kaspersky

Kaspersky Endpoint Security для Windows 11.6.0

Содержание

Часто задаваемые вопросы

Что нового

Kaspersky Endpoint Security для Windows

- Комплект поставки
- Аппаратные и программные требования
- Сравнение функций программы в зависимости от типа операционной системы
- Сравнение функций программы в зависимости от инструментов управления
- Совместимость с другими программами

Установка и удаление программы

- Развертывание через Kaspersky Security Center 12
  - Стандартная установка программы
  - Создание инсталляционного пакета
  - Обновление баз в инсталляционном пакете
  - Создание задачи удаленной установки
- Локальная установка программы с помощью мастера
- Установка программы из командной строки
- Удаленная установка программы с помощью System Center Configuration Manager
- Описание параметров установки в файле setup.ini
- Изменение состава компонентов программы
- Обновление предыдущей версии программы
- Удаление программы
  - Удаление через Kaspersky Security Center
  - Удаление программы с помощью мастера
  - Удаление программы из командной строки

Лицензирование программы

- О Лицензионном соглашении
- О лицензии
- О лицензионном сертификате
- О подписке
- О лицензионном ключе
- О коде активации
- О файле ключа
- Активация программы
  - Активация программы через Kaspersky Security Center
  - Активация программы с помощью мастера активации программы
  - Активация программы с помощью командной строки
- Просмотр информации о лицензии
- Приобретение лицензии
- Продление подписки

Предоставление данных

- Предоставление данных в рамках Лицензионного соглашения
- Предоставление данных при использовании Kaspersky Security Network
- Соответствие законодательству Европейского союза (GDPR)

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 программы
Значок программы в области уведомлений
Упрощенный интерфейс программы
Настройка отображения интерфейса программы
Подготовка программы к работе
Управление политиками
Управление задачами
Настройка локальных параметров программы
Запуск и остановка Kaspersky Endpoint Security
Приостановка и возобновление защиты и контроля компьютера
Проверка компьютера
Запуск и остановка задачи проверки
Изменение уровня безопасности
Изменение действия над зараженными файлами
Формирование списка проверяемых объектов
Выбор типа проверяемых файлов
Оптимизация проверки файлов
Проверка составных файлов
Использование методов проверки
Использование технологий проверки
Выбор режима запуска для задачи проверки
Настройка запуска задачи проверки с правами другого пользователя
Проверка съемных дисков при подключении к компьютеру
Фоновая проверка
Проверка целостности программы
Обновление баз и модулей программы
Схемы обновления баз и модулей программы
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
Настройка обновления из папки общего доступа
Обновление модулей программы
Использование прокси-сервера при обновлении
Откат последнего обновления
Работа с активными угрозами
Защита компьютера
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
Защита от веб-угроз
Включение и выключение Защиты от веб-угроз
Изменение действия над вредоносными объектами веб-трафика
Проверка ссылок по базам фишинговых и вредоносных веб-адресов
Использование эвристического анализа в работе компонента Защита от веб-угроз
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
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 атак по типам
Сетевой экран
Включение и выключение Сетевого экрана
Изменение статуса 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
Работа с сетевыми правилами программ
Создание сетевого правила программы
Включение и выключение сетевого правила программ
Изменение действия Сетевого экрана для сетевого правила программ
Изменение приоритета сетевого правила программ
Мониторинг сети
Защита от атак BadUSB
Включение и выключение Защиты от атак BadUSB
Использовании экранной клавиатуры при авторизации USB-устройств
AMSI-защита
Включение и выключение AMSI-защиты
Проверка составных файлов AMSI-защитой
Защита от эксплойтов
Включение и выключение Защиты от эксплойтов

Выбор действия при обнаружении эксплойта
Защита памяти системных процессов
Анализ поведения
Включение и выключение Анализа поведения
Выбор действия при обнаружении вредоносной активности программы
Защита папок общего доступа от внешнего шифрования
Включение и выключение защиты папок общего доступа от внешнего шифрования
Выбор действия при обнаружении внешнего шифрования папок общего доступа
Создание исключения для защиты папок общего доступа от внешнего шифрования
Настройка адресов исключений из защиты папок общего доступа от внешнего шифрования
Экспорт и импорт списка исключений из защиты папок общего доступа от внешнего шифрования
Предотвращение вторжений
Включение и выключение Предотвращения вторжений
Работа с группами доверия программ
Изменение группы доверия для программы
Настройка прав группы доверия
Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security
Выбор группы доверия для неизвестных программ
Выбор группы доверия для программ с цифровой подписью
Работа с правами программ
Защита ресурсов ОС и персональных данных
Удаление информации о неиспользуемых программах
Мониторинг работы Предотвращения вторжений
Защита доступа к аудио и видео
Откат вредоносных действий
Kaspersky Security Network
Включение и выключение использования Kaspersky Security Network
Ограничения работы с Локальным KSN
Включение и выключение облачного режима для компонентов защиты
Проверка подключения к Kaspersky Security Network
Проверка репутации файла в Kaspersky Security Network
Проверка защищенных соединений
Настройка параметров проверки защищенных соединений
Проверка защищенных соединений в Firefox и Thunderbird
Исключение защищенных соединений из проверки
Контроль компьютера
Веб-Контроль
Включение и выключение Веб-Контроля
Действия с правилами доступа к веб-ресурсам
Добавление правила доступа к веб-ресурсам
Назначение приоритета правилам доступа к веб-ресурсам
Включение и выключение правила доступа к веб-ресурсам
Экспорт и импорт списка доверенных веб-адресов
Проверка работы правил доступа к веб-ресурсам
Экспорт и импорт списка адресов веб-ресурсов
Мониторинг активности пользователей в интернете
Изменение шаблонов сообщений Веб-Контроля
Правила формирования масок адресов веб-ресурсов

Миграция правил доступа к веб-ресурсам из предыдущих версий программы
Контроль устройств
Включение и выключение Контроля устройств
О правилах доступа
Изменение правила доступа к устройствам
Изменение правила доступа к шине подключения
Добавление сети Wi-Fi в список доверенных
Мониторинг использования съемных дисков
Изменение периода кеширования
Действия с доверенными устройствами
Добавление устройства в список доверенных из интерфейса программы
Добавление устройства в список доверенных из Kaspersky Security Center
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
Включение и выключение 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
Просмотр отчетов Адаптивного контроля аномалий
Контроль программ
Ограничения функциональности Контроля программ
Включение и выключение Контроля программ
Выбор режима Контроля программ
Действия с правилами Контроля программ в интерфейсе программы
Добавление правила Контроля программ
Добавление условия срабатывания в правило Контроля программ
Изменение статуса правила Контроля программ
Управление правилами Контроля программ в Kaspersky Security Center
Получение информации о программах, которые установлены на компьютерах пользователей
Создание категорий программ
Добавление в категорию программ исполняемых файлов из папки Исполняемые файлы
Добавление в категорию программ исполняемых файлов, связанных с событиями
Добавление и изменение правила Контроля программ с помощью Kaspersky Security Center
Изменение статуса правила Контроля программ с помощью Kaspersky Security Center
Экспорт и импорт правил Контроля программ
Тестирование правил Контроля программ с помощью Kaspersky Security Center
Просмотр событий по результатам тестовой работы компонента Контроля программ

Просмотр отчета о запрещенных программах в тестовом режиме
Просмотр событий по результатам работы компонента Контроль программ
Просмотр отчета о запрещенных программах
Тестирование правил Контроля программ
Мониторинг активности программ
Правила формирования масок имен файлов или папок
Изменение шаблонов сообщений Контроля программ
Лучшие практики по внедрению режима списка разрешенных программ
Настройка режима списка разрешенных программ
Тестирование режима списка разрешенных программ
Поддержка режима списка разрешенных программ
Контроль сетевых портов
Включение контроля всех сетевых портов
Формирование списка контролируемых сетевых портов
Формирование списка программ, для которых контролируются все сетевые порты
Экспорт и импорт списков контролируемых портов
Расширения защиты
Managed Detection and Response
Kaspersky Endpoint Agent
Удаление данных
Защита паролем
Включение Защиты паролем
Предоставление разрешений для отдельных пользователей или групп
Использование временного пароля для предоставления разрешений
Особенности разрешений Защиты паролем
Доверенная зона
Создание исключения из проверки
Запуск и остановка работы исключения из проверки
Формирование списка доверенных программ
Включение и выключение действия правил доверенной зоны на программу из списка доверенных программ
Использование доверенного системного хранилища сертификатов
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 программы в области уведомлений
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
Включение и выключение защиты от внешнего управления
Обеспечение работы программ удаленного администрирования
Производительность Kaspersky Endpoint Security и совместимость с другими программами
Выбор типов обнаруживаемых объектов
Включение и выключение технологии лечения активного заражения
Включение и выключение режима энергосбережения
Включение и выключение режима передачи ресурсов другим программам
Создание и использование конфигурационного файла
Восстановление параметров программы по умолчанию
Обмен сообщениями между пользователем и администратором
Шифрование данных
Ограничения функциональности шифрования
Смена длины ключа шифрования (AES56 / AES256)
Шифрование диска Kaspersky
Особенности шифрования SSD-дисков
Полнодисковое шифрование с помощью технологии Шифрование 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
Обновление операционной системы
Устранение ошибок при обновлении функциональности шифрования
Выбор уровня трассировки 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
Шифрование файлов на локальных дисках компьютера
Запуск шифрования файлов на локальных дисках компьютера
Формирование правил доступа программ к зашифрованным файлам
Шифрование файлов, создаваемых и изменяемых отдельными программами
Формирование правила расшифровки
Расшифровка файлов на локальных дисках компьютера
Создание зашифрованных архивов
Восстановление доступа к зашифрованными 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
Управление программой из командной строки
Команды
SCAN. Антивирусная проверка
UPDATE. Обновление баз и модулей программы
ROLLBACK. Откат последнего обновления
TRACES. Трассировка
START. Запуск профиля
STOP. Остановка профиля
STATUS. Статус профиля
STATISTICS. Статистика выполнения профиля
RESTORE. Восстановление файлов
EXPORT. Экспорт параметров программы
IMPORT. Импорт параметров программы
ADDKEY. Применение файла ключа
LICENSE. Лицензирование
RENEW. Покупка лицензии
PBATESTRESET. Сбросить результаты проверки перед шифрованием диска
EXIT. Завершение работы программы
EXITPOLICY. Выключение политики
STARTPOLICY. Включение политики
DISABLE. Выключение защиты
SPYWARE. Обнаружение шпионского ПО
MDRLICENSE. Активация MDR
KSN. Переключение Глобальный / Локальный KSN
Команды KESCLI
Scan. Антивирусная проверка
GetScanState. Статус выполнения проверки
GetLastScanTime. Определения времени выполнения проверки
GetThreats. Получение данных об обнаруженных угрозах
UpdateDefinitions. Обновление баз и модулей программы
GetDefinitionState. Определение времени выполнения обновления
EnableRTP. Включение защиты
GetRealTimeProtectionState. Статус Защиты от файловых угроз
Version. Определение версии программы
Коды ошибок
Приложение. Профили программы
Управление программой через REST API
Установка программы с REST API
Работа с API

Источники информации о программе
Обращение в Службу технической поддержки
О составе и хранении файлов трассировки
Трассировка работы программы
Трассировка производительности программы
Запись дампов
Защита файлов дампов и трассировок
Ограничения и предупреждения
Глоссарий
OLE-объект
Агент администрирования
Агент аутентификации
Активный ключ
Антивирусные базы
Архив
База вредоносных веб-адресов
База фишинговых веб-адресов
Группа администрирования
Доверенный платформенный модуль
Дополнительный ключ
Задача
Зараженный файл
Издатель сертификата
Лечение объектов
Лицензионный сертификат
Ложное срабатывание
Маска
Нормализованная форма адреса веб-ресурса
Область защиты
Область проверки
Портативный файловый менеджер
Потенциально заражаемый файл
Приложения
Приложение 1. Параметры программы
Защита от файловых угроз
Защита от веб-угроз
Защита от почтовых угроз
Защита от сетевых угроз
Сетевой экран
Защита от атак BadUSB
AMSI-защиты
Защита от эксплойтов
Анализ поведения
Предотвращение вторжений
Откат вредоносных действий
Kaspersky Security Network
Веб-Контроль
Контроль устройств

Контроль программ
Адаптивный контроль аномалий
Endpoint Sensor
Полнодисковое шифрование
Шифрование файлов
Шифрование съемных дисков
Шаблоны (шифрование данных)
Исключения
Настройки программы
Отчеты и хранилище
Настройки сети
Интерфейс
Управление настройками
Управление задачами
Проверка компьютера
Фоновая проверка
Проверка из контекстного меню
Проверка съемных дисков
Проверка целостности программы
Обновление баз и модулей программы
Приложение 2. Группы доверия программ
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 программы в журнале событий Windows
Информация о стороннем коде
Уведомления о товарных знаках

Часто задаваемые вопросы

ОБЩЕЕ

На каких компьютерах работает Kaspersky Endpoint Security?

Что изменилось с последней версии?

С какими другими программами "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 антивирусную проверку 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?

ПРОГРАММЫ

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

Как предотвратить запуск компьютерных игр?

Как проверить, что Контроль программ настроен верно?

Как добавить программу 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?

Что нового

Обновление 11.6.0

В Kaspersky Endpoint Security для Windows 11.6.0 появились следующие возможности и улучшения:

1. Поддержка операционной системы Windows 10 21H1. Особенности поддержки операционной системы Microsoft Windows 10 вы можете узнать в базе знаний Службы технической поддержки.

2. Добавлен компонент Managed Detection and Response. Компонент обеспечивает взаимодействие с решением Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* обеспечивает круглосуточную защиту от растущего количества угроз, способных обойти автоматические средства защиты, для организаций, которым сложно найти квалифицированных специалистов или у которых ограничены внутренние ресурсы. Подробную информацию о работе решения *см. в справке Kaspersky Managed Detection and Response*.

3. Программа Kaspersky Endpoint Agent, входящая в комплект поставки, обновлена до версии 3.10. В Kaspersky Endpoint Agent 3.10 добавили новые функции, исправили ошибки и повысили стабильность работы. Подробнее о работе программы см. в документации к решениям "Лаборатории Касперского", которые поддерживают Kaspersky Endpoint Agent.

4. Добавлена возможность управления защитой от атак типа Интенсивные сетевые запросы (англ. Network Flooding) и Сканирование портов в настройках компонента Защита от сетевых угроз.

5. Добавлен новый способ создания сетевых правил для работы Сетевого экрана. Вы можете добавлять пакетные правила и правила программ для соединений, которые отображаются в окне Мониторинга сети. При этом параметры соединения для сетевого правила будут настроены автоматически.

6. Улучшен интерфейс инструмента Мониторинга сети. Добавлена информация о сетевой активности: ID процессов, которые инициируют сетевую активность; тип сети (локальная сеть или интернет); локальные порты. Информация о типе сети по умолчанию скрыта.

7. Добавлена возможность автоматического создания учетных записей Агента аутентификации для новых пользователей Windows. Агент позволяет пользователю пройти аутентификацию для доступа к дискам, зашифрованным с помощью технологии Шифрование диска Kaspersky, и для загрузки операционной системы. Программа проверяет информацию об учетных записях Windows на компьютере. Если Kaspersky Endpoint Security обнаружит учетную запись Windows, для которой нет учетной записи Агента аутентификации, программа создаст новую учетную запись для доступа к зашифрованным дискам. Таким образом, вам не нужно вручную добавлять учетные записи Агента аутентификации для компьютеров с уже зашифрованными дисками.

8. Добавлена возможность контролировать процесс шифрования дисков в интерфейсе программы на компьютерах пользователей (Шифрование диска Kaspersky и BitLocker). Вы можете запустить инструмент Мониторинг шифрования из главного окна программы.

Обновление 11.5.0

В Kaspersky Endpoint Security для Windows 11.5.0 появились следующие возможности и улучшения:

1. Поддержка операционной системы Windows 10 20H2. Особенности поддержки операционной системы Microsoft Windows 10 вы можете узнать в базе знаний Службы технической поддержки.

2. Обновлен интерфейс программы. Также обновлен значок программы в области уведомлений, уведомления программы и диалоговые окна.

3. Улучшен интерфейс веб-плагина Kaspersky Endpoint Security для компонентов Контроль программ, Контроль устройств, Адаптивный контроль аномалий.

4. Добавлена функция импорта и экспорта списков правил и исключений в XML-формат. XML-формат позволяет редактировать списки после экспорта. Вы можете работать со списками только в консоли Kaspersky Security Center. Для экспорта / импорта доступны следующие списки:

   - Анализ поведения (список исключений).
   - Защита от веб-угроз (список доверенных веб-адресов).
   - Защита от почтовых угроз (список расширений фильтра вложений).
   - Защита от сетевых угроз (список исключений).
   - Сетевой экран (список сетевых пакетных правил).
   - Контроль программ (список правил).
   - Веб-Контроль (список правил).
   - Контроль сетевых портов (списки портов и программ, которые контролирует Kaspersky Endpoint Security).
   - Шифрование диска Kaspersky (список исключений).
   - Шифрование съемных дисков (список правил).

5. В отчет об обнаружении угроз добавлена информация о MD5 объекта. В предыдущих версиях программы Kaspersky Endpoint Security показывал только SHA256 объекта.

6. Добавлена возможность назначить приоритет для правил доступа к устройствам в параметрах Контроля устройств. Приоритет позволяет гибко настроить доступ пользователей к устройствам. Если пользователь добавлен в несколько групп, Kaspersky Endpoint Security регулирует доступ к устройству по записи правила с высшим приоритетом. 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 0, а группе "Все" приоритет 1. Вы можете настроить приоритет только для устройств с файловой системой. К устройствам с файловой системой относятся жесткие диски, съемные диски, дискеты, CD/DVD-приводы, портативные устройства (MTP).

7. Добавлены новые функции:

   - Управление звуковыми сигналами уведомлений.
   - Учет стоимости подключения. Kaspersky Endpoint Security ограничивает собственный сетевой трафик в том случае, если подключение к интернету является лимитным (например, мобильное подключение).
   - Управление параметрами Kaspersky Endpoint Security через доверенные программы удаленного администрирования (такие как TeamViewer, LogMeIn Pro и Remotely Anywhere). С помощью программ удаленного администрирования вы можете запустить Kaspersky Endpoint Security и управлять параметрами в интерфейсе программы.
   - Управление параметрами проверки защищенного трафика в программах Firefox и Thunderbird. Вы можете выбрать хранилище сертификатов, которое будут использовать программы Mozilla: хранилище сертификатов Windows или хранилище сертификатов Mozilla. Функция доступна только для компьютеров, к которым не применена политика. Если к компьютеру применена политика, Kaspersky

Endpoint Security автоматически включает использование хранилища сертификатов Windows в программах Firefox и Thunderbird.

8. Добавлена возможность настроить режим проверки защищенного трафика: проверять трафик всегда, даже если компоненты защиты выключены, или проверять трафик по запросу компонентов защиты.

9. Изменен порядок удаления информации из отчетов. Пользователь может удалить только все отчеты. В предыдущих версиях программы пользователь мог выбрать компоненты программы, информацию из отчетов которых нужно удалить.

10. Изменен порядок импорта конфигурационного файла с параметрами Kaspersky Endpoint Security, а также порядок восстановления параметров программы. Перед импортом или восстановлением Kaspersky Endpoint Security показывает только предупреждение. В предыдущих версиях программы был доступен просмотр значений новых параметров перед их применением.

11. Упрощена процедура восстановления доступа к диску, зашифрованному BitLocker. После прохождения процедуры восстановления доступа Kaspersky Endpoint Security предложит пользователю задать новый пароль или PIN-код. После установки нового пароля BitLocker зашифрует диск. В предыдущей версии программы пользователю нужно было сбрасывать пароль вручную в параметрах BitLocker.

12. Для пользователя добавлена 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 и доверенных программ. Администратор может разрешить или запретить использование локальных исключений или локальных доверенных программ. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера.

13. Добавлена возможность ввести комментарий в свойствах доверенных программ. Комментарий позволяет упростить поиск и сортировку доверенных программ.

14. Управление программой через REST API:

    - Добавлена возможность настроить параметры расширения компонента Защита от почтовых угроз для Outlook.

    - Запрещено выключать обнаружение объектов следующих типов: вирусы, черви, троянские программы.

Обновление 11.4.0

В Kaspersky Endpoint Security для Windows 11.4.0 появились следующие возможности и улучшения:

1. Обновлен дизайн значка программы в области уведомлений. Вместо значка теперь используется значок . Если от пользователя требуется выполнить действие (например, перезагрузить компьютер после обновления программы), значок изменится на . Если работа компонентов защиты программы выключена или нарушена, значок изменится на или . Если навести курсор на значок, Kaspersky Endpoint Security покажет описание проблемы в защите компьютера.

2. Программа Kaspersky Endpoint Agent, входящая в комплект поставки, обновлена до версии 3.9. Kaspersky Endpoint Agent 3.9 поддерживает интеграцию с новыми решениями "Лаборатории Касперского". Подробнее о работе программы см. в документации к решениям "Лаборатории Касперского", которые поддерживают Kaspersky Endpoint Agent.

3. Добавлен статус *Не поддерживается лицензией* для компонентов Kaspersky Endpoint Security. Вы можете просмотреть статус компонентов по кнопке **Компоненты защиты** в главном окне программы.

4. В отчеты добавлены новые события о работе компонента Защита от эксплойтов.

5. Драйверы для работы технологии Шифрование диска Kaspersky автоматически добавляются в среду восстановления Windows (англ. WinRE – Windows Recovery Environment) при запуске шифрования диска. В предыдущей версии программа добавляла драйверы при установке Kaspersky Endpoint Security. Добавление драйверов в WinRE позволяет повысить стабильность работы программы при восстановлении операционной системы на компьютерах, защищенных технологией Шифрование диска Kaspersky.

Компонент Endpoint Sensor исключен из программы Kaspersky Endpoint Security. Вы можете продолжать настраивать параметры Endpoint Sensor с помощью политики, если на компьютере установлена программа Kaspersky Endpoint Security версий 11.0.0 – 11.3.0.

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.

Для защиты компьютера Kaspersky Endpoint Security использует следующие 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".

- **Kaspersky 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.

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

К компонентам контроля относятся следующие компоненты программы:

- **Контроль программ**. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.

- **Контроль устройств**. Компонент позволяет установить гибкие ограничения доступа к устройствам, являющимся источниками информации (например, жесткие диски, съемные диски, CD/DVD-диски), инструментами передачи информации (например, модемы), инструментами преобразования информации (например, принтеры) или интерфейсами, с помощью которых устройства подключаются к компьютеру (например, USB, Bluetooth).

- **Веб-Контроль**. Компонент позволяет установить гибкие ограничения доступа к веб-ресурсам для разных групп пользователей.

- **Адаптивный контроль аномалий**. Компонент отслеживает и регулирует потенциально опасные действия, нехарактерные для защищаемого компьютера.

К компонентам защиты относятся следующие компоненты программы:

- **Анализ поведения**. Компонент получает данные о действиях программ на вашем компьютере и предоставляет эту информацию другим компонентам для более эффективной защиты.

- **Защита от эксплойтов**. Компонент отслеживает исполняемые файлы, запускаемые уязвимыми программами. Если попытка запустить исполняемый файл из уязвимой программы не была инициирована пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла.

- **Предотвращение вторжений**. Компонент регистрирует действия, совершаемые программами в операционной системе, и регулирует действия программ исходя из того, к какой группе компонент относит эту программу. Для каждой группы программ задан набор правил. Эти правила регламентируют доступ программ к персональным данным пользователя и ресурсам операционной системы. К таким данным относятся файлы пользователя в папке "Документы", файлы cookie, файлы с историей активности пользователя, а также файлы, папки и ключи реестра, содержащие параметры работы и важные данные наиболее часто используемых программ.

- **Откат вредоносных действий**. Компонент позволяет Kaspersky Endpoint Security отменить действия, произведенные вредоносными программами в операционной системе.

- **Защита от файловых угроз**. Компонент позволяет избежать заражения файловой системы компьютера. Компонент начинает работать сразу после запуска Kaspersky Endpoint Security, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на компьютере и на всех присоединенных запоминающих устройствах. Компонент перехватывает каждое обращение к файлу и проверяет этот файл на присутствие вирусов и других программ, представляющих угрозу.

- **Защита от веб-угроз**. Компонент проверяет трафик, поступающий на компьютер пользователя по протоколам HTTP и FTP, а также устанавливает принадлежность веб-адресов к вредоносным или фишинговым.

- **Защита от почтовых угроз**. Компонент проверяет входящие и исходящие сообщения электронной почты на наличие вирусов и других программ, представляющих угрозу.

- **Защита от сетевых угроз**. Компонент отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Endpoint Security блокирует сетевую активность атакующего компьютера.

- **Сетевой экран**. Компонент обеспечивает защиту данных, хранящихся на компьютере пользователя, блокируя большинство возможных для операционной системы угроз в то время, когда компьютер подключен к интернету или к локальной сети.

- **Защита от атак BadUSB**. Компонент позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру.

- **AMSI-защита**. Компонент проверяет объекты по запросу от сторонних приложений и сообщает результат проверки тому приложению, от которого был получен запрос.

В дополнение к постоянной защите, реализуемой компонентами программы, рекомендуется периодически выполнять *проверку компьютера* на присутствие вирусов и других программ, представляющих угрозу. Это нужно делать для того, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами, например, из-за установленного низкого уровня защиты.

Чтобы поддерживать защиту компьютера в актуальном состоянии, требуется *обновление баз и модулей программы*, используемых в работе программы. По умолчанию программа обновляется автоматически, но при необходимости вы можете вручную обновить базы и модули программы.

В программе Kaspersky Endpoint Security предусмотрены следующие задачи:

- **Проверка целостности**. Kaspersky Endpoint Security проверяет модули программы, находящиеся в папке установки программы, на наличие повреждений или изменений. Если модуль программы имеет некорректную цифровую подпись, то такой модуль считается поврежденным.

- **Полная проверка**. Kaspersky Endpoint Security выполняет проверку операционной системы, включая память ядра, загружаемые при запуске операционной системы объекты, загрузочные секторы, резервное хранилище операционной системы, а также все жесткие и съемные диски.

- **Выборочная проверка**. Kaspersky Endpoint Security проверяет объекты, выбранные пользователем.

- **Проверка важных областей**. Kaspersky Endpoint Security проверяет память ядра, загружаемые при запуске операционной системы объекты и загрузочные секторы.

- **Обновление**. Kaspersky Endpoint Security загружает обновленные базы и модули программы. Это обеспечивает актуальность защиты компьютера от вирусов и других программ, представляющих угрозу.

- **Откат последнего обновления**. Kaspersky Endpoint Security отменяет последнее обновление баз и модулей. Это позволяет вернуться к использованию предыдущих баз и модулей программы при необходимости, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасную программу.

Служебные функции программы

Kaspersky Endpoint Security включает ряд служебных функций. Служебные функции предусмотрены для поддержки программы в актуальном состоянии, для расширения возможностей использования программы, для оказания помощи в работе.

- **Отчеты**. В процессе работы программы для каждого компонента формируется отчет. Также в отчетах вы можете отслеживать результаты выполнения задач. Отчеты содержат списки событий, произошедших во время работы Kaspersky Endpoint Security, и всех выполненных программой операций. В случае возникновения проблем отчеты можно отправлять в "Лабораторию Касперского", чтобы специалисты Службы технической поддержки могли подробнее изучить ситуацию.

- **Хранилище данных**. Если в ходе проверки компьютера на вирусы и другие программы, представляющие угрозу, программа обнаруживает зараженные файлы, она блокирует эти файлы. Копии вылеченных и удаленных файлов Kaspersky Endpoint Security сохраняет в *резервном хранилище*. Файлы, которые не были обработаны по каким-либо причинам, Kaspersky Endpoint Security помещает в *список активных угроз*. Вы можете проверять файлы, восстанавливать файлы в папку их исходного размещения, а также очищать хранилище данных.

- **Служба уведомлений**. Служба уведомлений позволяет пользователю отслеживать события, влияющие на состояние защиты компьютера и работу Kaspersky Endpoint Security. Уведомления могут доставляться на экран или по электронной почте.

- **Kaspersky Security Network**. Участие пользователя в Kaspersky Security Network позволяет повысить эффективность защиты компьютера за счет оперативного использования информации о репутации файлов, веб-ресурсов и программного обеспечения, полученной от пользователей во всем мире.

- **Лицензия**. Приобретение лицензии обеспечивает полнофункциональную работу программы, доступ к обновлению баз и модулей программы, а также консультации по телефону и электронной почте по вопросам, связанным с установкой, настройкой и использованием программы.

- **Поддержка**. Все зарегистрированные пользователи Kaspersky Endpoint Security могут обращаться за помощью к специалистам Службы технической поддержки. Вы можете отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount или позвонить в Службу технической поддержки по телефону.

Если во время работы программы возникают ошибки или зависания, программа может быть автоматически перезапущена.

