициировавшего соединение.
- Данные при консольном вводе:
    - Уникальный идентификатор процесса, инициировавший консольный ввод.
    - Тип консольного ввода.
    - Текст, который был введен пользователем или процессом.
- Данные о создании процесса:
    - Уникальный идентификатор процесса.
    - Уникальный идентификатор родительского процесса.
    - Уникальный системный идентификатор процесса.
    - Команда, используемая для запуска процесса.
    - Идентификатор сеанса входа.
    - Уровень целостности процесса.
    - Уникальный идентификатор файла процесса.
    - Список уникальных идентификаторов интерпретируемых файлов.
    - Тип процесса.
- Данные о загрузке модуля процессом:
    - Уникальный идентификатор процесса, который произвел загрузку.
    - Полный путь к файлу, который был загружен в процесс.
    - Уникальный идентификатор файла-модуля.
    - Полное квалифицированное имя .NET-сборки, если загруженный файл является .NET-модулем.
    - Флаги .NET-сборки, определяемые в ее манифесте.
- Данные о завершении процесса:
    - Уникальный идентификатор завершенного процесса.

- Данные об изменении реестра:
  - Уникальный идентификатор процесса, который инициировал изменение реестра.
  - Тип операции над реестром.
  - Полный путь к ключу реестра.
  - Имя значения внутри ключа реестра.
  - Тип данных, которые записаны в значение ключа реестра.
  - Данные, записанные в значение ключа реестра.
  - Предыдущее имя ключа до переименования.
  - Информация о смене владельца или основной группы ключа.
  - Список изменений в списке контроля доступа (ACL) ключа.
- Данные об обнаруженной угрозе и ее обработке:
  - Флаг, указывающий, что обнаружение угрозы прошло в фоновом режиме.
  - Вердикт, присвоенный угрозе.
  - Наименование вердикта.
  - Уникальный идентификатор записи в базе.
  - Время, когда запись об угрозе была сохранена в базе.
  - Режим обработки угрозы.
  - Тип зараженного объекта.
  - Имя зараженного объекта.
  - MD5 и SHA256-хеши объекта.
  - Уникальный идентификатор зараженного объекта.
  - Уникальный идентификатор процесса, скачавшего зараженный объект из интернета.
  - URL, по которому был скачан зараженный объект.
  - Электронный адрес отправителя, приславшего зараженный объект.
  - Сетевой протокол, через который был получен зараженный объект.
  - Локальный адрес, с которого был получен зараженный объект.
  - Внешний адрес, с которого был получен зараженный объект.

    - Тип содержимого объекта.
    - Содержание объекта.
- Данные о доступе к процессам:
    - Уникальный идентификатор процесса совершившего попытку доступа.
    - Уникальный идентификатор целевого процесса, к которому осуществлялся доступ.
    - Набор прав, запрошенных у целевого процесса.
    - Тип операции.
    - Набор вызовов в момент обращения к процессу.
    - Дескриптор процесса-источника.
    - Дескриптор целевого процесса.
- Данные о DNS:
    - Уникальный идентификатор процесса, который инициировал DNS-запрос.
    - IP-адрес DNS сервера.
    - Флаги, управляющие поведением DNS запроса.
    - Статус выполнения запроса.
    - Полное доменное имя, указанное в DNS запросе.
    - Тип данных в DNS запросе.
    - Ответы DNS сервера.
- Данные о внедрении кода:
    - Уникальный идентификатор процесса, который пытался внедрить код.
    - Использованный способ доступа.
    - Набор вызовов в момент обнаружения внедренного кода.
    - Уникальный идентификатор целевого процесса, в который был загружен код.
    - Данные об изменении командного ряда целевого процесса.
    - Адрес целевого процесса.
    - Имя DLL-библиотеки, которая была загружена в целевой процесс.
    - Полный путь к DLL-файлу.