Если в работе программы возникают повторяющиеся ошибки, которые приводят к прекращению работы, программа 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 программы пытается восстановить работоспособность.

Комплект поставки

Комплект поставки содержит следующие дистрибутивы:

- **Strong encryption (AES256)**

  Дистрибутив содержит криптографические средства, реализующие криптографический алгоритм AES (Advanced Encryption Standard) с эффективной длиной ключа 256 бит.

- **Lite encryption (AES56)**

  Дистрибутив содержит криптографические средства, реализующие криптографический алгоритм AES с эффективной длиной ключа 56 бит.

Каждый дистрибутив содержит следующие файлы:

`kes_win.msi`	Пакет установки Kaspersky Endpoint Security.
`setup_kes.exe`	Файлы, необходимые для установки программы всеми доступными способами.
`kes_win.kud`	Файл для создания инсталляционного пакета Kaspersky Endpoint Security.
`klcfginst.msi`	Пакет установки плагина управления Kaspersky Endpoint Security для Kaspersky Security Center.
`bases.cab`	Файлы пакетов обновлений, которые используются при установке программы.
`cleaner.cab`	Файлы для удаления несовместимого программного обеспечения.
`incompatible.txt`	Файл со списком несовместимого программного обеспечения.
`ksn_<ID языка>.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.
`endpointagent.msi`	Пакет установки программы Kaspersky Endpoint Agent версии 3.10, необходимой для интеграции с другими решениями "Лаборатории Касперского" (например, Kaspersky Sandbox).
`NDP<версия>-<свойства пакета>`	Пакет установки Microsoft .NET Framework.
`keswin_web_plugin.zip`	Архив с файлами, необходимыми для установки веб-плагина Kaspersky

	Endpoint Security.

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

Аппаратные и программные требования

Для функционирования Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Минимальные общие требования:

- 2 ГБ свободного места на жестком диске;
- процессор:
  - рабочая станция – 1 ГГц;
  - сервер – 1.4 ГГц;
  - поддержка инструкций SSE2.
- оперативная память:
  - рабочая станция (x86) – 1 ГБ;
  - рабочая станция (x64) – 2 ГБ;
  - сервер – 2 ГБ.
- Microsoft .NET Framework 4.0 или выше.

Поддерживаемые операционные системы для рабочих станций:

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

Алгоритм подписи модулей SHA-1 больше не поддерживается Microsoft. Для успешной установки Kaspersky Endpoint Security на компьютер под управлением операционной системы Microsoft Windows 7 необходимо установить на компьютер обновление KB4474419. Подробнее об этом обновлении см. на сайте Службы технической поддержки Microsoft.

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

Поддерживаемые операционные системы для серверов:

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

  Microsoft 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 и выше;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

Алгоритм подписи модулей SHA-1 больше не поддерживается Microsoft. Для успешной установки Kaspersky Endpoint Security на компьютер под управлением операционной системы Microsoft Windows Server 2008 R2 необходимо установить на компьютер обновление KB4474419. Подробнее об этом обновлении см. на сайте Службы технической поддержки Microsoft.

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

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.

Поддерживаемые виртуальные платформы:

- VMWare Workstation 16 Pro;
- VMware ESXi 7.0 Update 1a;
- Microsoft Hyper-V Server 2019;
- Citrix Virtual Apps and Desktops 7;
- Citrix Provisioning 2009;
- Citrix Hypervisor 8.2 LTSR.

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

- Kaspersky Security Center 11;
- Kaspersky Security Center 12;
- Kaspersky Security Center 12 Patch A;
- Kaspersky Security Center 12 Patch B;
- Kaspersky Security Center 13;
- Kaspersky Security Center 13.1;
- Kaspersky Security Center 13.2.

Сравнение функций программы в зависимости от типа операционной системы

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

Сравнение функций Kaspersky Endpoint Security

Функция	Рабочая станция	Сервер
Продвинутая защита		
Kaspersky Security Network	✓	✓
Анализ поведения	✓	✓
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		
Контроль программ	✓	✓
Контроль устройств	✓	–
Веб-Контроль	✓	–

Адаптивный контроль аномалий	✓	–
Шифрование данных		
Шифрование диска Kaspersky	✓	–
Шифрование диска BitLocker	✓	✓
Шифрование файлов	✓	–
Шифрование съемных дисков	✓	–
Endpoint Agent	✓	✓
Managed Detection and Response	✓	✓

Сравнение функций программы в зависимости от инструментов управления

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

Вы можете управлять программой с помощью следующих консолей Kaspersky Security Center 12:

- 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, который имеет доступ к Серверу администрирования.

Вы также можете управлять программой 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 программой с помощью Kaspersky Security Center Cloud Console *см. в справке Kaspersky Security Center Cloud Console*.

Сравнение функций Kaspersky Endpoint Security

Функция	Kaspersky Security Center 12		Kaspersky Security Center
	Консоль администрирования	Web Console	Cloud Console
Продвинутая защита			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Анализ поведения	✓	✓	✓
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	✓	✓	✓
Managed Detection and Response	✓	✓	✓
AMSI-защита	✓	✓	✓
Контроль безопасности			
Контроль программ	✓	✓	✓
Контроль устройств	✓	✓	✓
Веб-Контроль	✓	✓	✓
Адаптивный контроль аномалий	✓	✓	✓
Шифрование данных			
Шифрование диска Kaspersky	✓	✓	–
Шифрование диска BitLocker	✓	✓	✓
Шифрование файлов	✓	✓	–
Шифрование съемных дисков	✓	✓	–
Endpoint Agent	✓	✓	✓
Задачи			
Добавление ключа	✓	✓	✓
Изменение состава компонентов программы	✓	✓	✓
Инвентаризация	✓	✓	✓
Обновление	✓	✓	✓
Откат обновления	✓	✓	✓
Поиск вирусов	✓	✓	✓
Проверка целостности	✓	✓	–
Удаление данных	✓	✓	✓
Управление учетными записями Агента аутентификации	✓	✓	–

Совместимость с другими программами

Kaspersky Endpoint Security проверяет компьютер на наличие программ "Лаборатории Касперского" перед установкой. Также программа проверяет компьютер на наличие несовместимого программного обеспечения. Список несовместимого ПО приведен в файле incompatible.txt в комплекте поставки.

ЗАГРУЗИТЬ ФАЙЛ INCOMPATIBLE.TXT

Программа Kaspersky Endpoint Security несовместима со следующими программами "Лаборатории Касперского":

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (в том числе компонент Endpoint Sensor).
- Kaspersky Sandbox (в том числе Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (в том числе компонент Endpoint Sensor).

  Если на компьютере установлен компонент Endpoint Agent с помощью инструментов развертывания других программ "Лаборатории Касперского", при установке Kaspersky Endpoint Security компонент будет удален автоматически. При этом Kaspersky Endpoint Security может включать в себя компонент Endpoint Sensor / Kaspersky Endpoint Agent, если в списке компонентов программы вы выбрали Endpoint Agent.

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

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

Установка и удаление программы

Программа Kaspersky Endpoint Security может быть установлена на компьютер следующими способами:

- локально с помощью мастера установки программы.
- локально из командной строки.
- удаленно с помощью Kaspersky Security Center 12.
- 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 программы 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.

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

Развертывание через Kaspersky Security Center 12

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. Kaspersky Security Center 12 поддерживает следующие основные способы развертывания:

- Установка программы 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 программы 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 12 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 12*.

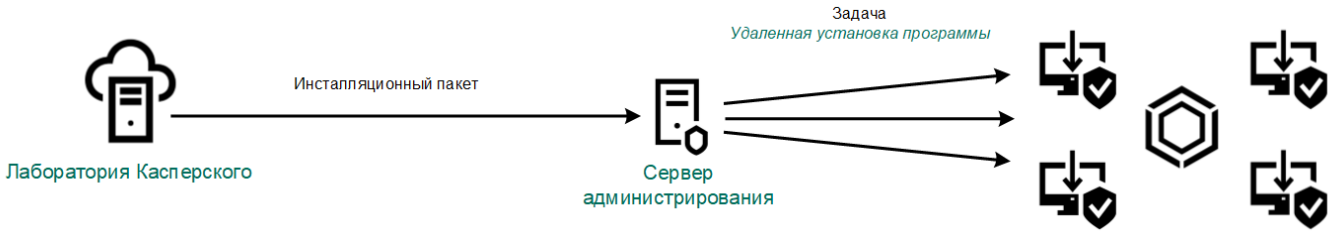
Стандартная установка программы

Для установки программы 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 программы "Лаборатории Касперского" при помощи Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы. 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 программы*.



Развертывание Kaspersky Endpoint Security

Как запустить мастер развертывания защиты в Консоли администрирования (MMC)

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

2. 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 программы, 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 устройств для установки

Выберите компьютеры, на которые будет установлена программа 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 3. Определение параметров задачи удаленной установки

Настройте следующие дополнительные параметры программы:

- **Принудительно загрузить инсталляционный пакет**. Выберите средства установки программы:

  - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала 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**. 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 одной и той же программы на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

- **Не устанавливать программу, если она уже установлена**. Снимите этот флажок, если вы хотите, например, установить программу 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 4. Выбор лицензионного ключа

Добавьте ключ в инсталляционный пакет для активации программы. 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 программу позднее с помощью задачи *Добавить ключ*.

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 программы. Также перезагрузка может потребоваться при обновлении версии программы.

Шаг 6. Удаление несовместимых программ перед установкой программы

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

Шаг 7. 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 8. Запуск установки

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

Как запустить мастер развертывания защиты в Web Console и Cloud 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 программ.

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

Шаг 2. Выбор лицензионного ключа

Добавьте ключ в инсталляционный пакет для активации программы. 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 программу позднее с помощью задачи *Добавить ключ*.

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 установлена программа 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 программы:

- **Принудительно загрузить инсталляционный пакет**. Выбор средства установки программы:
  - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала 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 программу 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 программы. Также перезагрузка может потребоваться при обновлении версии программы.

Шаг 7. Удаление несовместимых программ перед установкой программы

Ознакомьтесь со списком несовместимых программы и разрешите удаление этих программ. Если на компьютере установлены несовместимые программы, 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 программы "Лаборатории Касперского" при помощи Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы. 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 программы "Лаборатории Касперского"**.

Шаг 2. Определение имени инсталляционного пакета

Введите имя инсталляционного пакета, например, `Kaspersky Endpoint Security для Windows 11.6.0`.

Шаг 3. Выбор дистрибутива программы 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.

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 программы. Также в параметрах инсталляционного пакета вы можете выбрать компоненты программы и настроить параметры установки программы (см. таблицу ниже). 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 и Cloud 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.

Шаг 1. Выбор типа инсталляционного пакета

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

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

Также вы можете создать инсталляционный пакет из файла.

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.

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 программы. Также в параметрах инсталляционного пакета вы можете выбрать компоненты программы и настроить параметры установки программы (см. таблицу ниже). 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.

Параметры инсталляционного пакета

Раздел	Описание
Компоненты защиты	В этом разделе вы можете выбрать компоненты программы, которые будут доступны. Вы можете изменить состав компонентов программы позднее с помощью задачи *Изменение состава компонентов программы*. Компоненты Защита от атак BadUSB, Endpoint Agent и компоненты шифрования данных не устанавливаются по умолчанию. Эти компоненты можно добавить в параметрах инсталляционного пакета.
Настройки установки	**Добавить путь к программе в переменную окружения %PATH%**. Вы можете добавить путь установки в переменную %PATH% для удобства использования интерфейса командной строки. **Не защищать процесс установки программы**. Защита установки включает в себя защиту от подмены дистрибутива вредоносными программами, блокирование доступа к папке установки Kaspersky Endpoint Security и блокирование доступа к разделу системного реестра с ключами программы. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку программы (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.

Путь к папке для установки программы. Вы можете изменить путь установки Kaspersky Endpoint Security на клиентском компьютере. По умолчанию программа устанавливается в папку `%ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security for Windows`.

Конфигурационный файл. Вы можете загрузить файл, который задает параметры работы Kaspersky Endpoint Security. Вы можете создать конфигурационный файл в локальном интерфейсе программы.

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 12 Web Console. Обновлять базы в инсталляционном пакете в программе Kaspersky Security Center Cloud Console невозможно.

Как обновить антивирусные базы в инсталляционном пакете через Консоль 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. Откройте свойства инсталляционного пакета.

3. 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 закладке **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 программы*. Задача *Удаленная установка программы* позволяет развернуть инсталляционный пакет программы на все компьютеры организации. Перед развертыванием инсталляционного пакета вы можете обновить антивирусные базы внутри пакета, а также выбрать доступные компоненты программы в свойствах инсталляционного пакета.

Как создать задачу удаленной установки в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку **Сервер администрирования → Задачи**.

   Откроется список задач.

2. 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 программы**.

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 программы, 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 программы:

- **Принудительно загрузить инсталляционный пакет**. Выберите средства установки программы:
  - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала 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**. 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 одной и той же программы на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

- **Не устанавливать программу, если она уже установлена**. Снимите этот флажок, если вы хотите, например, установить программу 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 программы. Также перезагрузка может потребоваться при обновлении версии программы.

Шаг 6. Выбор устройств, которым будет назначено задача

Выберите компьютеры, на которые будет установлена программа 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 11.6.0`

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 программы будет выполнена в тихом режиме. После установки в области уведомлений компьютера пользователя будет добавлен значок  . Если значок имеет вид , убедитесь, что вы активировали программу.

Как создать задачу удаленной установки в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства** → **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 раскрывающимся списке **Программа** выберите **Kaspersky Security Center**.
2. В раскрывающемся списке **Тип задачи** выберите **Удаленная установка программы**.
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 установлена программа 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 (11.6.0).
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 загружать инсталляционный пакет** выберите средства установки программы:

   - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала 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 **Количество попыток установки** установите ограничение попыток установить программу. Если установка Kaspersky Endpoint Security завершается с ошибкой, задача автоматически запускает установку повторно.

6. Если требуется, снимите флажок **Не устанавливать программу, если она уже установлена**. Это позволит, например, установить программу более ранней версии.

7. Если требуется, снимите флажок **Предварительно проверять версию операционной системы**. Это позволит избежать загрузки дистрибутива программы, 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 программы**. Установка Kaspersky Endpoint Security требует ресурсов компьютера. Для удобства пользователя мастер установки программы предлагает закрыть работающие программы перед началом установки. Это позволит избежать замедление в работе других программ и возможных сбоев в работе компьютера.

10. В блоке **Поведение устройств, управляемых этим Сервером** 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 одной и той же программы 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 программы будет выполнена в тихом режиме. После установки в области уведомлений компьютера пользователя будет добавлен значок . Если значок имеет вид , убедитесь, что вы активировали программу.

Локальная установка программы с помощью мастера

Интерфейс мастера установки программы состоит из последовательности окон, соответствующих шагам установки программы.

Чтобы установить программу или обновить предыдущую версию программы с помощью мастера установки программы, выполните следующие действия

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

   Запустится мастер установки программы.

Подготовка к установке

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

- наличие несовместимого программного обеспечения (список несовместимого ПО приведен в файле incompatible.txt в комплекте поставки);
- выполнение аппаратных и программных требований;
- наличие прав на установку программного обеспечения.

Если какое-либо из перечисленных условий не выполнено, на экран выводится соответствующее уведомление.

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

Если в числе обнаруженных программ есть предыдущие версии Kaspersky Endpoint Security, то все данные, которые могут быть мигрированы (например, информация об активации, параметры программы), сохраняются и используются при установке Kaspersky Endpoint Security 11.6.0 для Windows, а предыдущая версия программы автоматически удаляется. Это относится к следующим версиям программы:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 для Windows (сборка 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 для Windows (сборка 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 для Windows (сборка 10.3.3.304).
- Kaspersky Endpoint Security для Windows 11.0.0 (сборка 11.0.0.6499).
- Kaspersky Endpoint Security для Windows 11.0.1 (сборка 11.0.1.90).

- Kaspersky Endpoint Security для Windows 11.0.1 SF1 (сборка 11.0.1.90).
- Kaspersky Endpoint Security для Windows 11.1.0 (сборка 11.1.0.15919).
- Kaspersky Endpoint Security для Windows 11.1.1 (сборка 11.1.1.126).
- Kaspersky Endpoint Security для Windows 11.2.0 (сборка 11.2.0.2254).
- Kaspersky Endpoint Security для Windows 11.2.0 CF1 (сборка 11.2.0.2254).
- Kaspersky Endpoint Security для Windows 11.3.0 (сборка 11.3.0.773).
- Kaspersky Endpoint Security для Windows 11.4.0 (сборка 11.4.0.233).
- Kaspersky Endpoint Security для Windows 11.5.0 (сборка 11.5.0.590).

Компоненты Kaspersky Endpoint Security

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

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

- Защита от атак BadUSB.
- Шифрование файлов.
- Полнодисковое шифрование.
- Управление BitLocker.
- Endpoint Agent. *Endpoint Agent* устанавливает программу Kaspersky Endpoint Agent 3.10 для взаимодействия между программой и решениями "Лаборатории Касперского" для обнаружения сложных угроз (например, Kaspersky Sandbox).

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

Дополнительные параметры

Защитить процесс установки программы. Защита установки включает в себя защиту от подмены дистрибутива вредоносными программами, блокирование доступа к папке установки Kaspersky Endpoint Security и блокирование доступа к разделу системного реестра с ключами программы. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку программы (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 программе в переменную окружения %PATH%. Вы можете добавить путь установки в переменную %PATH% для удобства использования интерфейса командной строки.

Установка программы из командной строки

Установку Kaspersky Endpoint Security из командной строки можно выполнить в одном из следующих режимов:

- В интерактивном режиме с помощью мастера установки программы.
- В тихом режиме. После запуска установки в тихом режиме ваше участие в процессе установки не требуется. Для установки программы в тихом режиме используйте ключи `/s` и `/qn`.

  Перед установкой программы 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 программы, 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.

Чтобы установить программу или обновить предыдущую версию программы, 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] [/pALLOWREBOOT=1]
   [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<имя пользователя>
   /pKLPASSWD=<пароль> /pKLPASSWDAREA=<область действия пароля>] [/pENABLETRACES=1|0
   /pTRACESLEVEL=<уровень трассировки>] [/s]
   ```

   или

   ```
   msiexec /i <название дистрибутива> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
   [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<имя пользователя> KLPASSWD=<пароль>
   KLPASSWDAREA=<область действия пароля>] [ENABLETRACES=1|0 TRACESLEVEL=<уровень
   трассировки>] [/qn]
   ```

`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 программы или обновления версии программы.
`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 программы или обновления версии программы.
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 программы. 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.
ALLOWREBOOT=1	Автоматическая перезагрузка компьютера после установки или обновления программы, 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 программы. Также перезагрузка может потребоваться при обновлении версии программы.
SKIPPRODUCTCHECK=1	Выключение проверки на наличие несовместимого ПО. Список несовместимого ПО приведен в файле incompatible.txt в комплекте поставки. Если параметр не задан, при обнаружении несовместимого ПО установка Kaspersky Endpoint Security будет прекращена.
SKIPPRODUCTUNINSTALL=1	Запрет на автоматическое удаление найденного несовместимого ПО. Если параметр не задан, Kaspersky Endpoint Security пытается удалить несовместимое ПО. Включить автоматическое удаление несовместимого ПО при установке Kaspersky Endpoint Security с помощью установщика msiexec невозможно. Для автоматического удаления несовместимого ПО используйте файл setup_kes.exe.
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 программы. • `EXIT` – завершение работы программы. • `DISPROTECT` – выключение компонентов защиты и остановка задач проверки. • `DISPOLICY` – выключение политики Kaspersky Security Center. • `UNINST` – удаление программы с компьютера. • `DISCTRL` – выключение компонентов контроля. • `REMOVELIC` – удаление ключа. • `REPORTS` – просмотр отчетов.
`ENABLETRACES`	Включение или выключение трассировки программы. После запуска Kaspersky Endpoint Security программа сохраняет файлы трассировки в папке %ProgramData%\Kaspersky Lab\KES\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 о всех ошибках, включая неустранимые. • `300` (диагностический). Сообщения о всех ошибках, а также предупреждения. • `400` (важный). Сообщения о всех ошибках, предупреждения, а также дополнительная информация. • `500` (обычный). Сообщения о всех ошибках, предупреждениях, а также подробная информация о работе программы в нормальном режиме (значение по умолчанию). • `600` (низкий). Все сообщения.
`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.
`RESTAPI`	Управление программой через REST API. Для управления программой 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 программой через REST API должно быть разрешено управление с помощью систем администрирования. Для этого задайте параметр `AdminKitConnector=1`. Если вы управляете программой через REST API, управлять программой с помощью систем администрирования "Лаборатории Касперского" невозможно.
`RESTAPI_User`	Имя пользователя доменной учетной записи Windows для управления программой через REST API. Управление программой 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 программой через REST API.
`RESTAPI_Port`	Порт для управления программой через REST API. По умолчанию используется порт 6782.
`ADMINKITCONNECTOR`	Управление программой 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 программой с помощью систем администрирования разрешено (значение по умолчанию). • `0` – разрешено управление программой только через локальный интерфейс.

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 программы 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 программы, вам нужно активировать программу по коммерческой лицензии с помощью мастера активации программы или специальной команды.

Во время установки программы или обновления версии программы в тихом режиме поддерживается использование следующих файлов:

- setup.ini – общие параметры установки программы;
- install.cfg – параметры работы Kaspersky Endpoint Security;
- 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 файлов setup.ini, install.cfg и setup.reg, разместите эти файлы 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 программы: `SETUPREG=<путь к файлу setup.reg>`.

Удаленная установка программы с помощью System Center Configuration Manager

Инструкция актуальна для версии System Center Configuration Manager 2012 R2.

Чтобы удаленно установить программу 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 программ*.
4. В мастере создания пакетов и программ 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 программы с указанием версии).
- В поле **Командная строка** укажите параметры установки Kaspersky Endpoint Security из командной строки.
- По кнопке **Обзор** задайте путь к исполняемому файлу программы.
- 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 была запущена другая программа.

  Выберите программу из раскрывающегося списка **Программа** или укажите путь к исполняемому файлу этой программы по кнопке **Обзор**.

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

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

Этот шаг является необязательным.

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 должна быть установлена программа, 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 программы 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.

ЗАГРУЗИТЬ ФАЙЛ SETUP.INI

Файл setup.ini состоит из следующих разделов:

- `[Setup]` – общие параметры установки программы.
- `[Components]` – выбор компонентов программы для установки. 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. Также в блоке отсутствует компонент Managed Detection and Response. Для установки компонента необходимо активировать Managed Detection and Response в консоли Kaspersky Security Center.
- `[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`.

Вместо значения `0` могут использоваться значения `no`, `off`, `disable`, `disabled`.

Параметры файла setup.ini

Раздел	Параметр	Описание
`[Setup]`	`InstallDir`	Путь к папке установки программы.
	`ActivationCode`	Код активации Kaspersky Endpoint Security.
	`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 программы или обновления версии программы.
	`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 программы или обновления версии программы.
	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 программы. 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.
	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.
	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 программы. • EXIT – завершение работы программы. • DISPROTECT – выключение компонентов защиты и остановка задач проверки. • DISPOLICY – выключение политики Kaspersky Security Center. • UNINST – удаление программы с компьютера.

		• `DISCTRL` – выключение компонентов контроля. • `REMOVELIC` – удаление ключа. • `REPORTS` – просмотр отчетов.
	`SelfProtection`	Включение или выключение механизма защиты установки программы. Возможные значения: • `1` – механизм защиты установки программы включен (значение по умолчанию). • `0` – механизм защиты установки программы выключен. Защита установки включает в себя защиту от подмены дистрибутива вредоносными программами, блокирование доступа к папке установки Kaspersky Endpoint Security и блокирование доступа к разделу системного реестра с ключами программы. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку программы (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop).
	`Reboot=1`	Автоматическая перезагрузка компьютера после установки или обновления программы, 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 программы. Также перезагрузка может потребоваться при обновлении версии программы.
	`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.
	`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.
	`SetupReg`	Включение записи ключей реестра из файла setup.reg в реестр. Значение параметра `SetupReg: setup.reg`.
	`EnableTraces`	Включение или выключение трассировки программы. После запуска Kaspersky Endpoint Security программа сохраняет файлы трассировки в папке %ProgramData%\Kaspersky Lab\KES\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 о всех ошибках, включая неустранимые. • `300` (диагностический). Сообщения о всех ошибках, а также предупреждения. • `400` (важный). Сообщения о всех ошибках, предупреждения, а также дополнительная информация. • `500` (обычный). Сообщения о всех ошибках, предупреждениях, а также подробная информация о работе программы в нормальном режиме (значение по умолчанию). • `600` (низкий). Все сообщения.
	`RESTAPI`	Управление программой через REST API. Для управления программой 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 программой через REST API должно быть разрешено управление с помощью систем администрирования. Для этого задайте параметр `AdminKitConnector=1`. Если вы управляете программой через REST API, управлять программой с помощью систем администрирования "Лаборатории Касперского" невозможно.
	`RESTAPI_User`	Имя пользователя доменной учетной записи Windows для управления программой через REST API. Управление программой 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 программой через REST API.
	`RESTAPI_Port`	Порт для управления программой через REST API. По умолчанию используется порт 6782.
`[Components]`	`ALL`	Установка всех компонентов. Если указано значение параметра `1`, все компоненты будут установлены независимо от параметров установки отдельных компонентов.
	`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 программ.
	`AdaptiveAnomaliesControl`	Адаптивный контроль аномалий.
	`FileEncryption`	Библиотеки для шифрования файлов.
	`DiskEncryption`	Библиотеки для полнодискового шифрования.
	`BadUSBAttackPrevention`	Защита от атак BadUSB.
	`AntiAPT`	Endpoint Agent. *Endpoint Agent* устанавливает

		программу Kaspersky Endpoint Agent 3.10 для взаимодействия между программой и решениями "Лаборатории Касперского" для обнаружения сложных угроз (например, Kaspersky Sandbox).
	`AdminKitConnector`	Управление программой 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 программой с помощью систем администрирования разрешено (значение по умолчанию). • `0` – разрешено управление программой только через локальный интерфейс.
`[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.
	`Updater`	Задача обновления. Возможные значения: • `1` – задача включается в список задач Kaspersky Endpoint Security. • `0` – задача не включается в список задач Kaspersky Endpoint Security.

Изменение состава компонентов программы

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

- Локально с помощью мастера установки программы.

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

- Удаленно с помощью Kaspersky Security Center.

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

Изменение состава программы 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.

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

1. В Консоли администрирования перейдите в папку **Сервер администрирования → 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 (11.6.0) → Изменение состава компонентов программы**.

Шаг 2. Параметры задачи изменения компонентов программы

Выберите компоненты программы, которые будут доступны на компьютере пользователя.

Установите флажок **Удалять несовместимые программы сторонних производителей**. Список несовместимых программ можно просмотреть в `incompatible.txt`, который входит в комплект поставки. Если на компьютере установлены несовместимые программы, установка Kaspersky Endpoint Security завершается с ошибкой.

Если требуется, включите защиту паролем на выполнение задачи:

1. Нажмите на кнопку **Дополнительно**.
2. Установите флажок **Использовать пароль для изменения состава компонентов**.
3. Введите учетные данные пользователя KLAdmin.

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, `Добавление компонента Контроль программ`.

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 изменен состав компонентов Kaspersky Endpoint Security в тихом режиме. В локальном интерфейсе программы будут отображаться параметры доступных компонентов. Компоненты, которые не вошли в состав программы, выключены, а параметры этих компонентов недоступны.

[Как добавить или удалить компоненты программы в Web Console и Cloud Console](#)

1. В главном окне Web Console выберите **Устройства** → **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 **Программа** выберите **Kaspersky Endpoint Security для Windows (11.6.0)**.
2. В раскрывающемся списке **Тип задачи** выберите **Изменение состава компонентов программы**.
3. В поле **Название задачи** введите короткое описание, например, `Добавление компонента Контроль программ`.
4. В блоке **Выбор устройств, 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 закладку **Параметры программы** и выберите компоненты программы, которые будут доступны.

Если требуется, включите защиту паролем на выполнение задачи:

1. В блоке **Дополнительные параметры** установите флажок **Использовать пароль для изменения состава компонентов**.
2. Введите учетные данные пользователя KLAdmin.

Сохраните внесенные изменения и запустите задачу.

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

Обновление предыдущей версии программы

Обновление предыдущей версии программы имеет следующие особенности:

- Kaspersky Endpoint Security 11.6.0 совместим с Kaspersky Security Center версии 12.
- Перед началом обновления программы рекомендуется закрыть все работающие программы.
- Если на компьютере установлены жесткие диски, к которым применено полнодисковое шифрование (FDE), для обновления Kaspersky Endpoint Security с версии 10 до версии 11.0.0 и более поздней нужно расшифровать все зашифрованные жесткие диски.

  Перед обновлением Kaspersky Endpoint Security блокирует функциональность полнодискового шифрования. Если функциональность полнодискового шифрования не удалось заблокировать, установка обновления не начнется. После обновления программы функциональность полнодискового шифрования будет восстановлена.

Kaspersky Endpoint Security поддерживает обновление следующих версий программы:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 для Windows (сборка 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 для Windows (сборка 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 для Windows (сборка 10.3.3.304).
- Kaspersky Endpoint Security для Windows 11.0.0 (сборка 11.0.0.6499).
- Kaspersky Endpoint Security для Windows 11.0.1 (сборка 11.0.1.90).
- Kaspersky Endpoint Security для Windows 11.0.1 SF1 (сборка 11.0.1.90).
- Kaspersky Endpoint Security для Windows 11.1.0 (сборка 11.1.0.15919).
- Kaspersky Endpoint Security для Windows 11.1.1 (сборка 11.1.1.126).
- Kaspersky Endpoint Security для Windows 11.2.0 (сборка 11.2.0.2254).
- Kaspersky Endpoint Security для Windows 11.2.0 CF1 (сборка 11.2.0.2254).
- Kaspersky Endpoint Security для Windows 11.3.0 (сборка 11.3.0.773).
- Kaspersky Endpoint Security для Windows 11.4.0 (сборка 11.4.0.233).
- Kaspersky Endpoint Security для Windows 11.5.0 (сборка 11.5.0.590).

При обновлении Kaspersky Endpoint Security 10 Service Pack 2 для Windows до Kaspersky Endpoint Security для Windows 11.6.0 в резервное хранилище новой версии программы переносятся файлы, помещенные в резервное хранилище и на карантин в предыдущей версии программы. Для более ранних версий Kaspersky Endpoint Security, чем Kaspersky Endpoint Security 10 Service Pack 2 для Windows, перенос файлов, помещенных в резервное хранилище и на карантин в предыдущей версии программы, не осуществляется.

Программа Kaspersky Endpoint Security может быть обновлена на компьютере следующими способами:

- локально с помощью мастера установки программы.
- локально из командной строки.
- удаленно с помощью Kaspersky Security Center 12.
- 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 развернута программа с набором компонентов, отличным от набора по умолчанию, обновление программы через Консоль администрирования (MMC) отличается от обновления программы через Web Console и Cloud Console. Обновление Kaspersky Endpoint Security имеет следующие особенности:

- Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console.

  Если вы создали инсталляционный пакет новой версии программы 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 программы после обновления будет соответствовать набору компонентов в инсталляционном пакете. То есть если новая версия программы имеет набор компонентов по умолчанию, то, например, компонент Защита от атак BadUSB будет удален с компьютера, так как этот компонент исключен из набора по умолчанию. Для продолжения использования программы с прежним набором компонентов нужно выбрать необходимые компоненты в параметрах инсталляционного пакета.

Удаление программы

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

Программа Kaspersky Endpoint Security может быть удалена с компьютера следующими способами:

- локально с помощью мастера установки программы;
- локально из командной строки;
- удаленно с помощью Kaspersky Security Center (подробнее см. в *справке Kaspersky Security Center*);
- удаленно через редактор управления групповыми политиками Microsoft Windows (подробнее см. на *сайте Службы технической поддержки Microsoft*).

Если при установке программы вы выбрали компонент Endpoint Agent, на компьютер будут установлены две программы: Kaspersky Endpoint Security и Kaspersky Endpoint Agent. После удаления Kaspersky Endpoint Security, программа Kaspersky Endpoint Agent также будет удалена автоматически.

Удаление через Kaspersky Security Center

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

Как удалить программу через Консоль администрирования (MMC)

1. В Консоли администрирования перейдите в папку **Сервер администрирования → Задачи**.

   Откроется список задач.

2. 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 программы**.

Шаг 2. Выбор удаляемой программы

Выберите **Удалить программу, поддерживаемую Kaspersky Security Center**.

Шаг 3. Параметры задачи удаления программы

Выберите **Kaspersky Endpoint Security для Windows (11.6.0)**.

Шаг 4. Параметры утилиты деинсталляции

Настройте следующие дополнительные параметры программы:

- **Принудительно загрузить 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 Microsoft Windows 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 распределения**. 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 точках распространения *см. в справке Kaspersky Security Center*.
- **Предварительно проверять версию операционной системы**. 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 программы 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 программы 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 11.6.0`.

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 программы будет выполнено в тихом режиме.

[Как удалить программу через Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **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 раскрывающимся списке **Программа** выберите **Kaspersky Security Center**.
2. В раскрывающемся списке **Тип задачи** выберите **Удаленная деинсталляция программы**.
3. В поле **Название задачи** введите короткое описание, например, `Удаление Kaspersky Endpoint Security на компьютерах Службы технической поддержки`.
4. В блоке **Выбор устройств, 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 программы

На этом шаге настройте параметры удаления программы:

1. Выберите тип **Удалить управляемую программу**.
2. Выберите программу **Kaspersky Endpoint Security для Windows (11.6.0)**.
3. **Принудительно загрузить 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 Microsoft Windows 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 распределения**. 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 точках 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 программы. Ограничение запросов позволит избежать перегрузки сети.

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

6. Если требуется, снимите флажок **Предварительно проверять версию операционной системы**. 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 программы будет выполнено в тихом режиме. После завершения удаления Kaspersky Endpoint Security покажет запрос на перезагрузку компьютера.

Если операция удаления программы 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 **Устройства** → **Задачи**.

   Откроется список задач.

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

   Откроется окно свойств задачи.

3. Выберите закладку **Параметры программы**.

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

5. Введите пароль учетной записи KLAdmin.

6. Нажмите на кнопку **Сохранить**.

Удаление программы с помощью мастера

Удаление Kaspersky Endpoint Security выполняется обычным способом, принятым для операционной системы Windows, через Панель управления. Запустится мастер установки программы. Следуйте указаниям на экране.

Вы можете указать, какие используемые программой данные вы хотите сохранить для дальнейшего использования при повторной установке программы (например, ее более новой версии). Если вы не укажете никаких данных, программа будет удалена полностью.

Вы можете сохранить следующие данные:

- **Информация об активации** – данные, позволяющие в дальнейшем не активировать программу повторно. Kaspersky Endpoint Security автоматически добавляет лицензионный ключ, если срок действия лицензии не истек к моменту установки.
- **Файлы резервного хранилища** – файлы, проверенные программой и помещенные в резервное хранилище.

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

  Если вы планируете использовать объекты резервного хранилища после удаления программы, вам нужно восстановить их до удаления программы. Однако эксперты "Лаборатории Касперского" не рекомендуют восстанавливать объекты из резервного хранилища, так как это может нанести вред компьютеру.
- **Настройки работы программы** – значения параметров работы программы, установленные в процессе ее настройки.
- **Локальное хранилище ключей шифрования** – данные, которые обеспечивают доступ к зашифрованным до удаления программы 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.

Удаление программы из командной строки

Удаление Kaspersky Endpoint Security из командной строки можно выполнить в одном из следующих режимов:

- В интерактивном режиме с помощью мастера установки программы.
- В тихом режиме. После запуска удаления в тихом режиме ваше участие в процессе удаления не требуется. Для удаления программы в тихом режиме используйте ключи `/s` и `/qn`.

Чтобы удалить программу 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 программы. Вы можете узнать GUID программы с помощью команды:

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

- Если операция удаления защищена паролем:

  ```
  setup_kes.exe /pKLLOGIN=<имя пользователя> /pKLPASSWD=<пароль> /s /x
  ```

  или

  ```
  msiexec.exe /x <GUID> KLLOGIN=<имя пользователя> KLPASSWD=<пароль> /qn
  ```

Пример:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin
KLPASSWD=!Password1 /qn
```

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

О Лицензионном соглашении

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

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

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 программы, а также находится в папке установки программы `%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows\Doc\<локаль>\KES`.

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

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.

- *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:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу 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 программы 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 программы 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 программы по подписке. 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 программу в соответствии с условиями Лицензионного соглашения.

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

Вы можете добавить лицензионный ключ в программу 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 программы вам нужно добавить другой ключ.

Ключ может быть активным и резервным.

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

Резервный ключ – ключ, подтверждающий право на использование программы, 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 программы, определенная лицензией, по которой программа активирована. Программа уведомляет пользователя о том, что ключ помещен в список запрещенных ключей. По истечении восьми дней функциональность программы соответствует ситуации, когда истекает срок действия лицензии. Вы можете использовать компоненты защиты и контроля и выполнять проверку на основе баз программы, установленных до истечения срока действия лицензии. Кроме того, программа 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 программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

При активации программы 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 программы, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Если код активации был потерян после активации программы, 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 программу.

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 программу 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.

При активации программы 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.

Активация программы

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

Вы можете активировать программу одним из следующих способов:

- Локально из интерфейса программы с помощью мастера активации программы. Этим способом вы можете добавить и активный, и резервный ключ.
- Удаленно с помощью программного комплекса Kaspersky Security Center путем создания и последующего запуска задачи добавления лицензионного ключа. Этим способом вы можете добавить и активный, и резервный ключ.
- Удаленно путем распространения на клиентские компьютеры файлов ключей и кодов активации, размещенных в хранилище ключей на Сервере администрирования Kaspersky Security Center. Подробнее о распространении ключей *см. в справке Kaspersky Security Center*. Этим способом вы можете добавить и активный, и резервный ключ.

  > Код активации, приобретенный по подписке, распространяется в первую очередь.

- С помощью командной строки.

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

Активация программы через Kaspersky Security Center

Вы можете активировать программу дистанционно через Kaspersky Security Center следующими способами:

- С помощью задачи *Добавить ключ*.

  Этот способ позволяет добавить ключ на конкретный компьютер или компьютеры, входящие в группу администрирования.

- 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*.

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 течении 30 дней. Все управляемые программы 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.

Вы можете контролировать использование лицензий следующими способами:

- Просмотреть *Отчет об использовании ключей* в инфраструктуре организации (**Мониторинг и отчеты** → **Отчеты**).

- Просмотреть статусы компьютеров на закладке **Устройства** → **Управляемые устройства**. Если программа не активирована, то у компьютера будет статус ⚠ и описание статуса **Программа не активирована**.

- Просмотреть информацию о лицензии в свойствах компьютера.

- Просмотреть свойства ключа (**Операции** → **Лицензирование**).

Как активировать программу в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку **Сервер администрирования → 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 (11.6.0) → 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 активирована программа Kaspersky Endpoint Security в тихом режиме.

[Как активировать программу в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **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 **Программа** выберите **Kaspersky Endpoint Security для Windows (11.6.0)**.
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 **Выбор устройств, которым будет назначена задача** выберите область действия задачи. Нажмите на кнопку **Далее**.

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 программу. Нажмите на кнопку **Далее**.

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 активирована программа Kaspersky Endpoint Security в тихом режиме.

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

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

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

   Откроется список лицензионных ключей.

2. Откройте свойства лицензионного ключа.

3. В разделе **Общие** установите флажок **Автоматически распространяемый лицензионный ключ**.

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 и Cloud Console

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

   Откроется список лицензионных ключей.

2. Откройте свойства лицензионного ключа.

3. На закладке **Общие** включите переключатель **Распространять ключ автоматически**.

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 закладке **Устройства**.

Активация программы с помощью мастера активации программы

Чтобы активировать Kaspersky Endpoint Security с помощью мастера активации программы, выполните следующие действия:

1. Нажмите на кнопку **Лицензия**, расположенную в нижней части главного окна программы.

2. В открывшемся окне нажмите на кнопку **Активировать программу по новой лицензии**.

Запустится мастер активации программы. Следуйте указаниям мастера активации программы.

Активация программы с помощью командной строки

Чтобы активировать программу с помощью командной строки,

введите в командной строке:

```
avp.com license /add <код активации или файл ключа> [/login=<имя пользователя>
/password=<пароль>]
```

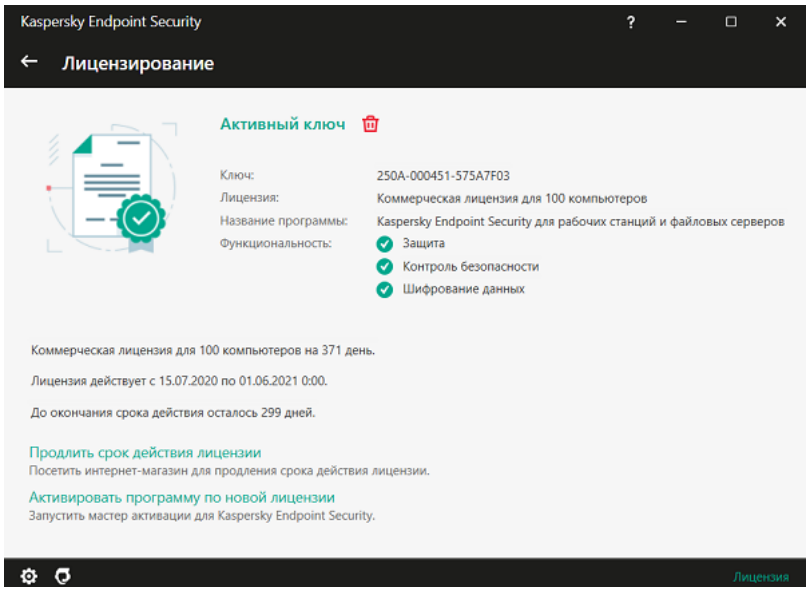
Учетные данные пользователя (`/login=<имя пользователя> /password=<пароль>`) нужно ввести, если включена Защита паролем.

Просмотр информации о лицензии

Чтобы просмотреть информацию о лицензии,

внизу главного окна программы нажмите на кнопку **Лицензия**.

Откроется окно **Лицензирование**, в котором представлена информация о лицензии (см. рис. ниже).



Окно Лицензирование

В окне **Лицензирование** представлена следующая информация:

- **Статус ключа**. На компьютере может быть несколько ключей. Ключ может быть активным и резервным. В программе 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 .
- **Ключ**. *Ключ* – это уникальная буквенно-цифровая последовательность, которая формируется из кода активации или файла ключа.

- **Лицензии**. Предусмотрены следующие типы лицензий: пробная и коммерческая.
- **Название программы**. Полное название приобретенной программы "Лаборатории Касперского".
- **Функциональность**. Функции программы, 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**. Тип лицензии, количество компьютеров, на которые распространяется лицензия, дата начала и дата и время окончания срока действия лицензии (только для активного ключа).

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

Также в окне лицензирования доступны следующие действия:

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

Приобретение лицензии

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

Чтобы приобрести лицензию, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Лицензия**.
2. В окне **Лицензирование** выполните одно из следующих действий:
   - Нажмите на кнопку **Приобрести 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 программы по подписке Kaspersky Endpoint Security автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки.

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

Если вы используете программу 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 программы, – программа работает без обновлений и Kaspersky Security Network недоступен.

Вы можете продлить подписку на веб-сайте поставщика услуг.

Вы можете обновить статус подписки вручную в окне **Лицензирование**. Это может потребоваться, если подписка продлена после истечения льготного периода, и программа автоматически не обновляет статус подписки.

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

1. В главном окне программы нажмите на кнопку **Лицензия**.

2. В окне **Лицензирование** нажмите на кнопку **Связаться с поставщиком подписки**.

Предоставление данных в рамках Лицензионного соглашения

Если для активации Kaspersky Endpoint Security применяется код активации, с целью проверки правомерности использования программы 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 программа Kaspersky Endpoint Security установлена в виртуальной среде;
- 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 программы;
- 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 программы 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 программы.

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, программа 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**, программа 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 программах и их модулях: данные о запущенных процессах в системе (идентификатор процесса в системе (PID), имя процесса, данные об учетной записи, от которой запущен процесс, программе и команде, запустившей процесс, а также признак доверенности программы 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 вредоносной программы: 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 вредоносной программой, 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 кэша, 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 кэша, 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.

Соответствие законодательству Европейского союза (GDPR)

Kaspersky Endpoint Security может передавать данные в "Лабораторию Касперского" при выполнении следующих условий:

- Использование Kaspersky Security Network.
- Активация программы с помощью кода активации.
- Обновление антивирусных баз и модулей программы.
- Переход по ссылкам в интерфейсе программы.
- Запись дампов.

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 программы 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 программы 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 программы.

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 Локальный KSN или выключите использование KSN. Подробнее о работе Локального KSN см. в *документации для Kaspersky Private Security Network*.

Активация программы 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 программы

Используя для обновления серверы "Лаборатории Касперского", вы соглашаетесь на автоматическую передачу данных, перечисленных в Лицензионном соглашении. Информация требуется для проверки правомерности использования программы 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 программы

Используя ссылки в интерфейсе программы, 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 программы и какую проблему она призвана решить. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", используйте упрощенный интерфейс программы или скройте интерфейс программы.

Запись дампов

Если вы включили запись дампов, Kaspersky Endpoint Security создаст файл дампа, который будет содержать всю информацию о рабочей памяти процессов программы на момент создания этого файла.

Начало работы

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

- Локальный интерфейс программы.
- Консоль администрирования Kaspersky Security Center.
- Kaspersky Security Center 12 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 программы, изменять состав компонентов программы, добавлять ключи, запускать и останавливать задачи обновления и проверки.

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

Подробнее об управлении программой через Kaspersky Security Center *см. в справке Kaspersky Security Center*.

Kaspersky Security Center 12 Web Console и Kaspersky Security Center Cloud Console

Kaspersky Security Center 12 Web Console (далее также "*Web Console*") представляет собой программу (веб-приложение), предназначенную для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Web Console является компонентом Kaspersky Security Center, предоставляющим пользовательский интерфейс. Подробную информацию о Kaspersky Security Center 12 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 программы "Лаборатории Касперского" на устройства вашей сети;
- управлять установленными программами;
- просматривать отчеты о состоянии системы безопасности.

Управление программой 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 программы. Для взаимодействия с Kaspersky Security Center 12 Web Console предназначен веб-плагин.

Версия плагина управления может отличаться от версии программы 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 12 Web Console. В отличие от плагина управления для Консоли администрирования Kaspersky Security Center, который устанавливается на рабочее место администратора, веб-плагин требуется установить на компьютер с установленной программой Kaspersky Security Center 12 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** → **Плагины**). Подробнее о совместимости версий веб-плагинов и Web Console см. в *справке Kaspersky Security Center*.

Установка веб-плагина

Вы можете установить веб-плагин следующими способами:

- Установить веб-плагин с помощью мастера первоначальной настройки Kaspersky Security Center 12 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 12 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** → **Плагины**). Список доступных дистрибутивов обновляется автоматически после выпуска новых версий программ "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** → **Плагины**). Дистрибутив веб-плагина вы можете загрузить, например, на веб-сайте "Лаборатории Касперского".

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** → **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** → **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** → **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 программой 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.

Обновление плагина управления Kaspersky Endpoint Security 10 для Windows

Если в Консоли администрирования установлен плагин управления Kaspersky Endpoint Security 10 для Windows, то установка плагина управления Kaspersky Endpoint Security 11 для Windows имеет следующие особенности:

- Плагин управления Kaspersky Endpoint Security 10 для Windows не будет удален и останется доступным для работы. Таким образом, вам будут доступны два плагина управления для работы с программой версии

10 и 11.

- Плагин управления Kaspersky Endpoint Security 11 для Windows не поддерживает управление программой Kaspersky Endpoint Security 10 для Windows на компьютерах пользователей.
- Плагин управления Kaspersky Endpoint Security 11 для Windows не поддерживает элементы (например, политики или задачи), созданные с помощью плагина управления Kaspersky Endpoint Security 10 для Windows.

  Вы можете выполнить конвертацию политик и задач с версии 10 на версию 11 с помощью мастера массовой конвертации политик и задач. Подробнее о конвертации политик и задач см. в *справке Kaspersky Security Center*.

Обновление плагина управления Kaspersky Endpoint Security 11 для Windows

Если в Консоли администрирования установлен плагин управления Kaspersky Endpoint Security 11 для Windows, то установка новой версии плагина управления Kaspersky Endpoint Security 11 для Windows имеет следующие особенности:

- Предыдущая версия плагина управления Kaspersky Endpoint Security 11 для Windows будет удалена.
- Плагин управления Kaspersky Endpoint Security 11 для Windows новой версии поддерживает управление программой Kaspersky Endpoint Security 11 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 программы вы можете узнать в Release Notes или в справке к программе.

- Если в блок параметров в новой версии плагина управления был добавлен новый параметр, то ранее заданный статус атрибута / для этого блока параметров не изменяется.
- При обновлении плагина управления до версии 11.2.0 для автоматической конвертации политики вам нужно открыть политику. При этом Kaspersky Endpoint Security запросит подтверждение участия в KSN. Если на компьютерах организации вы уже обновили программу до версии 11.20, то участие в KSN будет выключено, пока вы не примите условия участия в KSN.

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 программы;
- активация программы с помощью кода активации (тип активации 2.0);
- использование Kaspersky Security Network.

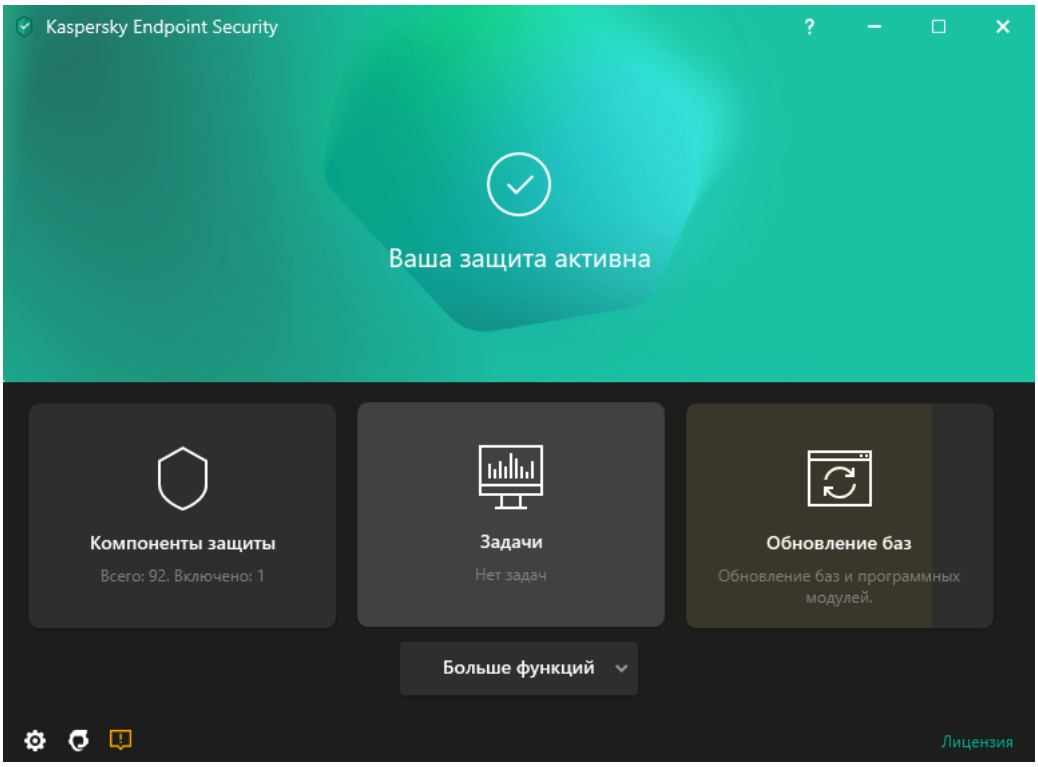
Использование TLS обеспечивает безопасность работы программы за счет следующих свойств:

- 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 программы



Главное окно программы

Компоненты защиты	Статус работы установленных компонентов. Также вы можете перейти к настройке любого из установленных компонентов, кроме компонентов шифрования.
Задачи	Управление задачами проверки Kaspersky Endpoint Security. Вы можете выполнять антивирусную проверку и проверку целостности программы. Администратор может скрыть задачи от пользователя или ограничить управление задачами.
Обновление баз	Управление задачами обновления Kaspersky Endpoint Security. Вы можете выполнять обновление антивирусных баз и модулей программы и откат последнего обновления. Администратор может скрыть задачи от пользователя или ограничить управление задачами.
Больше функций	Переход к другим функциям программы: • **Отчеты**. Просмотр событий, произошедших во время работы программы, отдельных компонентов и задач. • **Хранилище**. Просмотр списка копий зараженных файлов, которые были удалены в ходе работы программы. • **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, программа Kaspersky Endpoint Security получает от служб KSN сведения о категории и репутации проверяемых файлов, а также сведения о репутации проверяемых веб-адресов.

	• **Мониторинг активности**. Просмотр информации о работе установленных программ. Мониторинг активности отслеживает файловые, реестровые и системные события в операционной системе, связанные с программой. • **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.
	Настройка параметров программы. Администратор может запретить изменение параметров в Kaspersky Security Center.
	Информация о программе: 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 программы.
/	Сообщения с информацией о доступных обновлениях, а также запросы доступа к зашифрованным файлам и устройствам.
Лицензия	Лицензирование программы. Вы можете приобрести лицензию, активировать программу или продлить подписку. Так же вы можете просмотреть информацию о действующей лицензии.

Значок программы в области уведомлений

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

Значок программы выполняет следующие функции:

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

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

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

Контекстное меню значка программы содержит следующие пункты:

- **Kaspersky Endpoint Security для Windows**. Открывает главное окно программы. В этом окне вы можете регулировать работу компонентов и задач программы, 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 программа 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 **Возобновление защиты** в контекстном меню программы.

  > Приостановка работы компонентов защиты и контроля не влияет на выполнение задач обновления и проверки. Также программа продолжает использование Kaspersky Security Network.

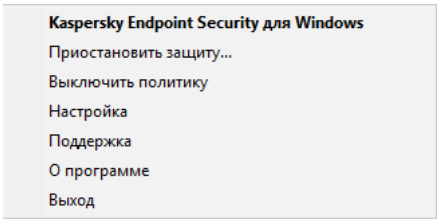
- **Выключить политику** / **Включить политику**. Выключает политику Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком (). При выключении политики программа запрашивает пароль доступа 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 программы.

- Настройка. Открывает окно настройки параметров программы.

- **Поддержка**. Вызов окна **Поддержка**, содержащего информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".

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

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



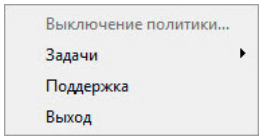
Контекстное меню значка программы

Упрощенный интерфейс программы

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

- **Выключить политику** / **Включить политику**. Выключает политику 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 программа 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 программы.

- **Задачи**. Раскрывающийся список, содержащий следующие элементы:
  - **Проверка целостности**.
  - **Откат последнего обновления**.
  - **Полная проверка**.
  - **Выборочная проверка**.
  - **Проверка важных областей**.
  - **Обновление**.
- **Поддержка**. Вызов окна **Поддержка**, содержащего информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".
- **Выход**. Завершает работу Kaspersky Endpoint Security. Если вы выбрали этот пункт контекстного меню, программа выгружается из оперативной памяти компьютера.



Контекстное меню значка программы при отображении упрощенного интерфейса программы

Настройка отображения интерфейса программы

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

- **С упрощенным интерфейсом**. На клиентском компьютере недоступно главное окно программы, 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 уведомления над значком программы.
- **С полным интерфейсом**. 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.
- **Без интерфейса**. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security. Также недоступны значок в области уведомлений Windows и уведомления.

Как настроить отображение интерфейса программы 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Общие настройки** → **Интерфейс**.
6. В блоке **Взаимодействие с пользователем** выполните одно из следующих действий:
   - Установите флажок **Отображать интерфейс программы**, если вы хотите, чтобы на клиентском компьютере отображались следующие элементы интерфейса:
     - папка с названием программы в меню **Пуск**;
     - значок Kaspersky Endpoint Security в области уведомлений панели задач Microsoft Windows;
     - всплывающие уведомления.

     Если установлен этот флажок, пользователь может просматривать и, при наличии прав, изменять параметры программы из интерфейса программы.
   - Снимите флажок **Отображать интерфейс программы**, если вы хотите скрыть все признаки работы Kaspersky Endpoint Security на клиентском компьютере.
7. В блоке **Взаимодействие с пользователем** установите флажок **Упрощенный интерфейс программы**, если вы хотите, чтобы на клиентском компьютере с установленной программой Kaspersky Endpoint Security отображался упрощенный интерфейс программы.

Как настроить отображение интерфейса программы в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите включить поддержку портативного режима.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Общие настройки** → **Интерфейс**.
5. В блоке **Взаимодействие с пользователем** настройте отображение интерфейса программы:

   - **С упрощенным интерфейсом**. На клиентском компьютере недоступно главное окно программы, 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 уведомления над значком программы.
   - **С полным интерфейсом**. 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.
   - **Без интерфейса**. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security. Также недоступны значок в области уведомлений Windows и уведомления.
6. Нажмите на кнопку **OK**.

Подготовка программы к работе

После развертывания программы 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 программы 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* и *Антивирусная проверка*.