- Данные об операциях с именованными каналами:
  - Уникальный идентификатор процесса, который создал или подключился к каналу.
  - Полное имя именованного канала.
  - Тип операции (создание или подключение).
- Данные о запросах WMI:
  - Уникальный идентификатор процесса, который инициировал WMI-операцию.
  - Тип WMI-операции.
  - Имя целевого устройства для WMI-запроса.
  - Учетная запись, от имени которой выполнен WMI-запрос.
  - Текст WMI-запроса.
  - Пространство имен, в котором выполняется WMI-запрос.
  - Имя WMI-фильтра.
  - Имя объекта-потребителя.
  - Текст, описывающий действие объекта-потребителя.
- Данные о LDAP запросах:
  - Уникальный идентификатор процесса, выполнившего LDAP-запрос.
  - Область поиска в LDAP запросах.
  - LDAP фильтр.
  - Параметр, указывающий, к какому разделу Active Directory был направлен запрос.
  - Атрибуты LDAP поиска.
- Данные о подключенных USB устройствах:
  - Тип операции USB устройства.
  - Тип USB устройства.
  - Идентификатор USB устройства.
  - Имя USB устройства.
  - Путь к USB устройству.
  - Флаг, указывающий, что USB устройство является системным диском.
- Данные о создании, удалении и изменении задачи по расписанию.

- Данные о создании, удалении и изменении служб.
- Данные о монтировании / размонтировании файловой системы.
- Данные о работе EDR Expert on-premise компонента:
  - Информация о запуске / остановке агента.
  - Информация об установке / удалении агента.
  - Уникальный идентификатор запуска агента.
  - Системный идентификатор процесса агента.
  - Уникальный идентификатор процесса агента.
  - Причина завершения работы агента.
  - Код завершения процесса агента.
- Параметры фильтрации событий:
  - Имена модулей.
  - Полные пути к объектам.
  - MD5 и SHA256-хеши объектов.
  - Идентификаторы записей в журнале событий Windows.
  - Параметры цифровых сертификатов.
  - Направление трафика, IP-адреса, порты, протоколы, полные пути к исполняемым файлам.
  - Имена пользователей.
  - Типы входа пользователей.
  - Типы событий телеметрии, для которых применяются фильтры.

Данные из запросов от EDR Expert к встроенному агенту Kaspersky Endpoint Security

- Общие параметры задач:
  - Типы задач.
  - Параметры расписания запуска задач.
  - Имена и пароли учетных записей, под которыми необходимо запускать задачи.
  - Версии параметров.

- Идентификаторы объектов на карантине.
- Пути к объектам.
- MD5 и SHA256-хеши объектов.
- Командная строка запуска процесса с аргументами.
- Флаги дополнительных действий, выполняемых по завершении задачи.
- Идентификаторы IOC-файлов, которые нужно получить с сервера.
- IOC-файлы.
- Наименование служб.
- Тип запуска служб.
- Папки, для которых необходимо получить результаты задачи *Сбор форензик*.
- Маски имен объектов и расширений для задачи *Сбор форензик*.

- Параметры Сетевой изоляции:
  - Типы параметров.
  - Версии параметров.
  - Списки исключений из Сетевой изоляции и параметры исключений: направление трафика, IP-адреса, порты, протоколы, полные пути к исполняемым файлам.
  - Флаги дополнительных действий.
  - Время автоматического отключения изоляции.
- Параметры Запрета запуска объектов:
  - Типы параметров.
  - Версии параметров.
  - Списки правил Запрета запуска объектов и параметры правил: пути к объектам, типы объектов, MD5 и SHA256-хеши объектов.
  - Флаги дополнительных действий.

Данные из запросов от Kaspersky Endpoint Security к компоненту EDR Expert

При интеграции с решением EDR Expert (on-premises) следующие данные хранятся локально на компьютерах.

- В запросах на синхронизацию:
  - Уникальный идентификатор.
  - Базовая часть веб-адреса сервера.
  - Имя компьютера.
  - IP-адрес компьютера.
  - MAC-адрес компьютера.
  - Локальное время на компьютере.
  - Статус самозащиты Kaspersky Endpoint Security.
  - Имя и версия операционной системы, установленной на компьютере.
  - Версия Kaspersky Endpoint Security.
  - Версии параметров приложения и параметров задач.
  - Состояние задач (идентификаторы задач, статусы выполнения, коды ошибок).
- В запросах на получение файлов с сервера:
  - Уникальные идентификаторы файлов.
  - Уникальный идентификатор Kaspersky Endpoint Security.
  - Уникальные идентификаторы задач.
  - Базовая часть веб-адреса сервера с компонентом Central Node.
  - IP-адрес узла.
- В отчетах о результатах выполнения задач:
  - IP-адрес узла.
  - Информация об объектах, обнаруженных при поиске IOC или YARA-проверке.
  - Флаги дополнительных действий, выполняемых по завершении задач.
  - Ошибки выполнения задач и коды возврата.
  - Статусы, с которыми завершались задачи.
  - Время завершения выполнения задач.