  Задача *Обновление* требуется для поддержания защиты компьютера в актуальном состоянии. При выполнении задачи Kaspersky Endpoint Security обновляет антивирусные базы и модули программы. Задача *Обновление* создается автоматически мастером первоначальной настройки Kaspersky Security Center. Для создания задачи *Обновления* во время работы мастера установите веб-плагин Kaspersky Endpoint Security для Windows.

  Задача *Антивирусная проверка* требуется для своевременного обнаружения вирусов и других программ, представляющих угрозу. Задачу *Антивирусная проверка* вам нужно создать вручную.

Как создать задачу Поиск вирусов в Консоли администрирования (MMC)

1. В Консоли администрирования перейдите в папку **Сервер администрирования → 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 (11.6.0) → Поиск вирусов**.

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 Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет.
- **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 программ, 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 программ. После окончания процедуры лечения активного заражения Kaspersky Endpoint Security перезагружает компьютер без запроса у пользователя подтверждения.

Настройте режим запуска проверки с помощью флажка **Выполнять только во время простоя компьютера**. Флажок включает / выключает функцию, которая приостанавливает задачу *Поиск вирусов*, если ресурсы компьютера заняты. Kaspersky Endpoint Security приостанавливает задачу *Поиск вирусов*, если не включена экранная заставка и разблокирован компьютер.

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 вирусов*. 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 антивирусная проверка в соответствии с установленным расписанием.

[Как создать задачу Антивирусная проверка в Web Console]

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Security для Windows (11.6.0)**.

   b. В раскрывающемся списке **Тип задачи** выберите **Антивирусная проверка**.

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

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

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

5. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.

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

   Рекомендуется настроить расписание выполнения задачи минимум раз в неделю.

7. Установите флажок напротив задачи.

8. 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 антивирусная проверка в соответствии с установленным расписанием.

Управление политиками

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

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.

Активная и неактивная политика

Политика предназначена для группы управляемых компьютеров и может быть активной или неактивной. 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.

Вы можете создать неограниченное количество неактивных политик. Неактивная политика не влияет на параметры программы 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.

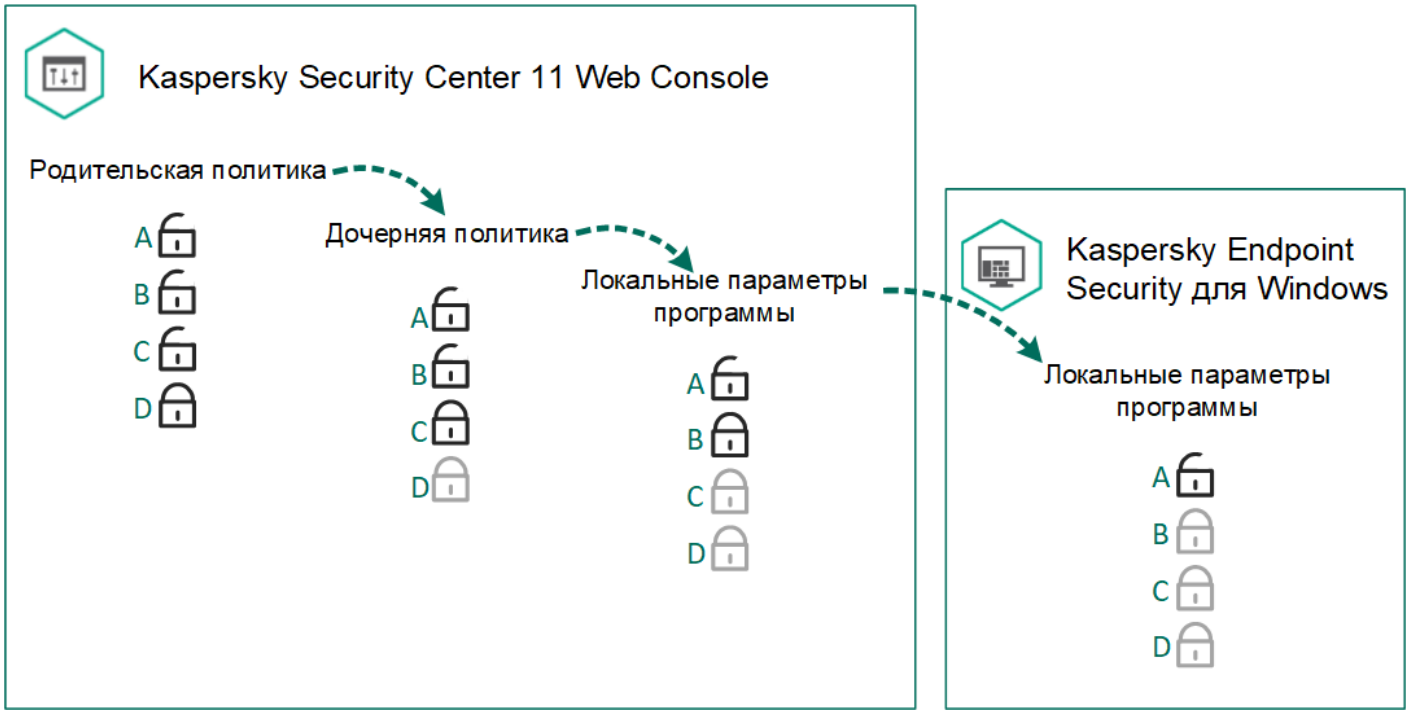
Политика для автономных пользователей

Политика для автономных пользователей активируется, когда компьютер покидает периметр сети организации.

Наследование параметров

Политики, как и группы администрирования, имеют иерархию. По умолчанию дочерняя политика наследует параметры родительской политики. *Дочерняя политика* – политика вложенного уровня иерархии, т.е. политика для вложенных групп администрирования и подчиненных Серверов администрирования. Вы можете выключить наследование параметров из родительской политики.

Каждый параметр, представленный в политике, имеет атрибут, который показывает, наложен ли запрет на изменение параметров в дочерних политиках и локальных параметрах программы. Атрибут работает только, если в дочерней политике включено 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.

Создание 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 закладку **Политики**.
4. Нажмите на кнопку **Новая политика**.

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

Как создать политику в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства → Политики и профили политик**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.
3. Выберите программу Kaspersky Endpoint Security и нажмите **Далее**.
4. Прочитайте и примите условия Положения о Kaspersky Security Network (KSN) и нажмите **Далее**.
5. На закладке **Общие** вы можете выполнить следующие действия:
   - Изменить имя политики.
   - Выбрать состояние политики:
     - **Активна**. После следующей синхронизации политика будет использоваться на компьютере в качестве действующей.
     - **Неактивна**. Резервная политика. При необходимости неактивную политику можно сделать активной.
     - **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 .
6. На закладке **Параметры программ** вы можете настроить параметры политики Kaspersky Endpoint Security.
7. Нажмите на кнопку **Сохранить**.

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 **Поддержка** 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*.

Индикатор уровня защиты

В верхней части окна **Свойства: <Название 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.
  - **Важные**. Категория включает следующие компоненты:
    - Kaspersky Security Network.
    - Защита от веб-угроз.
    - Защита от почтовых угроз.
    - Предотвращение вторжений.
- **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 **Рекомендованные компоненты защиты**. В этом окне вы можете включить любой из рекомендованных компонентов защиты.

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:

- **Антивирусная проверка**. Kaspersky Endpoint Security проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи. Задача *Антивирусная проверка* 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 программ, 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 программы**. 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 программ, хранящихся на компьютерах. Задачу *Инвентаризация* выполняет компонент Контроль программ. Если компонент Контроль программ не установлен, задача завершит работу с ошибкой.

- **Обновление**. Kaspersky Endpoint Security обновляет базы и модули программы. Задача *Обновление* 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 программы. Это может понадобиться, например, если новые базы содержат некорректные данные, из-за которых Kaspersky Endpoint Security может блокировать безопасную программу.

- **Проверка целостности**. Kaspersky Endpoint Security анализирует файлы программы, проверяет файлы на наличие повреждений или изменений и проверяет цифровые подписи файлов программы.

- **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.

Запуск задач на компьютере выполняется только в том случае, если запущена программа 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 и Cloud Console

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

   Откроется список задач.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. Настройте параметры задачи:
   a. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Security для Windows (11.6.0)**.
   b. В раскрывающемся списке **Тип задачи** выберите задачу, которую вы хотите запустить на компьютерах пользователей.
   c. В поле **Название задачи** введите короткое описание, например, `Обновление программы для бухгалтерии`.
   d. В блоке **Выбор устройств, которым будет назначена задача** выберите область действия задачи.
4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.
5. Завершите работу мастера по кнопке **Готово**.

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 и отчеты** → **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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Локальные задачи** → **Управление задачами**.
6. Настройте режим работы с задачами (см. таблицу ниже).
7. Сохраните внесенные изменения.

Как настроить режим работы с задачами в интерфейсе Kaspersky Endpoint Security через Web Console

1. В главном окне Web Console выберите закладку **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите включить поддержку портативного режима.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Локальные задачи** → **Управление задачами**.
5. Настройте режим работы с задачами (см. таблицу ниже).
6. Нажмите на кнопку **ОК**.
7. Подтвердите изменения по кнопке **Сохранить**.

Параметры управления задачами

Параметр	Описание
Разрешить использование	Если флажок установлен, то локальные задачи отображаются в локальном

локальных задач	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 использование локальных задач прекращается. 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 антивирусную 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.
Разрешить отображение групповых задач	Если флажок установлен, то групповые задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь может просмотреть полный список задач в интерфейсе программы. Если флажок снят, Kaspersky Endpoint Security показывает пустой список задач.
Разрешить управление групповыми задачами	Если флажок установлен, пользователь может запускать и останавливать заданные в Kaspersky Security Center групповые задачи. Пользователь может запускать и останавливать задачи в интерфейсе программы или в упрощенном интерфейсе программы. Если флажок снят, Kaspersky Endpoint Security запускает задачи автоматически по расписанию, или администратор запускает задачи вручную в Kaspersky Security Center.

Настройка локальных параметров программы

В Kaspersky Security Center вы можете настроить параметры Kaspersky Endpoint Security на конкретном компьютере – *локальные параметры программы*. Некоторые параметры могут быть недоступны для изменения. Эти параметры заблокированы атрибутом в свойствах политики.

Как настроить локальные параметры программы 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 закладку **Устройства**.
4. Выберите компьютер, для которого вы хотите настроить параметры Kaspersky Endpoint Security.
5. В контекстном меню клиентского компьютера выберите пункт **Свойства**.

   Откроется окно свойств клиентского компьютера.
6. В окне свойств клиентского компьютера выберите раздел **Программы**.

   Справа в окне свойств клиентского компьютера отобразится список программ "Лаборатории Касперского", установленных на клиентском компьютере.
7. Выберите программу Kaspersky Endpoint Security.
8. Нажмите на кнопку **Свойства** под списком программ "Лаборатории Касперского".

   Откроется окно **Параметры программы "Kaspersky Endpoint Security для Windows"**.
9. В разделе **Общие параметры** настройте параметры работы Kaspersky Endpoint Security, а также параметры отчетов и хранилищ.

   Остальные разделы окна **Параметры программы "Kaspersky Endpoint Security для Windows"** стандартны для программы Kaspersky Security Center. Описание этих разделов вы можете прочитать в справке для Kaspersky Security Center.

   > Если для программы создана политика, в которой запрещено изменение некоторых параметров, то во время настройки параметров программы в разделе **Общие параметры** их изменение недоступно.
10. В окне **Параметры программы "Kaspersky Endpoint Security для Windows"** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

[Как настроить локальные параметры программы в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры программы.

   Откроются свойства компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на **Kaspersky Endpoint Security для Windows**.

   Откроются локальные параметры программы
5. Выберите закладку **Параметры программы**.
6. Настройте локальные параметры программы.
7. Локальные параметры программы повторяют параметры политики, кроме параметров шифрования.

Запуск и остановка Kaspersky Endpoint Security

После установки Kaspersky Endpoint Security на компьютер пользователя запуск программы выполняется автоматически. Далее по умолчанию запуск Kaspersky Endpoint Security выполняется сразу после операционной системы. Настроить автоматический запуск программы 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 программы 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Общие настройки** → **Настройки программы**.
6. С помощью флажка **Запускать Kaspersky Endpoint Security для Windows при включении компьютера** настройте запуск программы.
7. Сохраните внесенные изменения.

Как настроить запуск Kaspersky Endpoint Security в Web Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите настроить запуск программы.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Выберите раздел **Общие настройки**.
5. Перейдите по ссылке **Настройки программы**.
6. С помощью флажка **Запускать Kaspersky Endpoint Security для Windows при включении компьютера** настройте запуск программы.
7. Нажмите на кнопку **ОК**.
8. Подтвердите изменения по кнопке **Сохранить**.

Как настроить запуск Kaspersky Endpoint Security в интерфейсе программы

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Общие**.
3. С помощью флажка **Запускать при включении компьютера** настройте запуск программы.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить 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 программы.

Вы можете контролировать статус работы программы 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 входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, на котором вы хотите запустить или остановить программу.
5. По правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Свойства**.
6. В окне свойств клиентского компьютера выберите раздел **Программы**.

   Справа в окне свойств клиентского компьютера отобразится список программ "Лаборатории Касперского", установленных на клиентском компьютере.
7. Выберите программу Kaspersky Endpoint Security.
8. Выполните следующие действия:
   - Если вы хотите запустить программу, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  .
   - Если вы хотите остановить работу программы, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  .

Как запустить или остановить Kaspersky Endpoint Security в Web Console

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите запустить или остановить Kaspersky Endpoint Security.

   Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Установите флажок напротив программы **Kaspersky Endpoint Security для Windows**.
5. Нажмите на кнопку **Запустить** или **Остановить**.

Как запустить или остановить Kaspersky Endpoint Security через командную строку

Для завершения работы программы из командной строки необходимо включить внешнее управление системными службами.

Для запуска или завершения работы программы из командной строки используется файл klpsm.exe, входящий в комплект поставки Kaspersky Endpoint Security.

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Для запуска программы в командной строке введите `klpsm.exe start_avp_service`.
4. Для остановки программы в командной строке введите `klpsm.exe stop_avp_service`.

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 программы отображается с помощью значка программы 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 программы, 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 перезагрузки программы** – защита и контроль компьютера включатся после перезапуска программы или перезагрузки операционной системы. Для использования этой возможности должен быть включен автоматический запуск программы.
   - **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 программы

Чтобы возобновить защиту и контроль компьютера, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка программы, 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.

Проверка компьютера

Антивирусная проверка является важным фактором для обеспечения безопасности компьютера. Требуется регулярно выполнять антивирусную проверку, чтобы исключить возможность распространения вредоносных программ, 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 запускать 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:

- память ядра;
- объекты, загрузка которых осуществляется при запуске операционной системы;

- резервное хранилище операционной системы;
- почтовый ящик Microsoft Outlook;
- 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

Kaspersky Endpoint Security проверяет модули программы на наличие повреждений или изменений.

Запуск и остановка задачи проверки

Независимо от выбранного режима запуска задачи проверки вы можете запустить или остановить задачу проверки в любой момент.

Чтобы запустить или остановить задачу проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.
2. Нажмите на кнопку **Запустить проверку**, если вы хотите запустить задачу проверки.

   Kaspersky Endpoint Security запустит проверку компьютера. Программа покажет процесс проверки, количество проверенных файлов и оставшиеся время. Вы можете остановить выполнение задачи в любое время по кнопке **Остановить**.

Чтобы запустить или остановить задачу проверки при отображении упрощенного интерфейса программы, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню в раскрывающемся списке **Задачи** выполните одно из следующих действий:
   - выберите незапущенную задачу проверки, чтобы запустить ее;
   - выберите запущенную задачу проверки, чтобы остановить ее;
   - выберите остановленную задачу проверки, чтобы возобновить ее или запустить ее заново.

Изменение уровня безопасности

Для проверки Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в программе, называются *уровнями безопасности*: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными. Они рекомендованы специалистами "Лаборатории Касперского". 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.

Чтобы изменить уровень безопасности, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:
     - **Высокий**. Kaspersky Endpoint Security проверяет файлы всех типов. Во время проверки составных файлов Kaspersky Endpoint Security дополнительно проверяет файлы почтовых форматов.
     - **Рекомендуемый**. Kaspersky Endpoint Security проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты. Kaspersky Endpoint Security не проверяет архивы и установочные пакеты.
     - **Низкий**. Kaspersky Endpoint Security проверяет только новые и измененные файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера. Kaspersky Endpoint Security не проверяет составные файлы.
   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента.

     Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности** в верхней части окна.
4. Сохраните внесенные изменения.

Изменение действия над зараженными файлами

По умолчанию при обнаружении зараженных файлов Kaspersky Endpoint Security пытается вылечить их или удаляет их, если лечение невозможно.

Чтобы изменить действие над зараженными файлами, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. В блоке **Действие при обнаружении угрозы** выберите один из следующих вариантов:

- **Лечить; удалять, 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 их удаляет.

- **Лечить; блокировать, 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 Kaspersky Endpoint Security 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.

4. Сохраните внесенные изменения.

Формирование списка проверяемых объектов

Чтобы сформировать список проверяемых объектов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Перейдите по ссылке **Изменить область проверки**.
4. В открывшемся окне выберите объекты, которые вы хотите добавить в область проверки или исключить из нее.

   Вы не можете удалить или изменить объекты, включенные в область проверки по умолчанию.

5. Если вы хотите добавить новый объект в область проверки, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   Откроется дерево папок.

   b. Выберите объект и нажмите на кнопку **Выбрать**.

   Вы можете исключить объект из проверки, не удаляя его из списка объектов области проверки. Для этого снимите флажок рядом с ним.

6. Сохраните внесенные изменения.

Выбор типа проверяемых файлов

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 другую программу, представляющую угрозу, на ваш компьютер в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки программа 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 программа проверяет его.

Чтобы выбрать тип проверяемых файлов выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.

2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять во время выполнения выбранной задачи 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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.

   Файлы без расширения Kaspersky Endpoint Security считает исполняемыми. Kaspersky Endpoint Security проверяет исполняемые файлы всегда, независимо от того, файлы какого типа вы выбрали для проверки.

5. Сохраните внесенные изменения.

Оптимизация проверки файлов

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, что 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).

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.

Чтобы оптимизировать проверку файлов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Оптимизация проверки** 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.
   - **Пропускать файлы, если их проверка длится более N секунд**. Ограничение длительности проверки одного объекта. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку файла. Это позволит сократить время выполнения проверки.
5. Сохраните внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие программы, 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.

Чтобы настроить проверку составных файлов, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты, файлы офисных форматов, файлы почтовых форматов, защищенные паролем архивы.
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. В блоке **Ограничение по размеру**, выполните одно из следующих действий:

   - Если вы не хотите распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение.
   - Если вы хотите распаковывать составные файлы независимо от размера, снимите флажок **Не распаковывать составные файлы большого размера**.

   Kaspersky Endpoint Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

7. 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 программы. 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 использовать методы проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Методы проверки** установите флажок **Эвристический анализ**, если вы хотите, чтобы программа использовала эвристический анализ во время выполнения задачи проверки. Далее при помощи ползунка задайте уровень эвристического анализа: **Поверхностный**, **Средний** или **Глубокий**.
5. Сохраните внесенные изменения.

Использование технологий проверки

Чтобы использовать технологии проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.

2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.

3. Нажмите на кнопку **Расширенная настройка**.

4. 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 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 программе структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

5. Сохраните внесенные изменения.

Выбор режима запуска для задачи проверки

Если по каким-либо причинам запуск задачи проверки невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи проверки, как только это станет возможным.

Вы можете отложить запуск задачи проверки после старта программы для случаев, если время запуска задачи проверки совпадает с запуском Kaspersky Endpoint Security. Задача проверки запускается только по истечении указанного времени после старта Kaspersky Endpoint Security.

Чтобы выбрать режим запуска для задачи проверки, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.

2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.

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.

   a. 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 проверки.

      Если в раскрывающемся списке **Запускать проверку** выбран элемент **По минутам**, **По часам**, **После запуска программы** или **После каждого обновления**, то флажок **Запускать проверку по расписанию на следующий день, если компьютер был выключен** недоступен.

b. Установите флажок **Выполнять только во время простоя компьютера**, если вы хотите, чтобы Kaspersky Endpoint Security приостанавливал задачу, когда ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка.

   Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.

6. Сохраните внесенные изменения.

Настройка запуска задачи проверки с правами другого пользователя

По умолчанию задача проверки запускается с правами учетной записи, под которой пользователь зарегистрирован в операционной системе. Однако может возникнуть необходимость запустить задачу проверки с правами другого пользователя. Вы можете указать пользователя, обладающего этими правами, в параметрах задачи проверки и запускать задачу проверки от имени этого пользователя.

Чтобы настроить запуск задачи проверки с правами другого пользователя, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Нажмите на кнопку **Расширенная настройка** → **Запускать проверку с правами**.
4. В открывшемся окне выберите пользователя, права которого требуется использовать для запуска задачи проверки.
5. Сохраните внесенные изменения.

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 программ, 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 обеспечивают 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.

Чтобы настроить проверку съемных дисков при их подключении к компьютеру, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки съемных дисков и нажмите на кнопку ⚙.
3. Используйте переключатель **Проверка съемных дисков**, чтобы включить или выключить проверку съемных дисков при подключении к компьютеру.
4. Выберите режим проверки съемных дисков при подключении к компьютеру:

- **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.

5. Если вы хотите, чтобы Kaspersky Endpoint Security проверял только те съемные диски, размер которых не превышает указанного значения, установите флажок **Максимальный размер съемного диска** и укажите в соседнем поле значение в мегабайтах.

6. Настройте отображение хода проверки съемного диска. Выполните одно из следующих действий:

   - Если вы хотите, чтобы программа Kaspersky Endpoint Security отображала ход проверки съемных дисков в отдельном окне, установите флажок **Отображать ход проверки**.

     В окне проверки съемного диска пользователь может остановить проверку. Чтобы сделать проверку съемных дисков обязательной и запретить пользователю останавливать проверку, установите флажок **Запретить остановку задачи проверки**.

   - Если вы хотите, чтобы программа Kaspersky Endpoint Security запускала проверку съемных дисков в фоновом режиме, снимите флажок **Отображать ход проверки**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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. 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.

Чтобы включить фоновую проверку компьютера, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Используйте переключатель **Фоновая проверка**, чтобы включить или выключить фоновую проверку.
4. Сохраните внесенные изменения.

Проверка целостности программы

Kaspersky Endpoint Security проверяет файлы программы, находящиеся в папке установки программы, на наличие повреждений или изменений. Например, если библиотека программы имеет некорректную цифровую подпись, то такая библиотека считается поврежденной. Для проверки файлов программы предназначена задача *Проверка целостности*. Запускайте задачу *Проверка целостности*, если программа Kaspersky Endpoint Security обнаружила вредоносный объект и не обезвредила его.

Вы можете создать задачу *Проверка целостности* в Kaspersky Security Center 12 Web Console и Консоли администрирования. Создать задачу в программе Kaspersky Security Center Cloud Console невозможно.

Как выполнить проверку целостности программы через Консоль администрирования (MMC)

1. В Консоли администрирования перейдите в папку **Сервер администрирования → 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 (11.6.0) → Проверка целостности**.

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 программы 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 программы. Вы также можете настроить расписание проверки целостности программы в свойствах задачи.

[Как выполнить проверку целостности программы через Web Console]

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Security для Windows (11.6.0)**.

   b. В раскрывающемся списке **Тип задачи** выберите **Проверка целостности**.

   c. В поле **Название задачи** введите короткое описание, например, `Проверка целостности программы после заражения компьютера`.

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

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

5. Завершите работу мастера по кнопке **Готово**.

   В списке задач отобразится новая задача.

6. Установите флажок напротив задачи.

В результате Kaspersky Endpoint Security выполнит проверку целостности программы. Вы также можете настроить расписание проверки целостности программы в свойствах задачи.

Нарушения целостности программы 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.

Обновление баз и модулей программы

Обновление баз и модулей программы Kaspersky Endpoint Security обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие программы, 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 программы.

Для регулярного обновления требуется действующая лицензия на использование программы. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

Основным источником обновлений Kaspersky Endpoint Security служат серверы обновлений "Лаборатории Касперского".

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 программ, 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 программы. Помимо баз Kaspersky Endpoint Security, можно обновлять и модули программы. Обновления модулей программы устраняют уязвимости Kaspersky Endpoint Security, добавляют новые функции или улучшают существующие.

В процессе обновления базы и модули программы на вашем компьютере сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы и модули программы отличаются от актуальной версии, на компьютер устанавливается недостающая часть обновлений.

Вместе с обновлением модулей программы может быть обновлена и контекстная справка программы.

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 блоке **Обновление** в окне **Задачи**.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении задачи обновления, записывается в отчет Kaspersky Endpoint Security.

Схемы обновления баз и модулей программы

Обновление баз и модулей программы Kaspersky Endpoint Security обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие программы, 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 программы.

На компьютерах пользователей обновляются следующие объекты:

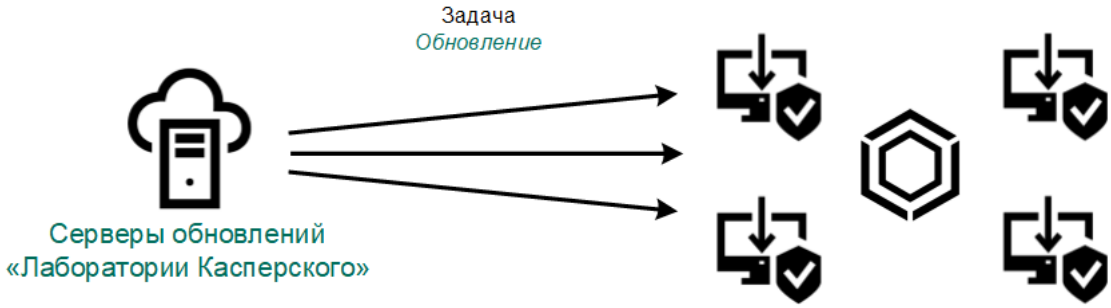
- Антивирусные базы. Антивирусные базы включают в себя базы сигнатур вредоносных программ, описание сетевых атак, базы вредоносных и фишинговых веб-адресов, базы баннеров, спам-базы и другие данные.

- Модули программы. Обновление модулей предназначено для устранения уязвимостей в программе и улучшения методов защиты компьютера. Обновления модулей могут менять поведение компонентов программы и добавлять новые возможности.

Kaspersky Endpoint Security поддерживает следующие схемы обновления баз и модулей программы:

- 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).

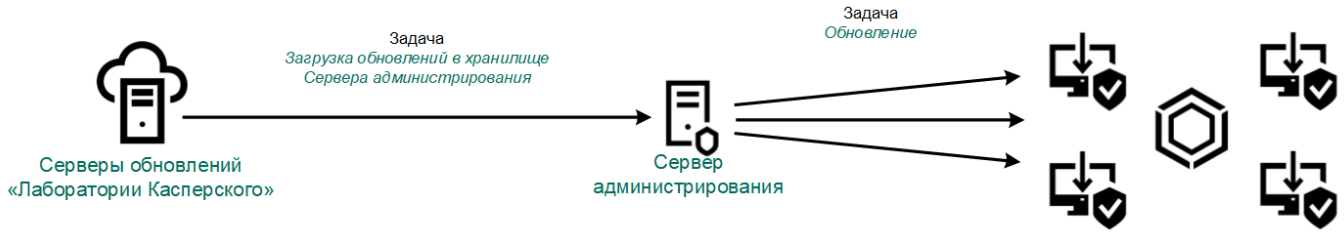
     Загрузку пакета обновлений в папку общего доступа можно обеспечить следующими способами:

     - С помощью задачи Kaspersky Endpoint Security *Обновление*. Задача предназначена для одного из компьютеров локальной сети организации.

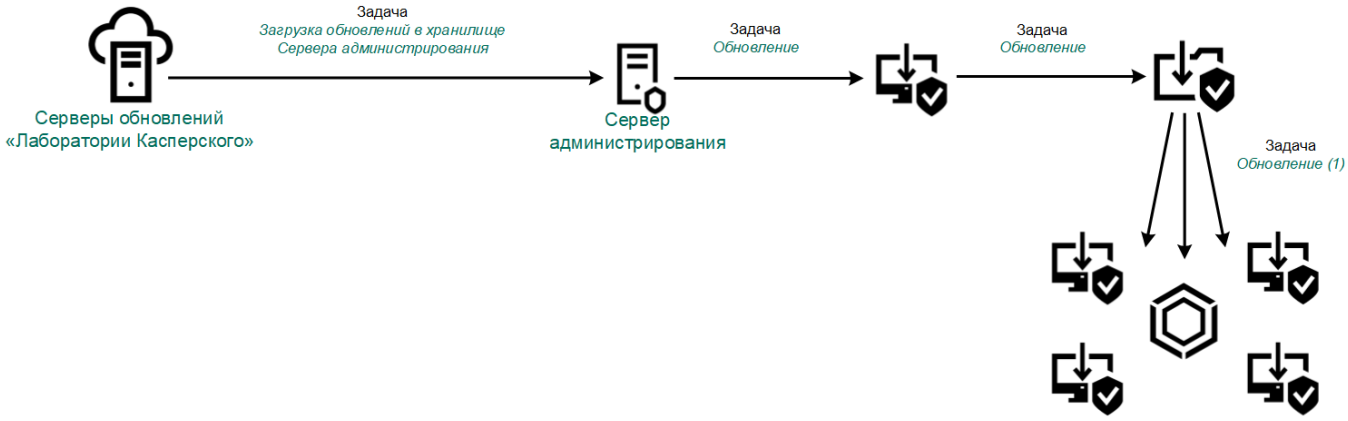
     - С помощью Kaspersky Update Utility. Подробную информацию о работе с Kaspersky Update Utility *см. в Базе знаний "Лаборатории Касперского"*.