- Версии параметров, с которыми выполнялись задачи.
- Информация об объектах, переданных на сервер, помещенных на карантин, восстановленных из карантина: пути к объектам, MD5 и SHA256-хеши объектов, идентификаторы объектов на карантине.
- Информация о процессах, запущенных или остановленных на компьютере по запросу сервера: PID и UniquePID, код ошибки, MD5 и SHA256-хеши объектов.
- Информация о службах, запущенных или остановленных на компьютере по запросу сервера (имя службы, тип запуска, код ошибки, MD5 и SHA256-хеши файловых образов служб).
- Информация об объектах, для которых был снят дамп памяти для YARA-проверки (пути, идентификатор файла дампа).
- Файлы, запрошенные сервером.

- Данные о запущенных процессах:
  - Имя исполняемого файла, включая полный путь и расширение.
  - Параметры автозапуска процесса.
  - Идентификатор процесса.
  - Код сеанса входа в систему.
  - Имя сеанса входа в систему.
  - Дата и время запуска процесса.
  - MD5 и SHA256-хеши объекта.
- Данные о файлах:
  - Путь к файлу.
  - Имя файла.
  - Размер файла.
  - Атрибуты файла.
  - Дата и время создания файла.
  - Дата и время последнего изменения файла.
  - Описание файла.
  - Название компании.
  - MD5 и SHA256-хеши объекта.
  - Раздел реестра (для точек автозапуска).

- Данные в ошибках получения информации об объектах:
  - Полное имя объекта, при обработке которого возникла ошибка.
  - Код ошибки.
- Данные о результатах YARA-проверки:

  Встроенный агент Kaspersky Endpoint Security автоматически передает данные результатов YARA-проверки в Kaspersky Anti Targeted Attack Platform для построения цепочки развития угрозы.

  Данные временно хранятся локально в очереди отправки результатов выполнения задач на сервер Kaspersky Anti Targeted Attack Platform. После отправки данные удаляются.
  - MD5 и SHA256-хеши файла.
  - Полное имя файла.
  - Путь к файлу.
  - Размер файла.
  - Имя процесса.
  - Аргументы процесса.
  - Путь к файлу процесса.
  - Windows идентификатор процесса (PID).
  - Windows идентификатор родительского процесса (PID).
  - Имя учетной записи пользователя, запустившего процесс.
  - Дата и время запуска процесса.
- Данные о результатах IOC проверки:
  - IP-адрес из ARP-таблицы.
  - Физический адрес из ARP-таблицы.
  - Имя DNS-записи.
  - Тип DNS-записи.
  - Имя хоста.
  - IP-адрес.
  - Идентификатор события в журнале.
  - Имя источника данных в журнале.
  - Имя журнала.
  - Имя пользователя.

- Дата и время генерации события в формате ISO.
- MD5 и SHA256-хеши файла.
- Полное имя файла.
- Размер файла.
- Удаленный IP и порт, с которым установлено соединение в момент проверки.
- IP и порт локального адаптера.
- Протокол.
- Имя процесса.
- Аргументы процесса.
- Путь к файлу процесса.
- Windows идентификатор процесса (PID).
- Windows идентификатор родительского процесса (PID).
- Имя учетной записи пользователя, запустившего процесс.
- Дата и время запуска процесса.
- Путь к ключу реестра.
- Имя ключа реестра.
- Текстовое значение ключа реестра.
- Имя сервиса.
- Описание сервиса.
- Путь и имя DLL сервиса.
- Путь и имя исполняемого файла сервиса.
- Windows идентификатор сервиса (PID).
- Тип сервиса.
- Статус сервиса.
- Режим запуска сервиса.
- Название операционной системы.
- Версия операционной системы.
- Сетевое имя компьютера без домена.

- Домен или рабочая группа.
- Имя пользователя.
- Имя тома.
- Буква тома.
- Тип тома.

Kaspersky Network Detection and Response (KATA)

Все данные, которые приложение хранит локально на компьютере, будут удалены с компьютера при удалении Kaspersky Endpoint Security.

Данные телеметрии

- **Данные о файлах**
  - Уникальный идентификатор файла.
  - Тип файла.
  - Полный путь к файлу.
  - Размер файла.
  - Атрибуты файла.
  - Идентификатор зоны.
  - Дата и время создания файла.
  - Дата и время последнего изменения файла.
  - Исходное имя файла.
  - Имя приложения.
  - Версия приложения.
  - Производитель приложения.
  - Описание файла.
  - Версия файла.
  - MD5 и SHA256-хеши объекта.