3. Распространение пакета обновлений на клиентские компьютеры.

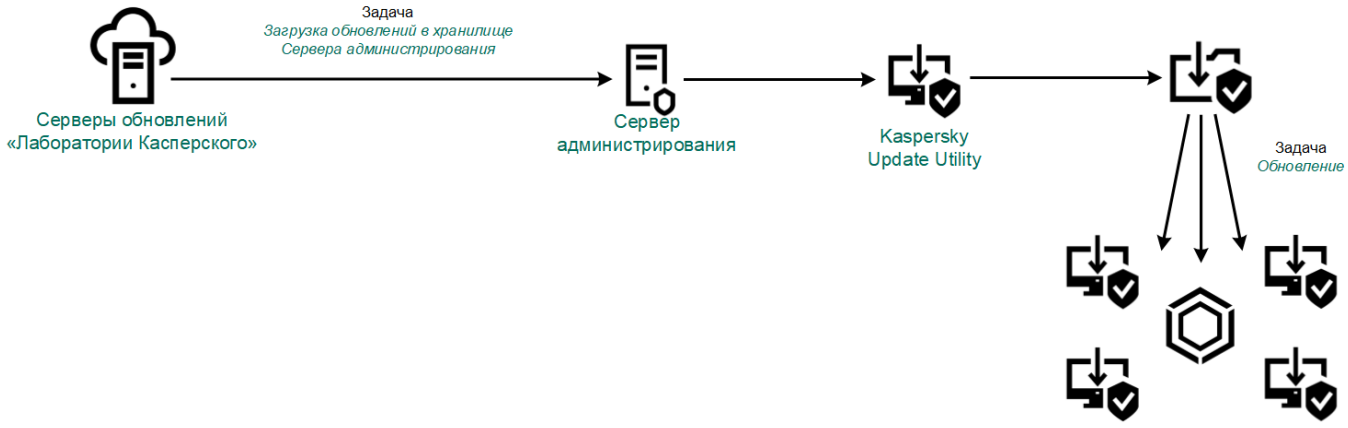
   Распространение пакета обновлений на клиентские компьютеры обеспечивает задача Kaspersky Endpoint Security *Обновление*. Вы можете создать неограниченное количество задач обновления для каждой из групп администрирования.



Обновление с серверного хранилища



Обновление из папки общего доступа



Обновление с помощью Kaspersky Update Utility

Для Web Console 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.

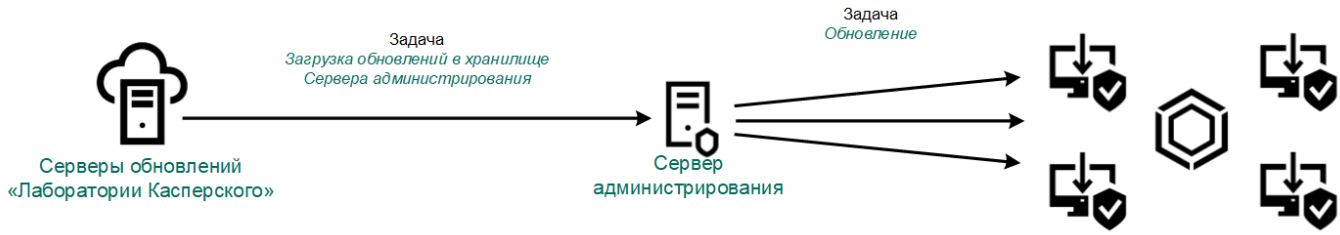
Обновление с серверного хранилища

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы 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 программы с серверного хранилища состоит из следующих этапов:

1. Настройка перемещения пакета обновлений в хранилище на Сервере администрирования (задача *Загрузка обновлений в хранилище Сервера администрирования*).

2. Настройка обновления баз и модулей программы из указанного серверного хранилища на остальных компьютерах локальной сети организации (задача *Обновление*).



Обновление с серверного хранилища

Чтобы настроить загрузку пакета обновлений в серверное хранилище, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на задачу Сервера администрирования **Загрузка обновлений в хранилище Сервера администрирования**.

   Откроется окно свойств задачи.

   Задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически мастером первоначальной настройки Kaspersky Security Center 12 Web Console и может существовать только в единственном экземпляре.

3. Выберите закладку **Параметры программы**.

4. В блоке **Прочие параметры** нажмите на кнопку **Настроить**.

5. В поле **Папка для хранения 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".

   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://<имя пользователя>:<пароль>@<узел>:<порт>`.

- 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\AVP11\Update distribution\`.

6. Сохраните внесенные изменения.

Чтобы настроить обновление Kaspersky Endpoint Security из указанного серверного хранилища, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление**.

   Откроется окно свойств задачи.

   Задача *Обновление* создается автоматически мастером первоначальной настройки Kaspersky Security Center. Для создания задачи *Обновления* во время работы мастера установите веб-плагин Kaspersky Endpoint Security для Windows.

3. Выберите закладку **Параметры программы** → **Локальный режим**.

4. В списке источников обновления нажмите на кнопку **Добавить**.

5. В поле **Источник** 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, указанный ранее в поле **Папка для хранения обновлений** при настройке загрузки обновлений в серверное хранилище (см. *инструкцию выше*).

6. В блоке **Статус** выберите вариант **Включено**.

7. Нажмите на кнопку **ОК**.

8. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

9. Нажмите на кнопку **Сохранить**.

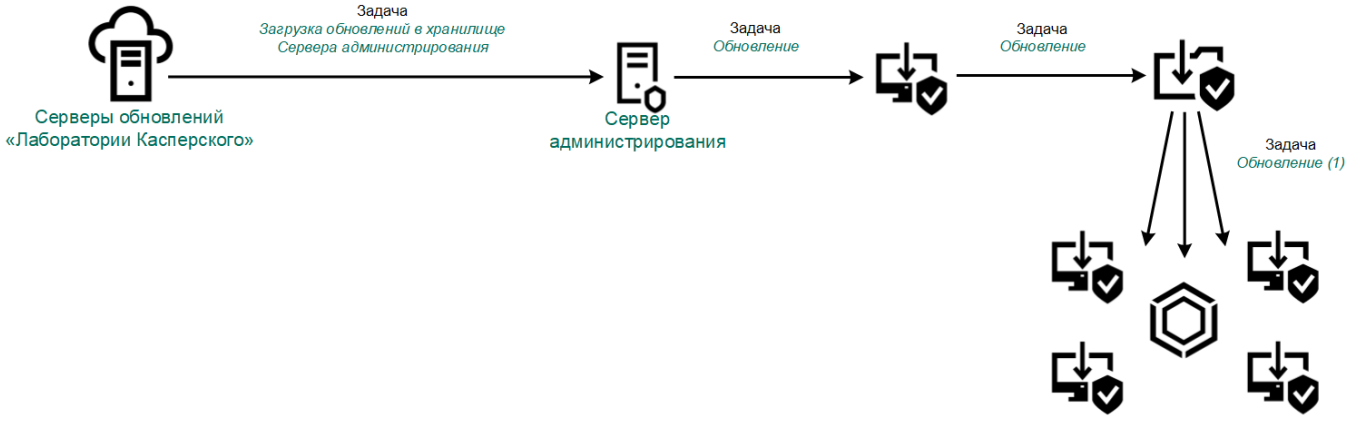
Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

Обновление из папки общего доступа

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы 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.

Настройка обновления баз и модулей программы из папки общего доступа состоит из следующих этапов:

1. Настройка обновления баз и модулей программы с серверного хранилища.
2. Включение режима копирования пакета обновлений в папку общего доступа на одном из компьютеров локальной сети организации (см. инструкцию ниже).
3. Настройка обновления баз и модулей программы из указанной папки общего доступа на остальных компьютерах локальной сети организации (см. инструкцию ниже).



Обновление из папки общего доступа

Чтобы включить режим копирования пакета обновлений в папку общего доступа, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление**.

   Откроется окно свойств задачи.

   Задача *Обновление* создается автоматически мастером первоначальной настройки Kaspersky Security Center. Для создания задачи *Обновления* во время работы мастера установите веб-плагин Kaspersky Endpoint Security для Windows.

3. Выберите закладку **Параметры программы** → **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\Share\Update distribution`).

Если оставить поле пустым, Kaspersky Endpoint Security будет копировать пакет обновлений в папку `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

7. Нажмите на кнопку **Сохранить**.

Задача *Обновление* должна быть назначена для одного компьютера, который будет считаться источником обновлений.

Чтобы настроить обновление из папки общего доступа, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Security для Windows (11.6.0)**.

   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 **Выбор устройств, 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 нажмите на кнопку **Далее**.

5. Завершите работу мастера по кнопке **Создать**.

   В таблице задач отобразится новая задача.

6. Нажмите на созданную задачу *Обновление*.

   Откроется окно свойств задачи.

7. Перейдите в раздел **Параметры программы**.

8. Выберите закладку **Локальный режим**.

9. В блоке **Источник обновлений** нажмите на кнопку **Добавить**.

10. В поле **Источник** укажите 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*).

11. Нажмите на кнопку **OK**.

12. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.

13. Нажмите на кнопку **Сохранить**.

Обновление с помощью Kaspersky Update Utility

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы 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.

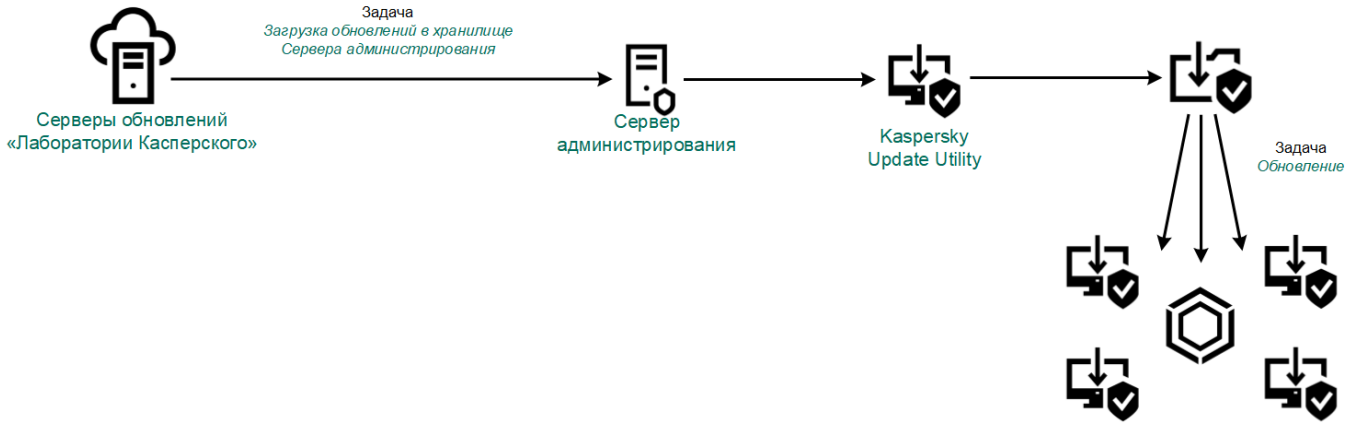
Настройка обновления баз и модулей программы из папки общего доступа состоит из следующих этапов:

1. Настройка обновления баз и модулей программы 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.

4. Настройка обновления баз и модулей программы из указанной папки общего доступа на остальных компьютерах локальной сети организации.



Обновление с помощью 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"*.

Чтобы настроить обновление из папки общего доступа, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление**.

Откроется окно свойств задачи.

Задача *Обновление* создается автоматически мастером первоначальной настройки Kaspersky Security Center. Для создания задачи *Обновления* во время работы мастера установите веб-плагин Kaspersky Endpoint Security для Windows.

3. Выберите закладку **Параметры программы** → **Локальный режим**.
4. В списке источников обновлений нажмите на кнопку **Добавить**.
5. В поле **Источник** введите UNC-путь к папке общего доступа (например, `\\Server\Share\Update distribution`).

   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**.
8. Нажмите на кнопку **Сохранить**.

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 программы. По умолчанию для обновления баз и модулей программы 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.

Чтобы настроить параметры обновления в мобильном режиме, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление**.

   Откроется окно свойств задачи.

   Задача *Обновление* создается автоматически мастером первоначальной настройки Kaspersky Security Center. Для создания задачи *Обновления* во время работы мастера установите веб-плагин Kaspersky Endpoint Security для Windows.

   Выберите закладку **Параметры программы** → **Мобильный режим**.

3. Настройте источники обновлений. В качестве источников обновлений могут быть использованы серверы обновлений "Лаборатории Касперского" или другие FTP- или HTTP-серверы, локальные или сетевые папки.
4. Нажмите на кнопку **Сохранить**.

В результате на компьютерах пользователей будут обновлены базы и модули программы 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 программы нажмите на кнопку **Обновление баз**.
2. В блоке **Обновление баз и программных модулей** нажмите на кнопку **Обновить**, если вы хотите запустить задачу обновления.

   Kaspersky Endpoint Security запустит обновление баз и модулей программы. Программа покажет процесс проверки, размер загруженных файлов и источник обновления. Вы можете остановить выполнение задачи в любое время по кнопке  .

Чтобы запустить или остановить задачу обновления при отображении упрощенного интерфейса программы, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка программы, 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 Kaspersky Endpoint Security запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление 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 Kaspersky Endpoint Security и запускать задачу обновления Kaspersky Endpoint Security от имени этого пользователя.

Чтобы запускать задачу обновления с правами другого пользователя, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.
3. Нажмите на кнопку **Настройки учетной записи**.

4. В открывшемся окне выберите вариант **Запускать обновление баз с правами 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 программы 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:

1. В главном окне программы нажмите на кнопку **Обновление баз**.

2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.

3. Нажмите на кнопку **Задать режим запуска обновления баз**.

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 вариант <**По расписанию**>, если вы хотите настроить расписание запуска задачи обновления. Настройте дополнительные параметры запуска задачи обновления:

     - В поле **Отложить запуск после старта программы на** укажите время, на которое следует отложить запуск задачи обновления после старта Kaspersky Endpoint Security.

     - Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы Kaspersky Endpoint Security запускал при первой возможности не запущенные вовремя задачи обновления.

5. Сохраните внесенные изменения.

Добавление источника обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей программы Kaspersky Endpoint Security.

Источником обновлений могут быть сервер Kaspersky Security Center, серверы обновлений "Лаборатории Касперского", сетевая или локальная папка.

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.

Чтобы добавить источник обновлений, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.
3. Нажмите на кнопку **Настроить источники обновлений**.
4. В открывшемся окне 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://<имя пользователя>:<пароль>@<узел>:<порт>`.
   - 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\AVP11\Update distribution\`.
6. Нажмите на кнопку **Выбрать**.
7. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.
8. Сохраните внесенные изменения.

Настройка обновления из папки общего доступа

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы 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.

Настройка обновления баз и модулей программы из папки общего доступа состоит из следующих этапов:

1. Включение режима копирования пакета обновлений в папку общего доступа на одном из компьютеров локальной сети организации.
2. Настройка обновления баз и модулей программы из указанной папки общего доступа на остальных компьютерах локальной сети организации.

Чтобы включить режим копирования пакета обновлений в папку общего доступа, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.
3. В блоке **Копирование обновлений** установите флажок **Копировать обновления в папку**.
4. Введите UNC-путь к папке общего доступа (например, `\\Server\Share\Update distribution`).
5. Сохраните внесенные изменения.

Чтобы настроить обновление из папки общего доступа, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.
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**.
8. Сохраните внесенные изменения.

Обновление модулей программы

Обновления модулей программы исправляют ошибки, улучшают производительность, а также добавляют новые функции. При появлении нового обновления модулей программы вам необходимо подтвердить установку обновления. Вы можете подтвердить установку обновления модулей программы в интерфейсе программы или в Kaspersky Security Center. При появлении обновления программа покажет уведомление в главном окне Kaspersky Endpoint Security: важное обновление – , или критическое обновление – . Если обновление модулей программы предполагает ознакомление и согласие с положениями Лицензионного соглашения, то программа устанавливает обновление после согласия с положениями Лицензионного соглашения. Подробнее об отслеживании обновлений модулей программы и подтверждении обновления в Kaspersky Security Center *см. в справке Kaspersky Security Center*.

После установки обновления программы может потребоваться перезагрузка компьютера.

Чтобы настроить обновление модулей программы, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.
3. В блоке **Загрузка и установка обновлений модулей программы** установите флажок **Загружать обновления модулей программы**.
4. Выберите обновления модулей программы, которые вы хотите устанавливать:

   - **Устанавливать критические и одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает критические обновления автоматически, а остальные обновления модулей программы – после одобрения их установки, локально через интерфейс программы или на стороне Kaspersky Security Center.
   - **Устанавливать только одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс программы 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 программы 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. Нажмите на кнопку **Сохранить**.

Чтобы выключить использование прокси-сервера для определенной группы администрирования, выполните следующие действия:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.

2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите выключить использование прокси-сервера.

   Откроется окно свойств политики.

3. Выберите закладку **Параметры программы**.

4. Перейдите в раздел **Общие настройки** → **Настройки сети**.

5. В блоке **Настройки прокси-сервера** выберите вариант **Не использовать прокси-сервер**.

6. Нажмите на кнопку **ОК**.

7. Подтвердите изменения по кнопке **Сохранить**.

Чтобы настроить параметры прокси-сервера в интерфейсе программы, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Настройки сети**.

3. В блоке **Прокси-сервер** перейдите по ссылке **Настройка прокси-сервера**.

4. В открывшемся окне выберите один из следующих вариантов определения адреса прокси-сервера:

   - **Автоматически определять настройки прокси-сервера**.

     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. Если вы хотите включить использование аутентификации на прокси-сервере, установите флажок **Использовать аутентификации на прокси-сервере** и укажите учетные данные пользователя.

6. Если вы хотите выключить использование прокси-сервера при обновлении баз и модулей программы 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 программы. 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 первого обновления баз и модулей программы становится доступна функция отката к предыдущим базам и модулям программы.

Каждый раз, когда пользователь запускает обновление, Kaspersky Endpoint Security создает резервную копию используемых баз и модулей программы и только потом приступает к их обновлению. Это позволяет вернуться к использованию предыдущих баз и модулей программы при необходимости. Возможность отката последнего обновления полезна, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасную программу.

Чтобы откатить последнее обновление, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. В блоке **Откат к предыдущей версии баз** нажмите на кнопку **Откатить**.

   Kaspersky Endpoint Security запустит откат последнего обновления баз. Программа покажет процесс отката, размер загруженных файлов и источник обновления. Вы можете остановить выполнение задачи в любое время по кнопке  .

Чтобы запустить или остановить задачу отката обновления при отображении упрощенного интерфейса программы, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню в раскрывающемся списке **Задачи** выполните одно из следующих действий:

   - Выберите незапущенную задачу отката обновления, чтобы запустить ее.
   - Выберите запущенную задачу отката обновления, чтобы остановить ее.
   - Выберите остановленную задачу отката обновления, чтобы возобновить ее или запустить ее заново.

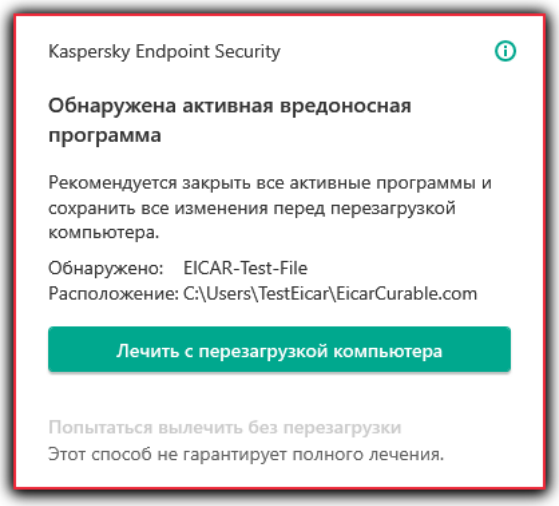
Работа с активными угрозами

Программа 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. Для работы с активными угрозами Kaspersky Endpoint Security использует технологию лечения активного заражения. Работа технологии лечения активного заражения для рабочих станций и серверов отличается. Вы можете настроить технологию лечения активного заражения в свойствах задачи *Антивирусная проверка* и в параметрах программы.

Лечение активных угроз на рабочих станциях

Для работы с активными угрозами на рабочих станциях вам нужно включить технологию лечения активного заражения в параметрах программы. Далее вам нужно настроить взаимодействие программы с пользователем в свойствах задачи *Антивирусная проверка*. В свойствах задачи есть флажок **Включить 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 программы;
- включите немедленное лечение активного заражения в свойствах задачи *Антивирусная проверка*.

Если программа Kaspersky Endpoint Security установлена 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 программы и включить немедленное лечение активного заражения в свойствах задачи *Антивирусная проверка*. Далее вам нужно запустить задачу *Антивирусная проверка*.

Обработка активных угроз

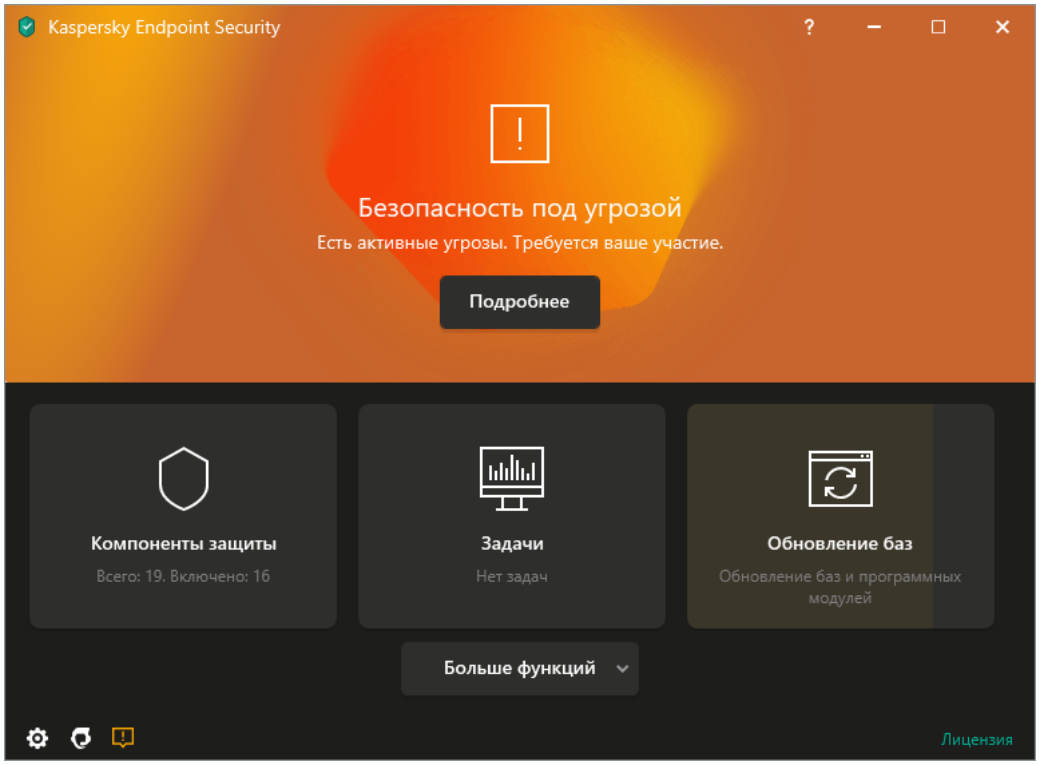
Зараженный файл считается *обработанным*, если Kaspersky Endpoint Security в процессе проверки компьютера на вирусы и другие программы, представляющие угрозу, совершил одно из следующих действий с этим файлом согласно заданным настройкам программы:

- Лечить.
- Удалять.
- Удалять, если лечение невозможно.

Kaspersky Endpoint Security помещает файл в список активных угроз, если в процессе проверки компьютера на вирусы и другие программы, представляющие угрозу, Kaspersky Endpoint Security по каким-либо причинам не совершил действие с этим файлом согласно заданным настройкам программы.

Такая ситуация возможна в следующих случаях:

- Проверяемый файл недоступен (например, находится на сетевом диске или внешнем диске без прав на запись данных).
- В настройках программы для задач проверки в блоке **Действие при обнаружении угрозы** выбрано действие **Информировать**, и когда на экране отобразилось уведомление о зараженном файле, пользователь выбрал вариант **Пропустить**.



Главное окно программы при обнаружении угрозы

Чтобы обработать активные угрозы, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Подробнее**.

   Откроется список активных угроз.

2. Выберите объект, который вы хотите устранить.

3. Выберите способ устранения угрозы:

   - **Устранить**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет.

   - **Игнорировать**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удалить 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 Вирусной энциклопедии "Лаборатории Касперского".

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. 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 программа. При обнаружении вредоносного файла Kaspersky Endpoint Security блокирует операцию с файлом. Далее программа 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 Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в программе, 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.

Чтобы включить или выключить компонент Защита от файловых угроз, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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. Значения параметров для рекомендуемого уровня безопасности см. в таблице ниже.

- **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.

  Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности** в верхней части окна.

5. 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, Kaspersky Endpoint Security 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 программ "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	**Включено**	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.
Технология iSwift	**Включено**	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	**Включено**	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 настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной программе структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Проверять файлы офисных форматов	**Включено**	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
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 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 Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет.

Автоматическая приостановка Защиты от файловых угроз

Вы можете настроить автоматическую приостановку Защиты от файловых угроз в указанное время или во время работы с определенными программами.

Приостановка работы Защиты от файловых угроз при конфликте с определенными программами 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 программами на вашем компьютере.

Чтобы настроить автоматическую приостановку работы Защиты от файловых угроз, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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 программ, 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 нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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 Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет.

   - **Лечить; блокировать, 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.

   - **Блокировать**. Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически блокирует зараженные файлы без попытки их вылечить.

   Перед лечением или удалением зараженного файла Kaspersky Endpoint Security 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 другую программу, представляющую угрозу, на ваш компьютер в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки программа 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 программа проверяет его.

Чтобы сформировать область защиты, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .

2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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. Выберите объект и нажмите на кнопку **Выбрать**.

   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 программы. 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Методы проверки** установите флажок **Эвристический анализ**, если вы хотите, чтобы программа использовала 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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:
   - **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 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 программе 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 нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.
5. Сохраните внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие программы, 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 RAR, ARJ, ZIP, CAB, LHA и удаляет файлы всех остальных форматов (кроме почтовых баз).

Чтобы настроить проверку составных файлов, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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 или файлы 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, программа 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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 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.