- Результат проверки подписи файла.
- Дата и время создания подписи файла.
- Цепочки сертификатов, примененные в файле подписи.
- Тип цепочки сертификатов.
- Сертификаты в цепочке.
- Имя издателя сертификата.
- Имя владельца сертификата.
- Серийный номер сертификата.
- Алгоритм отпечатка сертификата.
- Отпечаток сертификата.
- Период действия сертификата.

- **Данные о сессии входа**
  - Идентификатор сессии входа.
  - Имя учетной записи пользователя, который осуществил вход.
  - Тип учетной записи пользователя.
  - Тип сессии.
  - IP-адрес машины, с которой была выполнена попытка входа.
  - IP-адрес локальной машины, для которой была выполнена попытка входа.
  - Флаг, указывающий, что сеанс, который представляет это событие, имеет повышенные права и администратора.
  - Параметр, указывающий, связаны ли с этой сессией входа в систему другие сессии.
  - Протокол для терминальной сессии.
  - IPv4-протокол для терминальной сессии.
- **Данные о сетевых коммуникациях**
  - Начало и конец временного интервала, за который собирались данные.
  - Список соединений.
  - Локальный IP-адрес компьютера.
  - Локальный MAC-адрес компьютера.

- Удаленный IP-адрес компьютера.
- Удаленный MAC-адрес компьютера.
- IP-адрес шлюза.
- Количество отправленных пакетов данных.
- Количество принятых пакетов данных.
- Общее количество переданных байт.
- Протокол передачи данных.
- Поле Ethernet-кадра EtherType.
- Префикс полезной нагрузки первого пакета в интервале.
- IPv4-адрес сетевого интерфейса, через который была зафиксирована коммуникация.

- **Данные о сетевых соединениях**
  - Уникальный идентификатор процесса, инициировавшего соединение.
  - Протокол передачи данных.
  - Локальный IP-адрес, через который инициировано соединение.
  - Удаленный IP-адрес конечной точки соединения.
  - HTTP метод.
  - Путь без имени хоста.
  - Имя хоста.
  - Динамическое состояние процесса в момент соединения.
  - Направление соединения.
  - Состояние динамического процесса.
  - Поле Ethernet-кадра EtherType.
- **Данные при прослушивании сетевого порта**
  - Уникальный идентификатор процесса, инициировавшего соединение.
  - Протокол передачи данных.
  - Локальный адрес.
  - Динамическое состояние процесса в момент соединения.

- **Результаты проверки соединения**
  - Сетевые настройки хоста.
  - Описание сетевого интерфейса.
  - DNS-имя домена.
  - Локальный MAC-адрес компьютера.
  - Номер метрики IP-соединения.
  - Список IP-адресов.
  - IP-адрес.
  - Сетевая маска.
  - IP-адрес шлюза.
  - MAC-адрес шлюза.
  - Список установленных патчей.
  - Номер патча.
  - Дата установки патча.
  - Модель устройства.
  - Производитель устройства.
  - ID хоста в Kaspersky Security Center.
  - Описание установленного антивирусного продукта "Лаборатории Касперского".
  - Наименование компонента установленного антивирусного продукта "Лаборатории Касперского".
  - Версия компонента установленного антивирусного продукта "Лаборатории Касперского".
  - Версия базы данных компонента установленного антивирусного продукта "Лаборатории Касперского".
  - Дата последнего обновления базы данных компонента установленного антивирусного продукта "Лаборатории Касперского".
  - Статус компонента установленного антивирусного продукта "Лаборатории Касперского".
  - Список лицензионных ключей.
  - Серийный номер ключа.
  - Тип ключа.

- Дата истечения срока действия ключа.
- Статус ключа.

- **Данные о создании процесса на хосте**
  - Уникальный идентификатор процесса.
  - Уникальный идентификатор родительского процесса.
  - Уникальный системный идентификатор процесса.
  - Команда, используемая для запуска процесса.
  - Идентификатор сеанса входа.
  - Идентификатор терминального сеанса.
  - Уникальный идентификатор файла процесса.
  - Уровень целостности процесса.
  - Список токенов прав процесса.
  - Права атрибутов.
  - Список уникальных идентификаторов интерпретируемых файлов.
  - Статус процесса.
  - Команда, используемая для запуска процесса.
- **Данные о завершении процесса**
  - Уникальный идентификатор процесса.
- **Данные об обнаруженной угрозе**
  - Информация об угрозе.
  - Вердикт, присвоенный угрозе.
  - Номер записи AMR.
  - Версия антивирусной базы данных.
  - Режим обнаружения угрозы.
  - Уникальный идентификатор угрозы.
  - Технология защиты.
  - Информация о зараженном объекте.
  - Тип зараженного объекта.

- Имя зараженного объекта.
- MD5 и SHA256-хеши объекта.
- Уникальный идентификатор зараженного процесса.
- Уникальный идентификатор зараженного объекта.
- Уникальный идентификатор процесса, скачавшего зараженный объект из интернета.
- URL, по которому был скачен зараженный объект.
- Электронный адрес отправителя, приславшего зараженный объект.
- Сетевой протокол, через который был получен зараженный объект.
- Локальный адрес, с которого был получен зараженный объект.
- Внешний адрес, с которого был получен зараженный объект.
- Тип содержимого объекта.
- Контекст обнаруженной угрозы.
- Содержание объекта.
- Флаг, указывающий, что обнаружение угрозы прошло в фоновом режиме.

- **Данные об обработке угрозы**
  - Информация об угрозе.
  - Вердикт, присвоенный угрозе.
  - Номер записи AMR.
  - Версия антивирусной базы данных.
  - Режим обнаружения угрозы.
  - Имя зараженного объекта.
  - MD5 и SHA256-хеши объекта.
  - Уникальный идентификатор зараженного процесса.
  - Уникальный идентификатор зараженного объекта.
  - Сетевой протокол, через который был получен зараженный объект.
  - Локальный адрес, с которого был получен зараженный объект.
  - Внешний адрес, с которого был получен зараженный объект.
  - Статус обработки угрозы.

- Причина невозможности исправления угрозы.
- Локальный физический адрес.

- **Данные о пользователях**
  - SID пользователя.
  - Идентификатор пользователя.
  - Имя пользователя.
  - Полное имя пользователя.
  - Описание пользователя.
  - Активен или заблокирован аккаунт.
  - Истекает или нет срок действия пароля.
  - Требуется ли смена пароля.
  - Доступна ли возможность смены пароля.
  - Тип аккаунта пользователя.
  - Включен ли автоматический вход под данным аккаунтом.
  - Список групп, к которым принадлежит пользователь.

Интеграция с Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Все данные, которые приложение хранит локально на компьютере, будут удалены с компьютера при удалении Kaspersky Endpoint Security.

При интеграции с Kaspersky Unified Monitoring and Analysis Platform (KUMA) передаются данные о настройках подключения, а также все события, зарегистрированные в журналах Windows.

Основные журналы событий Windows: System, Security, Application, ForwardedEvents и HardwareEvents. Также пользователи могут создавать и работать с индивидуальными журналами в соответствии со своими требованиями.

Соответствие законодательству Европейского союза (GDPR)

Kaspersky Endpoint Security может передавать данные в "Лабораторию Касперского" при выполнении следующих условий:

- Использование Kaspersky Security Network.
- Активация приложения с помощью кода активации.

- Обновление антивирусных баз и модулей приложения.
- Переход по ссылкам в интерфейсе приложения.

Вне зависимости от классификации и территории, откуда данные были получены, "Лаборатория Касперского" использует высокий уровень стандартов защиты данных и применяет правовые, организационные и технические меры, чтобы защитить данные пользователей, гарантировать безопасность и конфиденциальность, а также обеспечить выполнение прав пользователей, гарантированных применимым законодательством. Текст Политики конфиденциальности входит в комплект поставки приложения и доступен на веб-сайте "Лаборатории Касперского".

Перед использованием Kaspersky Endpoint Security ознакомьтесь с описанием передаваемых данных в Лицензионном соглашении и Положении о Kaspersky Security Network. Если в соответствии с вашим локальным законодательством или стандартом данные, передаваемые из Kaspersky Endpoint Security в рамках любого из описанных сценариев, могут быть классифицированы как персональные, вам необходимо обеспечить законность их обработки и получить согласие конечных пользователей на сбор и передачу этих данных.

Более подробную информацию о получении, обработке, хранении и уничтожении информации об использовании приложения после принятия Лицензионного соглашения и согласия с Положением о Kaspersky Security Network вы можете узнать, прочитав тексты этих документов, а также на веб-сайте "Лаборатории Касперского". Файлы license.txt и ksn_<ID языка>.txt с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки приложения.

Если вы не хотите предоставлять данные в "Лабораторию Касперского", вы можете выключить передачу данных.