Защита от веб-угроз

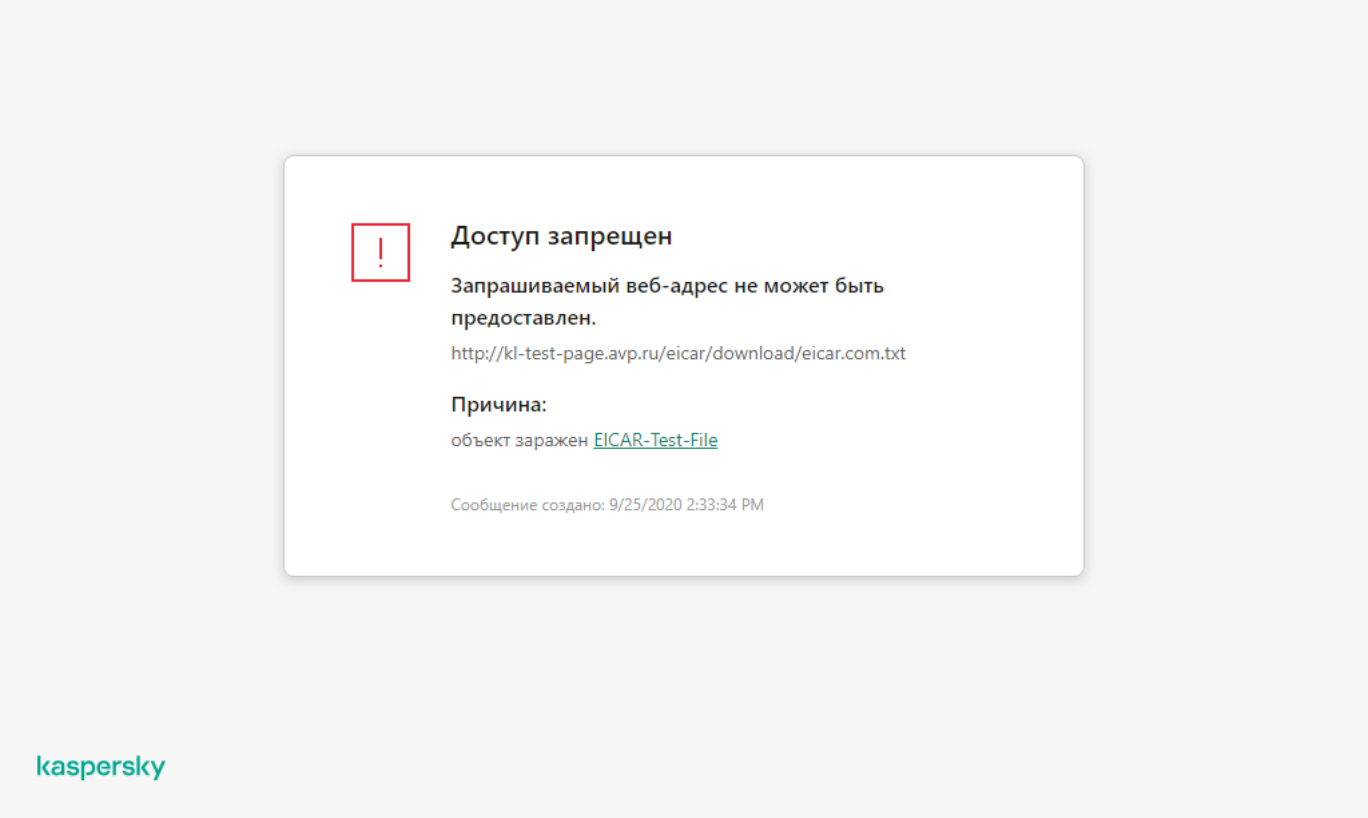
Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует вредоносные и фишинговые веб-сайты. 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. Вы можете задать порты, которые Kaspersky Endpoint Security будет контролировать, или выбрать все порты.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений.

При попытке пользователя открыть вредоносный или фишинговый веб-сайт, Kaspersky Endpoint Security заблокирует доступ и покажет предупреждение (см. рис. ниже).



Сообщение о запрете доступа к веб-сайту

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 Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в программе, 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.

Чтобы включить или выключить компонент Защита от веб-угроз выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **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 программы, а также выполняет максимально глубокий эвристический анализ.

- **Рекомендуемый**. Уровень безопасности веб-трафика, обеспечивающий оптимальный баланс между производительностью Kaspersky Endpoint Security и безопасностью веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на уровне **Средний**. 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 уровне **Поверхностный**.

- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента.

  Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности** в верхней части окна.

5. Сохраните внесенные изменения.

Параметры Защиты от веб-угроз, рекомендованные специалистами "Лаборатории Касперского", (рекомендованный уровень безопасности)

Параметр	Значение	Описание
Проверять ссылки по базе вредоносных веб-адресов	**Включено**	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 программы и пополняется при обновлении баз Kaspersky Endpoint Security.
Проверять веб-адрес по базе фишинговых веб-адресов	**Включено**	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 программы и пополняется при обновлении баз Kaspersky Endpoint Security.
Использовать эвристический анализ (Защита от веб-угроз)	**Средний**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "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 программ, 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)	**Включено**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

Действие при обнаружении угрозы	**Запрещать загрузку**	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.

Изменение действия над вредоносными объектами веб-трафика

По умолчанию в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и выводит на экран окно уведомления о блокировке.

Чтобы изменить действие над вредоносными объектами веб-трафика, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от веб-угроз**.
3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами веб-трафика:
   - **Запрещать загрузку**. 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.
4. Сохраните внесенные изменения.

Проверка ссылок по базам фишинговых и вредоносных веб-адресов

Проверка ссылок на принадлежность к фишинговым веб-адресам 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 тексте ICQ-сообщения, 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.

Чтобы настроить проверку компонентом Защита от веб-угроз ссылок по базам фишинговых и вредоносных веб-адресов, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от веб-угроз**.

3. Нажмите на кнопку **Расширенная настройка**.

4. Выполните следующие действия:

   - В блоке **Методы проверки** установите флажок **Проверять веб-адрес по базе вредоносных веб-адресов**, если вы хотите, чтобы компонент Защита от веб-угроз проверял ссылки по базам вредоносных веб-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 программы и пополняется при обновлении баз Kaspersky Endpoint Security.

     Kaspersky Endpoint Security проверяет все ссылки по базам вредоносных веб-адресов. Параметры проверки защищенных соединений программы 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.

   - 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 программы и пополняется при обновлении баз Kaspersky Endpoint Security.

     Для проверки ссылок вы также можете использовать репутационные базы Kaspersky Security Network.

5. Сохраните внесенные изменения.

Использование эвристического анализа в работе компонента Защита от веб-угроз

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Kaspersky Endpoint Security анализирует активность, которую программы производят в операционной системе. Эвристический анализ позволяет обнаруживать угрозы, записей о которых еще нет в базах Kaspersky Endpoint Security.

Чтобы настроить использование эвристического анализа, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от веб-угроз**.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Методы проверки** установите флажок **Использовать эвристический анализ**, если вы хотите, чтобы программа использовала эвристический анализ при проверке веб-трафика на наличие вирусов и других программ, представляющих угрозу. Далее при помощи ползунка задайте уровень эвристического анализа: **Поверхностный**, **Средний** или **Глубокий**.

5. В блоке **Анти-Фишинг** установите флажок **Использовать эвристический анализ**, если вы хотите, чтобы программа использовала эвристический анализ при проверке веб-страниц на наличие фишинговых ссылок.

6. Сохраните внесенные изменения.

Формирование списка доверенных веб-адресов

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 программ, 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.

Чтобы сформировать список доверенных веб-адресов, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .

2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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.

6. Сохраните внесенные изменения.

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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Базовая защита** → **Защита от веб-угроз**.
6. Нажмите на кнопку **Настройка**.
7. В открывшемся окне выберите закладку **Доверенные веб-адреса**.
8. 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 **Экспорт**.
   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. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список доверенных веб-адресов в XML-файл.
9. Для импорта списка доверенных адресов выполните следующие действия:
   a. Нажмите на ссылку **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных адресов.

   b. Нажмите на кнопку **Открыть**.

      Если на компьютере уже есть список доверенных адресов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
10. Сохраните внесенные изменения.

[Как экспортировать / импортировать список доверенных веб-адресов в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите экспортировать или импортировать список доверенных веб-адресов.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Базовая защита** → **Защита от веб-угроз**.
5. Для экспорта списка исключений в блоке **Доверенные веб-адреса** выполните следующие действия:
   a. Выберите доверенные веб-адреса, которые вы хотите экспортировать.
   b. Нажмите на ссылку **Экспорт**.
   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. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список доверенных веб-адресов в XML-файл.
6. Для импорта списка исключений в блоке **Доверенные веб-адреса** выполните следующие действия:
   a. Нажмите на ссылку **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных адресов.
   b. Нажмите на кнопку **Открыть**.

      Если на компьютере уже есть список доверенных адресов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
7. Сохраните внесенные изменения.

Защита от почтовых угроз

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других программ, представляющих угрозу. Также компонент проверяет сообщения на наличие вредоносных и фишинговых ссылок. По умолчанию компонент Защита от почтовых угроз постоянно находится в оперативной памяти компьютера и проверяет все сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, NNTP или в почтовом клиенте Microsoft Office Outlook (MAPI). Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Компонент Защита от почтовых угроз не проверяет сообщения, если почтовый клиент открыт в браузере.

При обнаружении вредоносного файла во вложении Kaspersky Endpoint Security меняет тему сообщения: `[Сообщение заражено] <тема сообщения>` или `[Зараженный объект удален] <тема сообщения>`.

Компонент взаимодействует с почтовыми клиентами, установленными на компьютере. Для почтового клиента Microsoft Office Outlook предусмотрено расширение с дополнительными параметрами. Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft Office Outlook во время установки Kaspersky Endpoint Security.

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 Kaspersky Endpoint Security применяет разные наборы параметров. Наборы параметров, сохраненные в программе, 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.

Чтобы включить или выключить компонент Защита от почтовых угроз выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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. Уровень безопасности почты **Высокий** 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 Kaspersky Endpoint Security 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. Уровень безопасности почты **Низкий** 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.

  Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности** в верхней части окна.

5. 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	**Включено**	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	**Включено**	Проверка архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Проверять вложенные файлы офисных форматов	**Включено**	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
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.
Эвристический анализ	**Средний**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "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 Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Endpoint Security удаляет зараженный объект. Kaspersky Endpoint Security добавит информацию о выполненном действии в тему сообщения: `[Зараженный объект удален] <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 нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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 Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Endpoint Security удаляет зараженный объект. Kaspersky Endpoint Security добавит информацию о выполненном действии в тему сообщения: `[Зараженный объект удален] <тема сообщения>`.

   - **Лечить; блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Endpoint Security добавит предупреждение к теме сообщения: `[Сообщение заражено] <тема сообщения>`. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Если вылечить объект не удалось, Kaspersky Endpoint Security блокирует отправку сообщения, почтовый клиент показывает ошибку.

- **Блокировать**. При обнаружении зараженного объекта во входящем сообщении Kaspersky Endpoint Security добавит предупреждение к теме сообщения: `[Сообщение заражено] <тема сообщения>`. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении Kaspersky Endpoint Security 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 нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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 программы 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 программу Microsoft Office Outlook.

  Снимите флажок **Подключить расширение для Microsoft Outlook**, если вы хотите закрыть доступ к настройке параметров компонента Защита от почтовых угроз из программы 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 программу 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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.
   - **Проверять вложенные архивы**. Проверка архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.

Если во время проверки приложение Kaspersky Endpoint Security 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**. 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**. 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

Функциональность фильтрации вложений не применяется для исходящих сообщений электронной почты.

Вредоносные программы 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 вредоносной программы.

Чтобы настроить фильтрацию вложений, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от почтовых угроз**.

3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Фильтр вложений** выполните одно из следующих действий:

   - Выберите вариант **Не применять фильтр**, если вы хотите, чтобы компонент Защита от почтовых угроз не фильтровал вложения в сообщениях.

   - Выберите вариант **Переименовывать вложения указанных типов**, если вы хотите, чтобы компонент Защита от почтовых угроз изменял названия вложенных в сообщения файлов указанных типов.

   - Выберите вариант **Удалять вложения указанных типов**, если вы хотите, чтобы компонент Защита от почтовых угроз удалял вложенные в сообщения 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Базовая защита** → **Защита от почтовых угроз**.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
7. В открывшемся окне выберите закладку **Фильтр вложений**.
8. 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. Нажмите на кнопку **Сохранить**.
      Kaspersky Endpoint Security экспортирует список расширений в XML-файл.
9. 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. Нажмите на кнопку **Открыть**.
      Если на компьютере уже есть список расширений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
10. Сохраните внесенные изменения.

[Как экспортировать / импортировать список расширений для работы фильтра вложений в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите экспортировать или импортировать список исключений.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Базовая защита** → **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. Нажмите на кнопку **Сохранить**.

      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. Нажмите на кнопку **Открыть**.

      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.

Проверка почты в Microsoft Office Outlook

Во время установки Kaspersky Endpoint Security в программу Microsoft Office Outlook (далее также "Outlook") встраивается расширение компонента Защита от почтовых угроз. Оно позволяет перейти к настройке параметров компонента Защита от почтовых угроз из программы Outlook, а также указать, в какой момент проверять сообщения электронной почты на присутствие вирусов и других программ, представляющих угрозу. Расширение компонента Защита от почтовых угроз для Outlook может проверять входящие и исходящие сообщения, переданные по протоколам POP3, SMTP, NNTP, IMAP и MAPI. Также Kaspersky Endpoint Security поддерживает работу с другими почтовыми клиентами (в том числе с Microsoft Outlook Express®, Windows Mail и Mozilla™ Thunderbird™).

Расширение компонента Защита от почтовых угроз поддерживает работу с Outlook 2010, 2013, 2016, 2019.

Работая с почтовым клиентом Mozilla Thunderbird, компонент Защита от почтовых угроз не проверяет на вирусы и другие программы, представляющие угрозу, сообщения, передаваемые по протоколу IMAP, в случае если используются фильтры, перемещающие сообщения из папки **Входящие**.

В программе Outlook входящие сообщения сначала проверяет компонент Защита от почтовых угроз (если в интерфейсе программы 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 программы Outlook доступна в том случае, если в интерфейсе программы Kaspersky Endpoint Security подключено расширения для Microsoft 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 рекомендациях по его использованию вы можете найти в базе знаний Microsoft.

Чтобы настроить режим работы расширения компонента Защита от почтовых угроз для Outlook с помощью Kaspersky Security Center, выполните следующие действия:

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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Базовая защита** → **Защита от почтовых угроз**.
6. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от почтовых угроз**.
7. В блоке **Встраивание в систему** 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. Сохраните внесенные изменения.

Защита от сетевых угроз

Компонент Защита от сетевых угроз (англ. IDS – Intrusion Detection System) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Endpoint Security блокирует сетевое соединение с атакующим компьютером.

Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах Kaspersky Endpoint Security. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей программы.

Включение и выключение Защиты от сетевых угроз

По умолчанию Защита от сетевых угроз включена и работает в оптимальном режиме. При необходимости вы можете выключить Защиту от сетевых угроз.

Чтобы включить или выключить Защиту от сетевых угроз, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Защита от сетевых угроз**.
3. Используйте переключатель **Защита от сетевых угроз**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Защита от сетевых угроз включена, Kaspersky Endpoint Security отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Endpoint Security блокирует сетевое соединение с атакующим компьютером.

Блокирование атакующего компьютера

Чтобы заблокировать атакующий компьютер, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Защита от сетевых угроз**.
3. Установите флажок **Добавить атакующий компьютер в список блокирования на N минут**.

   Если флажок установлен, то 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.

   Вы можете посмотреть список блокирования в окне инструмента Мониторинг сети.

Kaspersky Endpoint Security очищает список блокирования при перезапуске программы и при изменении параметров Защиты от сетевых угроз.

4. Измените время блокирования атакующего компьютера в поле, расположенном справа от флажка **Добавить атакующий компьютер в список блокирования на N минут**.

5. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security, обнаружив попытку сетевой атаки на компьютер пользователя, блокирует все соединения с атакующим компьютером.

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.

Чтобы настроить адреса исключений из блокирования, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Защита 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.

6. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security не отслеживает активность от устройств из списка исключений.

Экспорт и импорт списка исключений из блокирования

Вы можете экспортировать список исключений в файл в формате 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Базовая защита** → **Защита от сетевых угроз**.
6. В блоке **Настройка защиты от сетевых угроз** нажмите на кнопку **Исключения**.
7. 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 ссылку **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. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список исключений в XML-файл.
8. 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. Нажмите на кнопку **Открыть**.

      Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
9. Сохраните внесенные изменения.

[Как экспортировать / импортировать список исключений в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите экспортировать или импортировать список исключений.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Базовая защита** → **Защита от сетевых угроз**.
5. В блоке **Параметры Защиты от сетевых угроз** нажмите на ссылку **Исключения**.

   Откроется список исключений.
6. Для экспорта списка исключений выполните следующие действия:
   a. Выберите исключения, которые вы хотите экспортировать.
   b. Нажмите на кнопку **Экспорт**.
   c. Подтвердите, что вы хотите экспортировать только выбранные исключения, или экспортируйте весь список.
   d. 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.
   e. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список исключений в XML-файл.
7. 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. Нажмите на кнопку **Открыть**.

      Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
8. Сохраните внесенные изменения.

Настройка защиты от сетевых атак 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 программы 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.

Чтобы настроить защиту от сетевых атак по типам, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Защита от сетевых угроз**.
3. Используйте переключатель **Считать атаками сканирование портов и интенсивные сетевые запросы**, чтобы включить или выключить обнаружение атак.
4. Используйте переключатель **Защита от MAC-спуфинга**.
5. В блоке **При обнаружении атаки MAC-спуфинг** выберите один из следующих вариантов:
   - **Только уведомлять**.
   - **Уведомлять и 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 программ 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 программа использует Агент администрирования. При этом Сетевой экран автоматически создает сетевые правила, необходимые для работы Агента администрирования и программы. 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 программы. 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 программ*. Используются для ограничения сетевой активности конкретной программы. Учитываются не только характеристики сетевого пакета, но и конкретная программа, которой адресован этот сетевой пакет, либо которая инициировала отправку этого сетевого пакета.

Контроль доступа программ к ресурсам операционной системы, процессам и персональным данным обеспечивает компонент Предотвращение вторжений с помощью *прав программ*.

Во время первого запуска программы Сетевой экран выполняет следующие действия:

1. Проверяет безопасность программы с помощью загруженных антивирусных баз.

2. Проверяет безопасность программы в Kaspersky Security Network.

   Для более эффективной работы Сетевого экрана вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает программу в одну из *групп доверия*: Доверенные, Слабые ограничения, Сильные ограничения, Недоверенные.

   Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля активности программ. Kaspersky Endpoint Security помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

   Kaspersky Endpoint Security помещает программу 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 программу в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации программы от KSN группа доверия может быть изменена автоматически.

4. Блокирует сетевую активность программы в зависимости от группы доверия. Например, программам из группы доверия "Сильные ограничения" запрещены любые сетевые соединения.

При следующем запуске программы Kaspersky Endpoint Security проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие сетевые правила. Если программа была изменена, Kaspersky Endpoint Security исследует программу 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 программ. Если для одного и того же вида сетевой активности заданы и сетевые пакетные правила, и сетевые правила программ, то эта сетевая активность обрабатывается по сетевым пакетным правилам.

Сетевые правила программ имеют особенность. Сетевые правило программ включает в себя правила доступа по статусу сети: *публичная*, *локальная*, *доверенная*. Например, для группы доверия "Сильные ограничения" по умолчанию запрещена любая сетевая активность программы в сетях всех статусов. Если для отдельной программы (родительская программа) задано сетевое правило, то дочерние процессы других программ будут выполнены в соответствии с сетевым правилом родительской программы. Если сетевое правило для программы отсутствует, дочерние процессы будут выполнены в соответствии с правилом доступа к сетям группы доверия.

Например, вы запретили любую сетевую активность всех программ для сетей всех статусов, кроме браузера X. Если в браузере X (родительская программа) 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.

Статусы сетевых соединений

Сетевой экран позволяет контролировать сетевую активность в зависимости от статуса сетевого соединения. Kaspersky Endpoint Security получает статус сетевого соединения от операционной системы компьютера. Статус сетевого соединения в операционной системе задает пользователь при настройке подключения. Вы можете изменить статус сетевого соединения в параметрах Kaspersky Endpoint Security. Сетевой экран будет контролировать сетевую активность в зависимости от статуса сети в параметрах Kaspersky Endpoint Security, а не операционной системы.

Выделены следующие статусы сетевого соединения:

- **Публичная сеть**. Сеть не защищена антивирусными программами, 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 каждой программы в соответствии с сетевыми правилами этой программы.

  Сетевой экран по умолчанию присваивает статус *Публичная сеть* сети Интернет. Вы не можете изменить статус 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.

Включение и выключение Сетевого экрана

По умолчанию Сетевой экран включен и работает в оптимальном режиме.

Чтобы включить или выключить Сетевой экран выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Базовая защита → Сетевой экран**.

3. Используйте переключатель **Сетевой экран**, чтобы включить или выключить компонент.

4. Сохраните внесенные изменения.

Изменение статуса сетевого соединения

Сетевой экран по умолчанию присваивает статус *Публичная сеть* сети Интернет. Вы не можете изменить статус сети Интернет.

Чтобы изменить статус сетевого соединения, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Базовая защита → Сетевой экран**.

3. Нажмите на кнопку **Доступные сети**.

4. Выберите сетевое соединение, статус которого вы хотите изменить.

5. В графе **Тип сети** выберите статус сетевого соединения:

   - **Публичная сеть**. Сеть не защищена антивирусными программами, 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 каждой программы в соответствии с сетевыми правилами этой программы.

   - **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

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 программы.

- 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 пакетные правила, следует помнить, что они имеют приоритет над сетевыми правилами программ.

Как создать сетевое пакетное правило в интерфейсе программы с помощью инструмента Мониторинг сети

1. В главном окне программы нажмите на кнопку **Больше функций → Мониторинг сети**.
2. Перейдите на закладку **Сетевая активность**.

   На закладке **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 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 в отчет**, 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 программы в параметрах Сетевого экрана

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Сетевой экран**.
3. Нажмите на кнопку **Пакетные правила**.

   Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.
4. Нажмите на кнопку **Добавить**.

   Откроются свойства сетевого правила.
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 в отчет**, 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Базовая защита** → **Сетевой экран**.
6. В блоке **Настройки Сетевого экрана** нажмите на кнопку **Настройка**.

   Откроются список сетевых пакетных правил и список сетевых правил программ.
7. Перейдите на закладку **Сетевые пакетные правила**.

   Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.
8. Нажмите на кнопку **Добавить**.

   Откроются свойства пакетного правила.
9. В поле **Название** введите название сетевой службы вручную.
10. 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.
11. Установите флажок **Записывать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете.
12. Нажмите на кнопку **Сохранить**.

    Новое сетевое правило будет добавлено в список.
13. Кнопками **Вверх** / **Вниз** установите приоритет сетевого правила.
14. 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 и Cloud Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Базовая защита** → **Сетевой экран**.
5. В блоке **Настройки Сетевого экрана** нажмите на ссылку **Сетевые пакетные правила**.

   Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.
6. Нажмите на кнопку **Добавить**.

   Откроются свойства пакетного правила.
7. В поле **Название** введите название сетевой службы вручную.
8. Настройте параметры сетевого правила (см. таблицу ниже).

   Вы можете выбрать предустановленный шаблон правила по ссылку **Выбрать шаблон**. 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. Нажмите на кнопку **Сохранить**.

    Новое сетевое правило будет добавлено в список.
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. Используйте переключатель в графе **Статус**, чтобы включить или выключить пакетное правило.

Параметры сетевого пакетного правила

Параметр	Описание
Действие	**Разрешать**. **Запрещать**. **По правилам программы**. Если выбран этот элемент, Сетевой экран применяет к сетевому соединению сетевые правила программы.
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 через запятую указать номера портов компьютера пользователя и удаленного компьютера, соединение между которыми следует контролировать.

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 как к входящему, так и к исходящему сетевому пакету, независимо от того, компьютер пользователя или удаленный компьютер инициировал сетевое соединение. **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. Протокол TCP устанавливает соединение. Для TCP используйте направления **Входящие**, **Исходящие** и **Входящие / Исходящие**. Остальные протоколы не устанавливают соединения, а отправляют пакеты. Для остальных протоколов используйте направления **Входящие (пакет)**, **Исходящие (пакеты)** и **Входящие / Исходящие**.
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. TTL, Time to Live).
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 или выбрать подсеть (Доверенные сети, Локальные сети, Публичные сети).
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 или создать отдельный список IP-адресов. Для программ 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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 программы**.
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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → 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. С помощью кнопок **Вверх** и **Вниз** переместите сетевое пакетное правило на нужную позицию в списке сетевых пакетных правил.

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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Базовая защита** → **Сетевой экран**.
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 **Экспорт**.
   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. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл.
7. Для импорта списка сетевых пакетных правил выполните следующие действия:
   a. Нажмите на ссылку **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

   b. Нажмите на кнопку **Открыть**.

      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 **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите экспортировать или импортировать список правил.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Базовая защита** → **Сетевой экран**.
5. Перейдите по ссылке **Сетевые пакетные правила**.
6. Для экспорта списка сетевых пакетных правил выполните следующие действия:
   a. Выберите правила, которые вы хотите экспортировать.
   b. Нажмите на кнопку **Экспорт**.
   c. Подтвердите, что вы хотите экспортировать только выбранные правила, или экспортируйте весь список.
   d. Нажмите на кнопку **Экспорт**.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл в папку для загрузки по умолчанию.
7. Для импорта списка сетевых пакетных правил выполните следующие действия:
   a. Нажмите на ссылку **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.
   b. Нажмите на кнопку **Открыть**.

      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.

Работа с сетевыми правилами программ

Kaspersky Endpoint Security по умолчанию группирует все программы, установленные на компьютере пользователя, по названию производителей программного обеспечения, файловую и сетевую активность которого он контролирует. Группы программ, в свою очередь, сгруппированы в группы доверия. Все программы и группы программ наследуют свойства своей родительской группы: правила контроля программ, сетевые правила программы, а также приоритет их выполнения.

Как и компонент Предотвращение вторжений, компонент Сетевой экран по умолчанию применяет сетевые правила группы программ для фильтрации сетевой активности всех помещенных в группу программ. Сетевые правила группы программ определяют, какими правами доступа к различным сетевым соединениям обладают программы, входящие в эту группу.

Сетевой экран по умолчанию создает набор сетевых правил для каждой группы программ, которые Kaspersky Endpoint Security обнаружил на компьютере. Вы можете изменить действие Сетевого экрана для сетевых правил группы программ, созданных по умолчанию. Вы не можете изменить, удалить или выключить сетевые правила группы программ, созданные по умолчанию, а также изменить их приоритет.

Вы также можете создать сетевое правило для отдельной программы. Такое правило будет иметь более высокий приоритет, чем сетевое правило группы, в которую входит эта программа.

Создание сетевого правила программы

По умолчанию для контроля работы программы применяются сетевые правила, определенные для той группы доверия, в которую Kaspersky Endpoint Security поместил программу при первом ее запуске. При необходимости вы можете создать сетевые правила для всей группы доверия, для отдельной программы или группы программ внутри группы доверия.

Сетевые правила, заданные вручную, имеют более высокий приоритет, чем сетевые правила, определенные для группы доверия. То есть, если правила программы, заданные вручную, отличаются от правил программ, определенных для группы доверия, Сетевой экран контролирует работу программы в соответствии с правилами программ, заданными вручную.

Сетевой экран по умолчанию создает следующие сетевые правила для каждой программы:

- Любая сетевая активность в Доверенных сетях.
- Любая сетевая активность в Локальных сетях.
- Любая сетевая активность в Публичных сетях.

Kaspersky Endpoint Security контролирует сетевую активность программ по предустановленным сетевым правилам следующим образом:

- "Доверенные" и "Слабые ограничения" – любая сетевая активность разрешена.
- "Сильные ограничения" и "Недоверенные" – любая сетевая активность запрещена.

Предустановленные правила программ невозможно изменить или удалить.

Вы можете создать сетевое правило программы 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 программы.

- 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 программ, следует помнить, что сетевые пакетные правила имеют приоритет над сетевыми правилами программ.

Как создать сетевое правило программы в интерфейсе программы с помощью инструмента Мониторинг сети

1. В главном окне программы нажмите на кнопку **Больше функций** → **Мониторинг сети**.
2. Перейдите на закладку **Сетевая активность** или **Открытые порты**.

   На закладке **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 закладке **Открытые порты** перечислены все открытые сетевые порты на компьютере пользователя.
3. В контекстном меню сетевого соединения выберите пункт **Создать правило программы**.

   Откроется окно свойств и правил программы.
4. Выберите закладку **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 в отчет**, 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 программы в интерфейсе программы в параметрах Сетевого экрана

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Сетевой экран**.
3. Нажмите на кнопку **Правила программ**.

   Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.
4. В списке программ выберите программу или группу программ, для которой вы хотите создать сетевое правило.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Подробности и правила**.

   Откроется окно свойств и правил программы.
6. Выберите закладку **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 в отчет**, 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 программы 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Базовая защита** → **Сетевой экран**.
6. В блоке **Настройки Сетевого экрана** нажмите на кнопку **Настройка**.

   Откроются список сетевых пакетных правил и список сетевых правил программ.
7. Перейдите на закладку **Сетевые правила программ**.
8. Нажмите на кнопку **Добавить**.
9. В открывшемся окне задайте параметры поиска программы, для которой вы хотите создать сетевое правило.

   Вы можете ввести название программы или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.
10. Нажмите на кнопку **Обновить**.

    Kaspersky Endpoint Security выполнит поиск программы в консолидированном списке программ, установленных на управляемых компьютерах. Kaspersky Endpoint Security покажет список программ, которые удовлетворяют параметрам поиска.
11. Выберите нужную программу.
12. В раскрывающемся списке **Добавить выделенные программы в группу <группа доверия>** выберите пункт **Исходные группы** и нажмите на кнопку **ОК**.

    Программа будет добавлена в исходную группу.
13. Выберите нужную программу и в контекстном меню программы выберите пункт **Права программы**.

    Откроется окно свойств и правил программы.
14. Выберите закладку **Сетевые правила**.

    Откроется список сетевых правил, установленных Сетевым экраном по умолчанию.
15. Нажмите на кнопку **Добавить**.

    Откроются свойства сетевого правила.
16. В поле **Название** введите название сетевой службы вручную.
17. 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.
18. Установите флажок **Записывать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете.

19. Нажмите на кнопку **Сохранить**.

    Новое сетевое правило будет добавлено в список.

20. Кнопками **Вверх** / **Вниз** установите приоритет сетевого правила.

21. Сохраните внесенные изменения.

[Как создать сетевое правило программы в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Базовая защита** → **Сетевой экран**.
5. В блоке **Настройки Сетевого экрана** нажмите на ссылку **Сетевые правила программ**.

   Откроется окно настройки прав программ и список защищаемых ресурсов.
6. Перейдите на закладку **Права программ**.

   Откроется список групп доверия в левой части окна и их свойства в правой части.
7. Нажмите на кнопку **Добавить**.

   Запустится мастер добавления программы в группу доверия.
8. По ссылке **Выбранная целевая группа** выберите группу доверия, в которую вы хотите поместить программу.
9. Выберите тип **Программа**. Нажмите на кнопку **Далее**.

   Если вы хотите создать сетевое правило для нескольких программ, выберите тип **Группа** и задайте имя группы программ.
10. В открывшемся списке программ выберите программы, для которых вы хотите создать сетевое правило.

    Используйте фильтр. Вы можете ввести название программы или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
11. Завершите работу мастера по кнопке **ОК**.

    Программа будет добавлена в группу доверия.
12. В левой части окна выберите нужную программу.
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 программы.
15. В поле **Название** введите название сетевой службы вручную.
16. Настройте параметры сетевого правила (см. таблицу ниже).

    Вы можете выбрать предустановленный шаблон правила по ссылку **Выбрать шаблон**. 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. Нажмите на кнопку **Сохранить**.

    Новое сетевое правило будет добавлено в список.

19. Кнопками **Вверх** / **Вниз** установите приоритет сетевого правила.

20. Сохраните внесенные изменения.

Параметры сетевого правила программы

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 через запятую указать номера портов компьютера пользователя и удаленного компьютера, соединение между которыми следует контролировать.
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 или выбрать подсеть (Доверенные сети, Локальные сети, Публичные сети).
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 или создать отдельный список IP-адресов. Для программ не всегда возможно получить локальный адрес. В этом случае этот параметр игнорируется.

Включение и выключение сетевого правила программ

Чтобы включить или выключить сетевое правило программ, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Базовая защита → Сетевой экран**.

3. Нажмите на кнопку **Правила программ**.

   Откроется список правил программ.

4. В списке программ выберите программу или группу программ, 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 программы.

6. Выберите закладку **Сетевые правила**.

7. В списке сетевых правил группы программ 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 программ, если оно создано Сетевым экраном по умолчанию.

9. Сохраните внесенные изменения.

Изменение действия Сетевого экрана для сетевого правила программ

Вы можете изменить действие Сетевого экрана для всех сетевых правил программы или группы программ, которые были созданы по умолчанию, а также изменить действие Сетевого экрана для одного сетевого правила программы или группы программ, которое было создано вручную.

Чтобы изменить действие Сетевого экрана для всех сетевых правил программы или группы программ, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Базовая защита → Сетевой экран**.

3. Нажмите на кнопку **Правила программ**.

   Откроется список правил программ.

4. В списке выберите программу или группу программ, 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**.
   - **Разрешать**.
   - **Запрещать**.

6. Сохраните внесенные изменения.

Чтобы изменить действие Сетевого экрана для одного сетевого правила программы или группы программ, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Сетевой экран**.
3. Нажмите на кнопку **Правила программ**.

   Откроется список правил программ.
4. В списке выберите программу или группу программ, для которой 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 программы.
6. Выберите закладку **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.**
   - **Разрешать**.
   - **Запрещать**.
   - **Записывать в отчет**.
9. Сохраните внесенные изменения.

Изменение приоритета сетевого правила программ

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 программ, созданных по умолчанию.

Чтобы изменить приоритет сетевого правила, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Сетевой экран**.
3. Нажмите на кнопку **Правила программ**.

   Откроется список правил программ.

4. В списке программ выберите программу или группу программ, для которой 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 программы.

6. Выберите закладку **Сетевые правила**.

7. Выберите сетевое правило, приоритет которого вы хотите изменить.

8. С помощью кнопок **Вверх** и **Вниз** переместите сетевое правило на нужную позицию в списке сетевых правил.

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 программы нажмите на кнопку **Больше функций** → **Мониторинг сети**.

Откроется окно **Мониторинг сети**. В этом окне информация о сетевой активности компьютера пользователя представлена на четырех закладках:

- На закладке **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 закладке вы также можете создавать сетевые пакетные правила для работы Сетевого экрана.

- На закладке **Открытые порты** перечислены все открытые сетевые порты на компьютере пользователя. На этой закладке вы также можете создавать сетевые пакетные правила и правила программ для работы Сетевого экрана.

- На закладке **Сетевой трафик** отображается объем входящего и исходящего сетевого трафика между компьютером пользователя и другими компьютерами сети, в которой пользователь работает в текущий момент.

- На закладке **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 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 вредоносную программу.

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, программа предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) цифровой код, сформированный программой (см. рис. ниже). Эта процедура называется авторизацией клавиатуры.

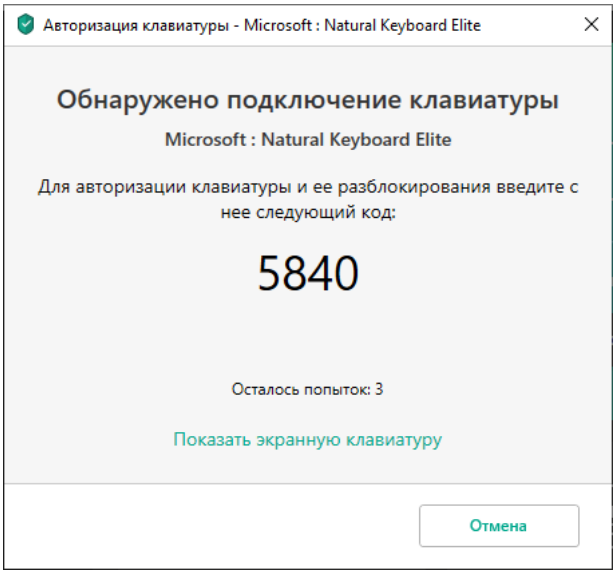
Если код введен правильно, программа сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется.

При подключении авторизованной клавиатуры через другой USB-порт компьютера программа снова запрашивает ее авторизацию.

Если цифровой код введен неправильно, программа формирует новый. Число попыток для ввода цифрового кода равно трем. Если цифровой код введен неправильно трижды или закрыто окно **Авторизация клавиатуры <Название клавиатуры>**, программа блокирует ввод с этой клавиатуры. При повторном подключении клавиатуры или перезагрузке операционной системы программа снова предлагает пройти авторизацию клавиатуры.

Программа разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.

Компонент Защита от атак BadUSB не устанавливается по умолчанию. Если вам нужен компонент Защита от атак BadUSB, вы можете добавить компонент в свойствах инсталляционного пакета перед установкой программы или измените состав компонентов программы после установки программы.



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.

Чтобы включить или выключить Защиту от атак BadUSB, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от атак BadUSB**.
3. Используйте переключатель **Защита от атак BadUSB**, чтобы включить или выключить компонент.
4. 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.

Использовании экранной клавиатуры при авторизации USB-устройств

Возможность использовать экранную клавиатуру предназначена только для авторизации USB-устройств, не поддерживающих произвольный ввод символов (например, сканеров штрих-кодов). Не рекомендуется использовать экранную клавиатуру для авторизации неизвестных вам USB-устройств.

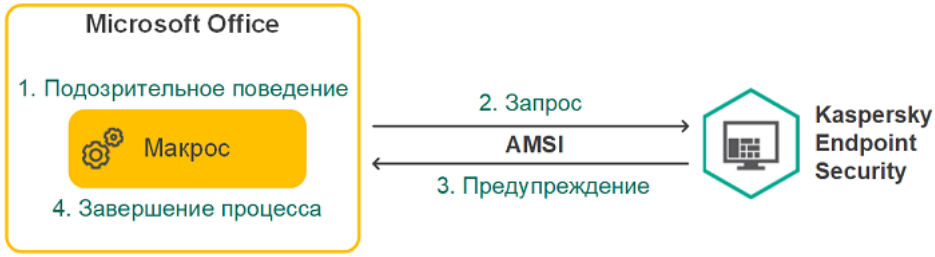
Чтобы разрешить или запретить использование экранной клавиатуры при авторизации, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от атак BadUSB**.
3. Используйте флажок **Запретить использование экранной клавиатуры для авторизации USB-устройств**, чтобы запретить или разрешить использование экранной клавиатуры для авторизации.
4. Сохраните внесенные изменения.

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, программы 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 установлен флажок **Не блокировать взаимодействие с AMSI-защитой**.

AMSI-защита доступна для следующих операционных систем рабочих станций и серверов:

- Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

Включение и выключение AMSI-защиты

По умолчанию AMSI-защита включена.

Чтобы включить или выключить AMSI-защиту, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → AMSI-защита**.
3. Используйте переключатель **AMSI-защита**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

Проверка составных файлов AMSI-защитой

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы. Чтобы обнаружить скрытые таким образом вирусы и другие программы, 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.

Чтобы настроить проверку составных файлов AMSI-защитой, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → AMSI-защита**.
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 в поле **Максимальный**

размер файла 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 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 уязвимую программу. При обработке этих данных уязвимая программа выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО.

Если попытка запустить исполняемый файл из уязвимой программы не была произведена пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла или информирует пользователя.

Включение и выключение Защиты от эксплойтов

По умолчанию Защита от эксплойтов включена и работает в режиме, рекомендованном специалистами "Лаборатории Касперского". Вы можете выключить Защиту от эксплойтов при необходимости.

Чтобы включить или выключить Защиту от эксплойтов, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Продвинутая защита → Защита от эксплойтов**.
3. Используйте переключатель **Защита от эксплойтов**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Защита от эксплойтов включена, Kaspersky Endpoint Security будет отслеживать исполняемые файлы, запускаемые уязвимыми программами. Если Kaspersky Endpoint Security обнаруживает, что исполняемый файл из уязвимой программы был запущен не пользователем, то Kaspersky Endpoint Security выполняет выбранное действие (например, блокирует операцию).

Выбор действия при обнаружении эксплойта

По умолчанию, обнаружив эксплойт, Kaspersky Endpoint Security блокирует операции этого эксплойта.

Чтобы выбрать действие при обнаружении эксплойта, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Продвинутая защита → Защита от эксплойтов**.
3. В блоке **При обнаружении эксплойта** выберите нужное действие:
   - **Блокировать операцию**. 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.
4. Сохраните внесенные изменения.

Защита памяти системных процессов

По умолчанию защита памяти системных процессов включена.

Чтобы включить или выключить защиту памяти системных процессов, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Продвинутая защита → Защита от эксплойтов**.
3. Используйте переключатель **Включить защиту памяти системных процессов**, чтобы включить или выключить функцию.
4. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет блокировать сторонние процессы, осуществляющие попытки доступа к системным процессам.

Анализ поведения

Компонент Анализ поведения получает данные о действиях программ на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы.

Компонент Анализ поведения использует шаблоны опасного поведения программ. Если активность программы 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.

Включение и выключение Анализа поведения

По умолчанию Анализ поведения включен и работает в режиме, рекомендованном специалистами "Лаборатории Касперского". Вы можете выключить Анализ поведения при необходимости.

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.

Чтобы включить или выключить Анализ поведения, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Анализ поведения**.
3. Используйте переключатель **Анализ поведения**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Анализ поведения включен, Kaspersky Endpoint Security будет анализировать активность программ в операционной системе, используя шаблоны опасного поведения.

Выбор действия при обнаружении вредоносной активности программы

Чтобы выбрать действие при обнаружении вредоносной активности программы, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Анализ поведения**.
3. В блоке **При обнаружении вредоносной активности программы** выберите нужное действие:
   - **Удалять файл**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security удаляет исполняемый файл вредоносной программы и создает резервную копию файла в резервном хранилище.
   - **Завершать работу программы**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security завершает работу этой программы.
   - **Информировать**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security добавляет информацию о вредоносной активности этой программы в список активных угроз.
4. Сохраните внесенные изменения.

Защита папок общего доступа от внешнего шифрования

Компонент обеспечивает отслеживание операций только над теми файлами, которые расположены на запоминающих устройствах с файловой системой NTFS и не зашифрованы системой EFS.

Функция защиты папок общего доступа от внешнего 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.

По умолчанию защита папок общего доступа от внешнего шифрования выключена.

После установки Kaspersky Endpoint Security функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки компьютера.

Включение и выключение защиты папок общего доступа от внешнего шифрования

После установки Kaspersky Endpoint Security функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки компьютера.

Чтобы включить или выключить защиту папок общего доступа от внешнего шифрования, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Анализ поведения**.
3. Используйте переключатель **Включить защиту папок общего доступа от внешнего шифрования**, чтобы включить или выключить анализ активности, характерную для внешнего шифрования.
4. Сохраните внесенные изменения.

Выбор действия при обнаружении внешнего шифрования папок общего доступа

Чтобы выбрать действие при обнаружении внешнего шифрования папок общего доступа, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Анализ поведения**.
3. В блоке **Защита папок общего доступа от внешнего шифрования** выберите нужное действие:
   - **Блокировать соединение на N мин**. Если выбран этот вариант, то при обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security выполняет следующие действия:
     - блокирует сетевую активность компьютера, осуществляющего изменение;
     - создает резервные копии подверженных изменению файлов;

- добавляет запись в отчеты локального интерфейса программы;
- 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.

- **Информировать**. Если выбран этот вариант, то при обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security выполняет следующие действия:
  - добавляет запись в отчеты локального интерфейса программы;
  - добавляет запись в список активных угроз;
  - отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.

4. Сохраните внесенные изменения.

Создание исключения для защиты папок общего доступа от внешнего шифрования

Исключение папки 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.

Как создать исключение для защиты папок общего доступа 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Общие настройки** → **Исключения**.
6. В блоке **Исключения из проверки и доверенные приложения** нажмите на кнопку **Настройка**.
7. В открывшемся окне выберите закладку **Исключения из проверки**.

   Откроется окно со списком исключений.
8. 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.
9. Установите флажок **Разрешить использование локальных доверенных программ**, 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. Если локальный список сформирован, после выключения функции Kaspersky Endpoint Security продолжает исключать из проверки файлы из списка.
10. Нажмите на кнопку **Добавить**.
11. В блоке **Свойства** установите флажок **Файл или папка**.
12. 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**.
13. 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.

14. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

15. По ссылке **любые**, расположенной в блоке **Описание исключения из проверки (нажмите на подчеркнутые элементы для их изменения)**, активируйте ссылку **выберите компоненты**.

16. По ссылке **выберите компоненты** откройте окно **Компоненты защиты**.

17. Установите флажок напротив компонента **Анализ поведения**.

18. Сохраните внесенные изменения.

[Как создать исключение для защиты папок общего доступа в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Общие настройки** → **Исключения**.
5. В блоке **Исключения из проверки и доверенные программы** перейдите по ссылке **Исключения из проверки**.
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 доверенных программ**, 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. Если локальный список сформирован, после выключения функции Kaspersky Endpoint Security продолжает исключать из проверки файлы из списка.
8. Нажмите на кнопку **Добавить**.
9. Выберите способ добавления исключения **Файл или папка**.
10. 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.
11. В блоке **Компоненты защиты** выберите компонент **Анализ поведения**.

12. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.
13. Установите статус для исключения **Активно**.

    Вы можете в любое время остановить работу исключения с помощью переключателя.
14. Сохраните внесенные изменения.

Как создать исключение для защиты папок общего доступа в интерфейсе приложения

1. В главном окне приложения нажмите на кнопку ⚙.
2. В окне параметров приложения выберите раздел **Общие настройки** → **Угрозы и исключения**.
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.
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.

Настройка адресов исключений из защиты папок общего доступа от внешнего шифрования

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.

Чтобы исключить из защиты удаленные компьютеры, осуществляющие внешнее шифрование папок общего доступа, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Анализ поведения**.
3. В блоке **Исключения** перейдите по ссылке **Настройка адресов исключений**.
4. Если вы хотите добавить IP-адрес или имя компьютера в список исключений, нажмите на кнопку **Добавить**.
5. Введите IP-адрес компьютера или имя компьютера, попытки внешнего шифрования с которого не должны обрабатываться.
6. Сохраните внесенные изменения.

Экспорт и импорт списка исключений из защиты папок общего доступа от внешнего шифрования

Вы можете экспортировать список исключений в файл в формате 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Продвинутая защита** → **Анализ поведения**.
6. В блоке **Защита папок общего доступа от внешнего шифрования** нажмите на кнопку **Исключения**.
7. 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 ссылку **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. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список исключений в XML-файл.
8. 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. Нажмите на кнопку **Открыть**.

      Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
9. Сохраните внесенные изменения.

[Как экспортировать / импортировать список исключений в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите экспортировать или импортировать список исключений.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита** → **Анализ поведения**.
5. Для экспорта списка исключений, в блоке **Исключения** выполните следующие действия:
   a. Выберите исключения, которые вы хотите экспортировать.
   b. Нажмите на кнопку **Экспорт**.
   c. Подтвердите, что вы хотите экспортировать только выбранные исключения, или экспортируйте весь список.
   d. 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.
   e. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список исключений в XML-файл.
6. Для импорта списка исключений, в блоке **Исключения** выполните следующие действия:
   a. Нажмите на кнопку **Импорт**.
   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.
   c. Нажмите на кнопку **Открыть**.

      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.

Предотвращение вторжений

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Предотвращение вторжений (англ. HIPS – Host Intrusion Prevention System) предотвращает выполнение программами 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 программ с помощью *прав программ*. Права программ включают в себя следующие параметры доступа:

- доступ к ресурсам операционной системы (например, параметры автозапуска, ключи реестра);
- доступ к персональным данным (например, к файлам, программам).

Сетевую активность программ контролирует Сетевой экран с помощью *сетевых правил*.

Во время первого запуска программы компонент Предотвращение вторжений выполняет следующие действия:

1. Проверяет безопасность программы с помощью загруженных антивирусных баз.
2. Проверяет безопасность программы в Kaspersky Security Network.

   Для более эффективной работы компонента Предотвращение вторжений вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает программу в одну из *групп доверия*: Доверенные, Слабые ограничения, Сильные ограничения, Недоверенные.

   Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля активности программ. Kaspersky Endpoint Security помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

   Kaspersky Endpoint Security помещает программу 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 программу в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации программы от KSN группа доверия может быть изменена автоматически.

4. Блокирует действия программы в зависимости от группы доверия. Например, программам из группы доверия "Сильные ограничения" запрещен доступ к модулям операционной системы.

При следующем запуске программы Kaspersky Endpoint Security проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие права программ. Если программа была изменена, Kaspersky Endpoint Security исследует программу 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Продвинутая защита** → **Предотвращение вторжений**.
6. Используйте флажок **Предотвращение вторжений**, чтобы включить или выключить компонент.
7. Сохраните внесенные изменения.

Как включить или выключить компонент Предотвращение вторжений в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита** → **Предотвращение вторжений**.
5. Используйте переключатель **Предотвращение вторжений**, чтобы включить или выключить компонент.
6. Сохраните внесенные изменения.

Как включить или выключить компонент Предотвращение вторжений в интерфейсе программы

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **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 программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера. Далее Kaspersky Endpoint Security будет блокировать действия программы в зависимости от группы доверия.

Работа с группами доверия программ

Во время первого запуска каждой программы компонент Предотвращение вторжений проверяет безопасность программы и помещает программу в одну из групп доверия.

На первом этапе проверки программы Kaspersky Endpoint Security ищет запись о программе во внутренней базе известных программ 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 программа помещается в группу доверия. При каждом повторном запуске программы Kaspersky Endpoint Security отправляет новый запрос в базу KSN и перемещает программу в другую группу доверия, если репутация программы в базе KSN изменилась.

Вы можете выбрать группу доверия, в которую Kaspersky Endpoint Security должен автоматически помещать все неизвестные программы. Программы, которые были запущены до Kaspersky Endpoint Security, автоматически помещаются в группу доверия, установленную в параметрах компонента Предотвращение вторжений.

Для программ, запущенных до Kaspersky Endpoint Security, контролируется только сетевая активность. Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана.

Изменение группы доверия для программы

Во время первого запуска каждой программы компонент Предотвращение вторжений проверяет безопасность программы и помещает программу в одну из групп доверия.

Специалисты "Лаборатории Касперского" не рекомендуют перемещать программы из группы доверия, определенной автоматически, в другую группу доверия. Вместо этого при необходимости измените права отдельной программы.

Как изменить группу доверия для программы 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Продвинутая защита** → **Предотвращение вторжений**.
6. В блоке **Права программ** нажмите на кнопку **Настройка**.

   Откроется окно настройки прав программ и список защищаемых ресурсов.
7. Перейдите на закладку **Права программ**.
8. Нажмите на кнопку **Добавить**.
9. В открывшемся окне задайте параметры поиска программы, для которой вы хотите изменить группу доверия.

   Вы можете ввести название программы или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
10. Нажмите на кнопку **Обновить**.

    Kaspersky Endpoint Security выполнит поиск программы в консолидированном списке программ, установленных на управляемых компьютерах. Kaspersky Endpoint Security покажет список программ, которые удовлетворяют параметрам поиска.
11. Выберите нужную программу.
12. В раскрывающемся списке **Добавить выделенные программы в группу <группа доверия>** выберите нужную группу доверия для программы.
13. Сохраните внесенные изменения.

Как изменить группу доверия для программы в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита** → **Предотвращение вторжений**.
5. В блоке **Права программ и защищаемые ресурсы** нажмите на ссылку **Права программ и защищаемые ресурсы**.

   Откроется окно настройки прав программ и список защищаемых ресурсов.
6. Перейдите на закладку **Права программ**.

   Откроется список групп доверия в левой части окна и их свойства в правой части.
7. Нажмите на кнопку **Добавить**.

   Запустится мастер добавления программы в группу доверия.
8. По ссылке **Выбранная целевая группа** выберите группу доверия, в которую вы хотите поместить программу.
9. Выберите тип **Программа**. Нажмите на кнопку **Далее**.

   Если вы хотите изменить группу доверия для нескольких программ, выберите тип **Группа** и задайте имя группы программ.
10. В открывшемся списке программ выберите программы, для которых вы хотите изменить группу доверия.

    Используйте фильтр. Вы можете ввести название программы или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
11. Завершите работу мастера по кнопке **OK**.

    Программа будет добавлена в группу доверия.
12. Сохраните внесенные изменения.

[Как изменить группу доверия для программы в интерфейсе программы]

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление программами**.

   Откроется список установленных программ.
4. Выберите нужную программу.
5. В контекстном меню программы выберите пункт **Ограничения** → <группа доверия>.
6. Сохраните внесенные изменения.

В результате программа будет перемещена в другую группу доверия. Далее Kaspersky Endpoint Security будет блокировать действия программы в зависимости от группы доверия. Программе будет присвоен статус *(задано пользователем)*. При изменении репутации программы в Kaspersky Security Network компонент Предотвращение вторжений оставит группу доверия для этой программы без изменений.

Настройка прав группы доверия

По умолчанию для разных групп доверия созданы оптимальные права программ. Параметры прав групп программ, входящих в группу доверия, наследуют значения параметров прав групп доверия.

Как изменить права группы доверия 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Продвинутая защита** → **Предотвращение вторжений**.
6. В блоке **Права программ** нажмите на кнопку **Настройка**.

   Откроется окно настройки прав программ и список защищаемых ресурсов.
7. Перейдите на закладку **Права программ**.
8. Выберите нужную группу доверия.
9. В контекстном меню группы доверия выберите пункт **Права группы**.

   Откроются свойства группы доверия.
10. Выполните одно из следующих действий:

    - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами программ.
    - Выберите закладку **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

    Сетевую активность программ контролирует Сетевой экран с помощью *сетевых правил*.
11. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт: **Наследовать**, **Разрешать** (✓) или **Запрещать** (⊘).
12. 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 программой операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о программах, которые используют каждый ресурс.
13. Сохраните внесенные изменения.

Как изменить права группы доверия в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита** → **Предотвращение вторжений**.
5. В блоке **Права программ и защищаемые ресурсы** нажмите на ссылку **Права программ и защищаемые ресурсы**.

   Откроется окно настройки прав программ и список защищаемых ресурсов.
6. Перейдите на закладку **Права программ**.

   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 программ.
   - Выберите пункт **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

   Сетевую активность программ контролирует Сетевой экран с помощью *сетевых правил*.
9. Для нужного ресурса в графе соответствующего действия выберите нужный пункт: **Наследовать**, **Разрешать** (), **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 программой операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о программах, которые используют каждый ресурс.
11. Сохраните внесенные изменения.

Как изменить права группы доверия в интерфейсе программы

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление программами**.

   Откроется список установленных программ.
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 закладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами программ.
   - Выберите закладку **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

   Сетевую активность программ 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**, **Разрешать** (), **Запрещать** ().
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 программой операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о программах, которые используют каждый ресурс.
9. Сохраните внесенные изменения.

В результате права группы доверия будут изменены. Далее Kaspersky Endpoint Security будет блокировать действия программы в зависимости от группы доверия. Группе доверия будет присвоен статус (*Настройки пользователя*).

Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security

Для программ, 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 программ, необходимо выбрать группу доверия.

Как выбрать группу доверия для программ, запускаемых до 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.
6. В блоке **Права программ** нажмите на кнопку **Изменить**.
7. Для параметра **Программы, запускаемые до Kaspersky Endpoint Security для Windows, автоматически помещаются в группу доверия: <группа доверия>** выберите нужную группу доверия.
8. Сохраните внесенные изменения.

Как выбрать группу доверия для программ, запускаемых до Kaspersky Endpoint Security, в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства → Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита → Предотвращение вторжений**.
5. Для параметра **Программы, запускаемые до Kaspersky Endpoint Security для Windows, автоматически помещаются в группу доверия: <группа доверия>** выберите нужную группу доверия.
6. Сохраните внесенные изменения.

Как выбрать группу доверия для программ, запускаемых до Kaspersky Endpoint Security, в интерфейсе программы

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. В блоке **Программы, запускаемые до Kaspersky Endpoint Security для Windows, автоматически помещаются в группу доверия: <группа доверия>** выберите нужную группу доверия.
4. Сохраните внесенные изменения.

В результате программа, запускаемая до Kaspersky Endpoint Security, будет помещена в другую группу доверия. Далее Kaspersky Endpoint Security будет блокировать действия программы в зависимости от группы доверия.

Выбор группы доверия для неизвестных программ

Во время первого запуска программы компонент Предотвращение вторжений определяет группу доверия для программы. Если у вас отсутствует доступ в интернет или в Kaspersky Security Network нет информации об этой программе, то Kaspersky Endpoint Security по умолчанию помещает программу в группу "Слабые ограничения". При обнаружении в KSN информации о ранее неизвестной программе Kaspersky Endpoint Security обновит права программы. После этого вы можете изменить права программы вручную.

Как выбрать группу доверия для неизвестных программ 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Продвинутая защита** → **Предотвращение вторжений**.
6. В блоке **Правила обработки программ** с помощью раскрывающегося списка **Группа доверия для программ, которые не удалось распределить по другим группам** выберите нужную группу доверия.

   Если участие в Kaspersky Security Network включено, Kaspersky Endpoint Security отправляет запрос о репутации программы в KSN при каждом запуске программы. На основе полученного ответа программа может быть перемещена в группу доверия, отличную от заданной в параметрах компонента Предотвращение вторжений.
7. Используйте флажок **Обновлять права для ранее неизвестных программ из базы KSN**, чтобы настроить автоматическое обновление прав неизвестных программы.
8. Сохраните внесенные изменения.

Как выбрать группу доверия для неизвестных программ в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита** → **Предотвращение вторжений**.
5. В блоке **Правила обработки программ** с помощью раскрывающегося списка **Группа доверия для программ, которые не удалось распределить по другим группам** выберите нужную группу доверия.

   Если участие в Kaspersky Security Network включено, Kaspersky Endpoint Security отправляет запрос о репутации программы в KSN при каждом запуске программы. На основе полученного ответа программа может быть перемещена в группу доверия, отличную от заданной в параметрах компонента Предотвращение вторжений.
6. Используйте флажок **Обновлять права для ранее неизвестных программ из базы KSN**, чтобы настроить автоматическое обновление прав неизвестных программы.
7. Сохраните внесенные изменения.

Как выбрать группу доверия для неизвестных программ в интерфейсе программы

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. В блоке **Группа доверия для неизвестных программ** выберите нужную группу доверия.

   Если участие в Kaspersky Security Network включено, Kaspersky Endpoint Security отправляет запрос о репутации программы в KSN при каждом запуске программы. На основе полученного ответа программа может быть перемещена в группу доверия, отличную от заданной в параметрах компонента Предотвращение вторжений.
4. Используйте флажок **Обновлять права для ранее неизвестных программ из базы KSN**, чтобы настроить автоматическое обновление прав неизвестных программы.
5. Сохраните внесенные изменения.