Использование Kaspersky Security Network

Используя Kaspersky Security Network, вы соглашаетесь на автоматическую передачу данных, перечисленных в Положении о Kaspersky Security Network. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", используйте Kaspersky Private Security Network (KPSN) или выключите использование KSN. Подробнее о работе KPSN см. в документации для Kaspersky Private Security Network.

Активация приложения с помощью кода активации

Используя код активации, вы соглашаетесь на автоматическую передачу данных, перечисленных в Лицензионном соглашении. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", используйте файл ключа для активации Kaspersky Endpoint Security.

Обновление антивирусных баз и модулей приложения

Используя для обновления серверы "Лаборатории Касперского", вы соглашаетесь на автоматическую передачу данных, перечисленных в Лицензионном соглашении. Информация требуется для проверки правомерности использования приложения Kaspersky Endpoint Security. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", используйте Kaspersky Security Center для обновления баз или Kaspersky Update Utility.

Переход по ссылкам в интерфейсе приложения

Используя ссылки в интерфейсе приложения, вы соглашаетесь на автоматическую передачу данных, перечисленных в Лицензионном соглашении. Точный перечень данных, передаваемых в каждой конкретной ссылке, зависит от того, где именно расположена ссылка в интерфейсе приложения и какую проблему она призвана решить. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", используйте упрощенный интерфейс приложения или скройте интерфейс приложения.

Запись дампов

Если вы включили запись дампов, Kaspersky Endpoint Security создаст файл дампа, который будет содержать всю информацию о рабочей памяти процессов приложения на момент создания этого файла.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Acrobat, Flash, Reader и Shockwave являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

Amazon, Amazon Web Services, AWS являются товарными знаками Amazon.com, Inc. или аффилированных лиц компании.

Apple, FireWire, iTunes, Mac и Safari – товарные знаки Apple Inc.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

AutoCAD – товарный знак или зарегистрированный в США и/или других странах товарный знак, принадлежащий Autodesk, Inc. и / или дочерним / аффилированным компаниям.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Borland – товарный знак или зарегистрированный товарный знак Borland Software Corporation.

Cisco, Cisco AnyConnect, IOS являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop и XenServer являются зарегистрированными товарными знаками или товарными знаками Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Core является товарным знаком Intel Corporation или ее дочерних компаний.

dBase – товарный знак dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC и другие товарные знаки являются товарными знаками компании Dell Inc или её дочерних компаний.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

ESET является товарным знаком или зарегистрированным товарным знаком ESET spol. s r.o. или соответствующей компании ESET.

Foxit – зарегистрированный товарный знак Foxit Corporation.

Radmin – зарегистрированный товарный знак Famatech.

Google, Android, Google Public DNS, Google Chrome, Chrome – товарные знаки Google LLC.

HUAWEI, FusionCompute и FusionSphere являются товарными знаками Huawei Technologies Co., Ltd.

ICQ – товарный знак и/или знак обслуживания ICQ LLC.

Intel является товарным знаком Intel Corporation или ее дочерних компаний.

IBM – товарный знак International Business Machines Corporation, зарегистрированный во многих юрисдикциях по всему миру.

Lenovo и Lenovo ThinkPad – товарные знаки Lenovo в США и/или других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Logitech является зарегистрированным товарным знаком или товарным знаком компании Logitech в США и (или) других странах.

LogMeIn Pro и Remotely Anywhere – товарные знаки компании LogMeIn, Inc.

Mail.ru – зарегистрированный товарный знак, правообладателем которого является ООО "Мэйл.Ру".

McAfee является товарным знаком или зарегистрированным товарным знаком McAfee LLC или ее дочерних компаний в США и других странах.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server и Windows Store являются товарными знаками группы компаний Microsoft.

Mozilla, Firefox и Thunderbird являются товарными знаками Mozilla Foundation в США и других странах.

NetApp – товарный знак или зарегистрированный в США и/или других странах товарный знак NetApp, Inc.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

OpenStack – зарегистрированный товарный знак OpenStack Foundation в США и других странах.

Oracle, Java и JavaScript – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Realtek – товарный знак Realtek Semiconductor Corporation.

SAMSUNG – товарный знак компании SAMSUNG в США или других странах.

Thawte – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

Trend Micro является товарным знаком или зарегистрированным товарным знаком Trend Micro Incorporated.

VERISIGN – зарегистрированный в США и других странах или незарегистрированный товарный знак VeriSign, Inc. и дочерних компаний.

VMware, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools, VMware vSphere – зарегистрированные товарные знаки и/или товарные знаки VMware, Inc. в США и других странах.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.