Выбор группы доверия для программ с цифровой подписью

Kaspersky Endpoint Security всегда помещает программы, подписанные сертификатами Microsoft или сертификатами "Лаборатории Касперского", в группу доверия "Доверенные".

Как выбрать группу доверия для программ с цифровой подписью 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.
6. В блоке **Правила обработки программ** используйте флажок **Доверять программам, имеющим цифровую подпись**, чтобы включить или выключить автоматическое перемещение программ 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 программы с цифровой подписью доверенными и распределяет их по группам доверия на основании других параметров.
7. Сохраните внесенные изменения.

Как выбрать группу доверия для программ с цифровой подписью в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства → Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита → Предотвращение вторжений**.
5. В блоке **Правила обработки программ** используйте флажок **Доверять программам, имеющим цифровую подпись**, чтобы включить или выключить автоматическое перемещение программ 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 программы с цифровой подписью доверенными и распределяет их по группам доверия на основании других параметров.
6. Сохраните внесенные изменения.

Как выбрать группу доверия для программ с цифровой подписью в интерфейсе программы

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. В блоке **Правила обработки программ** используйте флажок **Доверять программам, имеющим цифровую подпись**, чтобы включить или выключить автоматическое перемещение программ 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 программы с цифровой подписью доверенными и распределяет их по группам доверия на основании других параметров.
4. Сохраните внесенные изменения.

Работа с правами программ

По умолчанию для контроля работы программы применяются права программ, определенные для той группы доверия, в которую Kaspersky Endpoint Security поместил программу при первом ее запуске. При необходимости вы можете изменить права программ для всей группы доверия, для отдельной программы или группы программ внутри группы доверия.

Права программ, заданные вручную, имеют более высокий приоритет, чем права программ, определенные для группы доверия. То есть, если права программы, заданные вручную, отличаются от прав программ, определенных для группы доверия, компонент Предотвращение вторжения контролирует работу программы в соответствии с правами программ, заданными вручную.

Правила, которые вы создаете для программ, наследуются дочерними программами. Например, если вы запретили любую сетевую активность программе cmd.exe, этот запрет будет распространятся на программу notepad.exe, если она была запущена с помощью cmd.exe. При опосредованном запуске программы (если программа не является дочерней по отношению к программе, из которой она запускается), правила унаследованы не будут.

Как изменить права программы 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Продвинутая защита** → **Предотвращение вторжений**.
6. В блоке **Права программ** нажмите на кнопку **Настройка**.

   Откроется окно настройки прав программ и список защищаемых ресурсов.
7. Перейдите на закладку **Права программ**.
8. Нажмите на кнопку **Добавить**.
9. В открывшемся окне задайте параметры поиска программы, для которой вы хотите изменить права программы.

   Вы можете ввести название программы или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
10. Нажмите на кнопку **Обновить**.

    Kaspersky Endpoint Security выполнит поиск программы в консолидированном списке программ, установленных на управляемых компьютерах. Kaspersky Endpoint Security покажет список программ, которые удовлетворяют параметрам поиска.
11. Выберите нужную программу.
12. В раскрывающемся списке **Добавить выделенные программы в группу <группа доверия>** выберите пункт **Исходные группы** и нажмите на кнопку **ОК**.

    Программа будет добавлена в исходную группу.
13. Выберите нужную программу и в контекстном меню программы выберите пункт **Права программы**.

    Откроются свойства программы.
14. Выполните одно из следующих действий:

    - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами программ.
    - Выберите закладку **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

    Сетевую активность программ контролирует Сетевой экран с помощью *сетевых правил*.
15. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт: **Наследовать**, **Разрешать** (✓) или **Запрещать** (⊘).

16. 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 программой операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о программах, которые используют каждый ресурс.

17. Сохраните внесенные изменения.

[Как изменить права программы в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита** → **Предотвращение вторжений**.
5. В блоке **Права программ и защищаемые ресурсы** нажмите на ссылку **Права программ и защищаемые ресурсы**.

   Откроется окно настройки прав программ и список защищаемых ресурсов.
6. Перейдите на закладку **Права программ**.

   Откроется список групп доверия в левой части окна и их свойства в правой части.
7. Нажмите на кнопку **Добавить**.

   Запустится мастер добавления программы в группу доверия.
8. По ссылке **Выбранная целевая группа** выберите группу доверия, в которую вы хотите поместить программу.
9. Выберите тип **Программа**. Нажмите на кнопку **Далее**.

   Если вы хотите изменить группу доверия для нескольких программ, выберите тип **Группа** и задайте имя группы программ.
10. В открывшемся списке программ выберите программы, для которых вы хотите изменить права программы.

    Используйте фильтр. Вы можете ввести название программы или название компании производителя. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
11. Завершите работу мастера по кнопке **OK**.

    Программа будет добавлена в группу доверия.
12. В левой части окна выберите нужную программу.
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 программ.
    - Выберите пункт **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

    > Сетевую активность программ контролирует Сетевой экран с помощью *сетевых правил*.
14. Для нужного ресурса в графе соответствующего действия выберите нужный пункт: **Наследовать**, **Разрешать** (✓), **Запрещать** (✗).

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 программой операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о программах, которые используют каждый ресурс.

16. Сохраните внесенные изменения.

[Как изменить права программы в интерфейсе программы]

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление программами**.

   Откроется список установленных программ.
4. Выберите нужную программу.
5. В контекстном меню программы выберите пункт **Подробности и правила**.

   Откроются свойства программы.
6. Выполните одно из следующих действий:

   - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами программ.
   - Выберите закладку **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**, **Разрешать** (), **Запрещать** ().
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 программой операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о программах, которые используют каждый ресурс.
9. Выберите закладку **Исключения** и настройте дополнительные параметры программы (см. таблицу ниже).
10. Сохраните внесенные изменения.

Дополнительные параметры программы

Параметр	Описание
Не проверять открываемые файлы	Kaspersky Endpoint Security исключает из проверки все файлы, открываемые с помощью программы. Например, если вы используете программы резервного копирования файлов, функция позволит снизить потребление ресурсов компьютера Kaspersky Endpoint Security.
Не контролировать активные программы	Kaspersky Endpoint Security не контролирует файловую и сетевую активности программы в операционной системе. Контроль за активностью программы выполняют следующие компоненты: Анализ поведения, Защита от эксплойтов, Предотвращение вторжений, Откат вредоносных действий и Сетевой экран.
Не наследовать ограничения родительского процесса (программы)	Kaspersky Endpoint Security не применяет ограничения к процессу, которые настроены для родительского процесса. Родительский процесс запускает программа, для которой настроены права программы (Предотвращение вторжений) и сетевые правила программы (Сетевой экран).

Не контролировать активность дочерних программ	Kaspersky Endpoint Security не контролирует файловую и сетевую активности программ, которые запускает программа.
Разрешить взаимодействие с интерфейсом Kaspersky Endpoint Security	Самозащита Kaspersky Endpoint Security блокирует все попытки управления службами программы с удаленного компьютера. Если флажок установлен, то программе 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 программой. Вы можете исключить из проверки весь трафик или только зашифрованный трафик. Также вы можете исключить из проверки отдельные IP-адреса или номера портов.

Защита ресурсов ОС и персональных данных

Компонент Предотвращение вторжений управляет правами программ 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 *Параметры автозапуска*, где перечислены все ключи реестра, относящиеся к автозапуску программ. 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Продвинутая защита** → **Предотвращение вторжений**.
6. В блоке **Права программ** нажмите на кнопку **Настройка**.

   Откроется окно настройки прав программ и список защищаемых ресурсов.
7. Перейдите на закладку **Защищаемые ресурсы**.

   Откроется список защищаемых ресурсов в левой части окна и права доступа к этим ресурсам, в зависимости от группы доверия.
8. Выберите категорию защищаемых ресурсов, в которую вы хотите добавить новый защищаемый ресурс.

   Если вы хотите добавить вложенную категорию, нажмите на кнопку **Добавить** → **Категорию**.
9. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите тип ресурса, который вы хотите добавить: **Файл или папку** или **Ключ реестра**.
10. В открывшемся окне выберите файл, папку или ключ реестра.

    Вы можете посмотреть права доступа программ 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 программ на операции с ресурсами с помощью флажка рядом с новым ресурсом.
11. Сохраните внесенные изменения.

Как добавить защищаемый ресурс в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита** → **Предотвращение вторжений**.
5. В блоке **Права программ и защищаемые ресурсы** нажмите на ссылку **Права программ и защищаемые ресурсы**.

   Откроется окно настройки прав программ и список защищаемых ресурсов.
6. Перейдите на закладку **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. По ссылке **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 папку** или **Ключ реестра**.
10. Выберите файл, папку или ключ реестра.
11. Завершите работу мастера по кнопке **OK**.

    Вы можете посмотреть права доступа программ 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 программ на операции с ресурсами с помощью флажка в графе **Статус**.
12. Сохраните внесенные изменения.

[Как добавить защищаемый ресурс в интерфейсе программы]

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **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 программ к добавленным ресурсам. Для этого выберите добавленный ресурс в левой части окна и Kaspersky Endpoint Security покажет список программ и права доступа для каждой из программ. Также вы можете выключить контроль действия программ на операции с ресурсами кнопкой **Выключить 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 программы к ресурсам на основании присвоенной группы доверия. Вы также можете изменить группу доверия для программы.

Удаление информации о неиспользуемых программах

Kaspersky Endpoint Security контролирует работу программ с помощью прав программ. Права программы определены группой доверия. Kaspersky Endpoint Security помещает программу в группу доверия при первом запуске. Вы можете изменить группу доверия для программы вручную. Также вы можете настроить права для отдельной программы вручную. Таким образом, Kaspersky Endpoint Security хранит следующую информацию о программе: группа доверия и права программы.

Kaspersky Endpoint Security автоматически удаляет информацию о неиспользуемых программах для экономии ресурсов компьютера. Kaspersky Endpoint Security удаляет информацию о программах по следующим правилам:

- Если группа доверия и права программы определены автоматически, Kaspersky Endpoint Security удаляет информацию об этой программе через 30 дней. Изменить время хранения информации о программе или выключить автоматическое удаление невозможно.
- Если вы вручную поместили программу в группу доверия или настроили права доступа, Kaspersky Endpoint Security удаляет информацию об этой программе через 60 дней (значение по умолчанию). Вы можете изменить время хранения информации о программе или выключить автоматическое удаление (см. инструкцию ниже).

При запуске программы, информация о которой была удалена, Kaspersky Endpoint Security исследует программу как при первом запуске.

[Как настроить автоматическое удаление информации о неиспользуемых программах 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Продвинутая защита → Предотвращение вторжений**.
6. В блоке **Правила обработки программ** выполните одно из следующих действий:
   - Если вы хотите настроить автоматическое удаление, установите флажок **Удалять права для программ, не запускавшихся более N дней** и укажите нужное количество дней.

     Kaspersky Endpoint Security будет удалять информацию о тех программах, 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 программах, для которых группа доверия и права программы определены автоматически, через 30 дней.
   - Если вы хотите выключить автоматическое удаление, снимите флажок **Удалять права для программ, не запускавшихся более N дней**.

     Kaspersky Endpoint Security будет хранить информацию о тех программах, 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 программах, для которых группа доверия и права программы определены автоматически, через 30 дней.
7. Сохраните внесенные изменения.

[Как настроить автоматическое удаление информации о неиспользуемых программах в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита** → **Предотвращение вторжений**.
5. В блоке **Правила обработки программ** выполните одно из следующих действий:

   - Если вы хотите настроить автоматическое удаление, установите флажок **Удалять права для программ, не запускавшихся более N дней** и укажите нужное количество дней.

     Kaspersky Endpoint Security будет удалять информацию о тех программах, 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 программах, для которых группа доверия и права программы определены автоматически, через 30 дней.

   - Если вы хотите выключить автоматическое удаление, снимите флажок **Удалять права для программ, не запускавшихся более N дней**.

     Kaspersky Endpoint Security будет хранить информацию о тех программах, 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 программах, для которых группа доверия и права программы определены автоматически, через 30 дней.
6. Сохраните внесенные изменения.

[Как настроить автоматическое удаление информации о неиспользуемых программах в интерфейсе программы](#)

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. В блоке **Правила обработки программ** выполните одно из следующих действий:
   - Если вы хотите настроить автоматическое удаление, установите флажок **Удалять права для программ, не запускавшихся более N дней** и укажите нужное количество дней.

     Kaspersky Endpoint Security будет удалять информацию о тех программах, 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 программах, для которых группа доверия и права программы определены автоматически, через 30 дней.

   - Если вы хотите выключить автоматическое удаление, снимите флажок **Удалять права для программ, не запускавшихся более N дней**.

     Kaspersky Endpoint Security будет хранить информацию о тех программах, 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 программах, для которых группа доверия и права программы 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 программой операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о программах, которые используют каждый ресурс.

Для мониторинга работы Предотвращения вторжений вам нужно включить запись в отчет. Например, вы можете включить отправку отчетов для отдельных программ 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

Злоумышленники могут с помощью специальных программ пытаться получить доступ к устройствам записи аудио и видео (например, микрофоны или веб-камеры). Kaspersky Endpoint Security контролирует получение программами аудиосигнала и видеосигнала и защищает данные от несанкционированного перехвата.

По умолчанию Kaspersky Endpoint Security контролирует доступ программ к аудиосагналу и видеосигналу следующим образом:

- "Доверенные" и "Слабые ограничения" – получение аудиосигнала и видеосигнала с устройств разрешено по умолчанию.
- "Сильные ограничения" и "Недоверенные" – получение аудиосигнала и видеосигнала с устройств запрещено по умолчанию.

Вы можете вручную разрешать программам получать аудиосигнал и видеосигнал.

Особенности защиты аудиосигнала

Функциональность защиты аудиосигнала имеет следующие особенности:

- Для работы функциональности необходимо, чтобы был включен компонент Предотвращение вторжений.
- Если программа начала получать аудиосигнал до запуска компонента Предотвращение вторжений, то Kaspersky Endpoint Security разрешает программе получение аудиосигнала и не показывает никаких уведомлений.
- Если вы поместили программу в группу "Недоверенные" или "Сильные ограничения" после того, как программа начала получать аудиосигнал, то Kaspersky Endpoint Security разрешает программе получение аудиосигнала и не показывает никаких уведомлений.
- При изменении параметров доступа программы к устройствам записи звука (например, программе было запрещено получение аудиосигнала) требуется перезапуск этой программы, чтобы она перестала получать аудиосигнал.
- Контроль получения аудиосигнала с устройств записи звука не зависит от параметров доступа программ 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 программы Kaspersky Endpoint Security с момента ее установки воспроизведение или запись аудио и видео могут быть прерваны в программах записи или воспроизведения аудио и видео. Это необходимо для того, чтобы включилась функциональность контроля доступа программ к устройствам записи звука. Системная служба управления средствами работы со звуком будет перезапущена при первом запуске программы Kaspersky Endpoint Security.

Особенности доступа программ к веб-камерам

Функциональность защиты доступа к веб-камере имеет следующие особенности и ограничения:

- Программа контролирует видео и статические изображения, полученные в результате обработки данных веб-камеры.
- Программа контролирует аудиосигнал, если он является частью видеопотока, получаемого с веб-камеры.
- Программа 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.

Откат вредоносных действий

Компонент Откат вредоносных действий позволяет Kaspersky Endpoint Security выполнить откат действий, произведенных вредоносными программами в операционной системе.

Во время отката действий вредоносной программы в операционной системе Kaspersky Endpoint Security обрабатывает следующие типы активности вредоносной программы:

- **Файловая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет исполняемые файлы, созданные вредоносной программой (на всех носителях, кроме сетевых дисков);
  - удаляет исполняемые файлы, созданные программами, в которые внедрилась вредоносная программа;
  - восстанавливает измененные или удаленные вредоносной программой файлы.

  Функциональность восстановления файлов имеет ряд ограничений.

- **Реестровая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет разделы и ключи реестра, созданные вредоносной программой;
  - не восстанавливает измененные или удаленные вредоносной программой разделы и ключи реестра.

- **Системная активность**

  Kaspersky Endpoint Security выполняет следующие действия:

- завершает процессы, которые запускала вредоносная программа;
- завершает процессы, в которые внедрялась вредоносная программа;
- не возобновляет процессы, которые остановила вредоносная программа.

- **Сетевая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - запрещает сетевую активность вредоносной программы;
  - запрещает сетевую активность тех процессов, в которые внедрялась вредоносная программа.

Откат действий вредоносной программы может быть запущен компонентом Защита от файловых угроз, Анализ поведения или при антивирусной проверке.

Откат действий вредоносной программы 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Продвинутая защита** → **Откат вредоносных действий**.
6. Используйте флажок **Откат вредоносных действий**, чтобы включить или выключить компонент.
7. Сохраните внесенные изменения.

Как включить или выключить компонент Откат вредоносных действий в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита** → **Откат вредоносных действий**.
5. Используйте переключатель **Откат вредоносных действий**, чтобы включить или выключить компонент.
6. Сохраните внесенные изменения.

[Как включить или выключить компонент Откат вредоносных действий в интерфейсе программы]

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **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 программы 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.

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, программа Kaspersky Endpoint Security получает от служб KSN сведения о категории и репутации проверяемых файлов, а также сведения о репутации проверяемых веб-адресов.

Использование Kaspersky Security Network является добровольным. Программа предлагает использовать KSN во время первоначальной настройки программы. 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 программы.

Для снижения нагрузки на серверы KSN специалисты "Лаборатории Касперского" могут выпускать обновления для программы, которые временно выключают или частично ограничивают обращения в Kaspersky Security Network. В этом случае статус подключения к KSN в локальном интерфейсе программы – *Включено с ограничениями*.

Инфраструктура KSN

Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения KSN:

- *Глобальный KSN* – это решение, которое используют большинство программ "Лаборатории Касперского". Участники KSN получают информацию от Kaspersky Security Network, 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 Security Network.

- *Локальный KSN* – это решение, позволяющее пользователям компьютеров, на которые установлена программа Kaspersky Endpoint Security или другие программы "Лаборатории Касперского", получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в KSN со своих компьютеров. Локальный KSN 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.

По умолчанию Kaspersky Security Center использует Глобальный KSN. Вы можете настроить использование Локального KSN в Консоли администрирования (MMC), Kaspersky Security Center 12 Web Console, а также с помощью командной строки. Настроить использование Локального KSN в Kaspersky Security Center Cloud Console невозможно.

Подробнее о работе Локального KSN см. в *документации для Kaspersky Private Security Network*.

KSN Proxy

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy.

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.

Подробную информацию о службе KSN Proxy см. в *справке Kaspersky Security Center*.

Включение и выключение использования Kaspersky Security Network

Чтобы включить или выключить использование Kaspersky Security Network, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита → Продвинутая защита → 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.

   По умолчанию Kaspersky Endpoint Security использует расширенный режим KSN. *Расширенный режим KSN* – режим работы программы, при котором Kaspersky Endpoint Security передает в "Лабораторию Касперского" дополнительные данные.
4. Если требуется, выключите переключатель **Включить расширенный режим KSN**.
5. Сохраните внесенные изменения.

В результате, если использование KSN включено, Kaspersky Endpoint Security использует информацию о репутации файлов, веб-ресурсов и программ, полученную из Kaspersky Security Network.

Ограничения работы с Локальным KSN

Локальный KSN (далее также "KPSN") 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 "недоверенный", а в KSN / KPSN объект имеет репутацию "доверенный", то Kaspersky Endpoint Security обнаружит файл как "недоверенный" 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:

- Программы "Лаборатории Касперского" используют офлайн репутационные базы. Офлайн репутационные базы предназначены для оптимизации ресурсов при работе программ "Лаборатории Касперского" и защите критически важных объектов компьютера. Офлайн репутационные базы формируют специалисты "Лаборатории Касперского" на основании данных Kaspersky Security Network. Программы "Лаборатории Касперского" обновляют офлайн репутационные базы с антивирусными базами программы. Если информация о проверяемом объекте содержится в офлайн репутационных базах, программа не запрашивает репутацию этого объекта в KSN / KPSN.
- В параметрах программы настроены исключения из проверки (доверенная зона). В этом случае программа не учитывает репутацию объекта в локальной репутационной базе.
- Программа использует технологии оптимизации проверки, например, технологии iSwift, iChecker или кеширование запросов репутации в
  KSN / KPSN. В этом случае программа может не запрашивать репутацию ранее проверенных объектов.

- Для оптимизации нагрузки программа проверяет файлы определенного формата и размера. Список форматов и ограничения по размеру определяют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами программы. Также вы можете настроить параметры оптимизации проверки в интерфейсе программы, например, для компонента Защита от файловых угроз.

Включение и выключение облачного режима для компонентов защиты

Облачный режим – режим работы программы, при котором Kaspersky Endpoint Security использует облегченную версию антивирусных баз. Работу программы 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.

Чтобы включить или выключить облачный режим для компонентов защиты, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **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.

Проверка подключения к Kaspersky Security Network

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Вы не участвуете в Kaspersky Security Network.
- Ваш компьютер не подключен к интернету.
- Текущий статус ключа не позволяет осуществить подключение к Kaspersky Security Network. Например, подключение к KSN может отсутствовать по следующим причинам:
  - Программа не активирована.
  - Срок действия лицензии или подписки истек.

- Выявлены проблемы, связанные с лицензионным ключом (например, ключ попал в список запрещенных ключей).

Чтобы проверить подключение к Kaspersky Security Network,

в главном окне программы нажмите на кнопку **Больше функций** → **Kaspersky Security Network**.

Откроется окно **Kaspersky Security Network**, в котором представлена информация о работе Kaspersky Security Network. Получение статистических данных по использованию KSN программа производит при открытии окна **Kaspersky Security Network**. Обновление глобальной статистики инфраструктуры облачных служб Kaspersky Security Network, а также времени синхронизации в режиме реального времени не производится.

В левой части окна **Kaspersky Security Network** отображается один из следующих статусов подключения компьютера к Kaspersky Security Network:

- *Включено.*

  Статус означает, что Kaspersky Security Network используется в работе Kaspersky Endpoint Security и серверы KSN доступны.

- *Включено. Доступно с ограничениями.*

  Статус означает, что Kaspersky Security Network используется в работе Kaspersky Endpoint Security и серверы KSN недоступны.

  Серверы KSN могут быть недоступны по следующим причинам:

  - На компьютере не запущена служба прокси-сервера KSN (ksnproxy).
  - Сетевой экран блокирует порт 13111.

  Если время, прошедшее после последней синхронизации с серверами KSN, превышает 15 минут или отображается статус *Неизвестно*, то статус подключения Kaspersky Endpoint Security к Kaspersky Security Network принимает значение *Включено. Недоступно*.

- *Выключено.*

  Статус означает, что Kaspersky Security Network не используется в работе Kaspersky Endpoint Security.

Если восстановить связь с серверами Kaspersky Security Network не удается, то рекомендуется обратиться в Службу технической поддержки или к поставщику услуг.

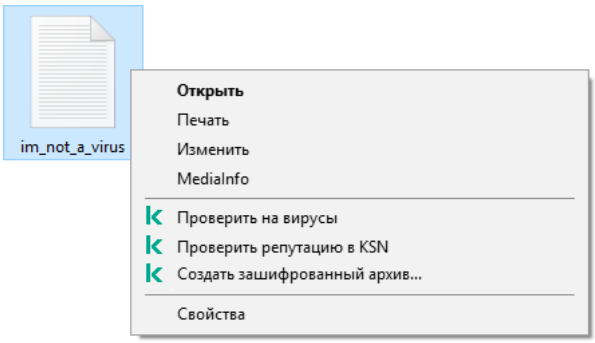
Проверка репутации файла в Kaspersky Security Network

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:

Доверенный. Большинство пользователей Kaspersky Security Network подтвердили, что файл доверенный.

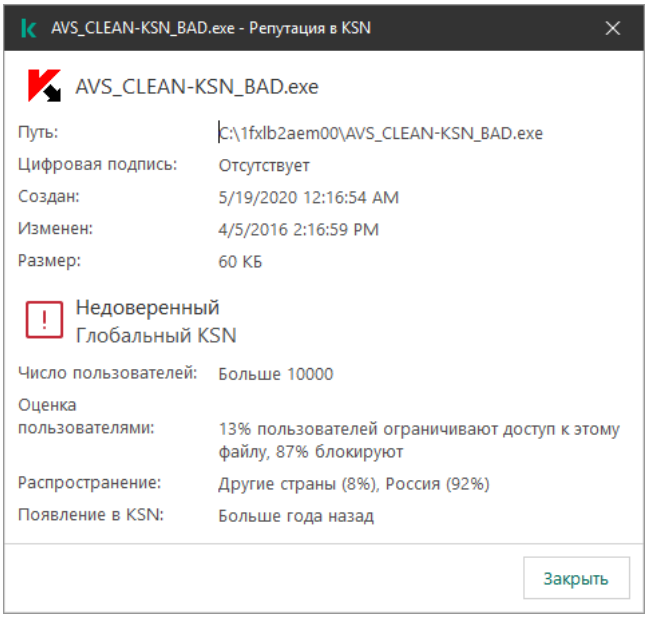
Легальная программа, которая может быть использована для нанесения вреда компьютеру или данным. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы злоумышленниками. Подробную информацию о легальных программах, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского". Вы можете добавить эти программы в список доверенных.

Недоверенный. Вирус или другая программа, представляющая угрозу.

Неизвестный. 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: *Глобальный KSN* или *Локальный KSN*.

Также Kaspersky Endpoint Security отображает дополнительную информацию о файле (см. рис. ниже).



Репутация файла в Kaspersky Security Network

Проверка защищенных соединений

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов (хранилище сертификатов Windows). Также Kaspersky Endpoint Security включает использование системного хранилища доверенных сертификатов в программах Firefox и Thunderbird для проверки трафика этих программ.

Компоненты Веб-Контроль, Защита от почтовых угроз, Защита от веб-угроз 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.

Настройка параметров проверки защищенных соединений

Чтобы настроить параметры проверки защищенных соединений, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
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 файловых 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 программами, 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 программы. 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 программы.

5. Нажмите на кнопку **Дополнительные настройки**.

6. Настройте параметры проверки защищенных соединений (см. таблицу ниже).

7. Сохраните внесенные изменения.

Параметры проверки защищенных соединений

Параметр	Описание
При переходе на домен с недоверенным сертификатом	• **Разрешать**. Если выбран этот вариант, то 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. 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. • **Блокировать соединение**. Если выбран этот вариант, то 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.
При возникновении ошибок проверки защищенных соединений	• **Блокировать соединение**. Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security блокирует это сетевое соединение. • **Добавлять домен в исключения**. Если выбран этот элемент, то 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 программы. Чтобы сбросить содержание списка, нужно выбрать элемент **Блокировать соединение**.
Блокировать соединение по протоколу SSL 2.0	Если флажок установлен, то Kaspersky Endpoint Security блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то Kaspersky Endpoint Security не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0, и не контролирует сетевой трафик, передаваемый по этим соединениям.
Расшифровать 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, Kaspersky Endpoint Security расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если флажок снят, Kaspersky Endpoint Security не имеет доступа к содержанию HTTPS-трафика. Поэтому программа контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://facebook.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.

Проверка защищенных соединений в Firefox и Thunderbird

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов (хранилище сертификатов Windows). Firefox и Thunderbird по умолчанию используют собственное хранилище сертификатов Mozilla, а не хранилище сертификатов Windows. Если в вашей организации развернуто решение Kaspersky Security Center и к компьютеру применена политика, Kaspersky Endpoint Security автоматически включает использование хранилища сертификатов Windows в программах Firefox и Thunderbird для проверки трафика этих программ. Если к компьютеру не применена политика, вы можете выбрать хранилище сертификатов, которое будут использовать программы Mozilla. Если вы выбрали хранилище сертификатов Mozilla, добавьте сертификат "Лаборатории Касперского" в хранилище вручную. Это позволит избежать ошибок при работе с HTTPS-трафиком.

Для проверки трафика в браузере Mozilla Firefox и почтовом клиенте Thunderbird должна быть включена проверка защищенных соединений. Если проверка защищенных соединений выключена, Kaspersky Endpoint Security не проверяет трафик в браузере Mozilla Firefox и почтовом клиенте Thunderbird.

Перед добавлением сертификата в хранилище Mozilla экспортируйте сертификат "Лаборатории Касперского" из Панели управления Windows (свойства браузера). Подробнее об экспорте сертификата "Лаборатории Касперского" вы можете узнать в базе знаний Службы технической поддержки. Подробнее о добавлении сертификата в хранилище см. на *сайте Службы технической поддержки Mozilla*.

Вы можете выбрать хранилище сертификатов только в локальном интерфейсе программы.

Чтобы выбрать хранилище сертификатов для проверки защищенных соединений в Firefox и Thunderbird, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Mozilla Firefox и Thunderbird** установите флажок **Проверять защищенный трафик в продуктах Mozilla**.
4. Выберите хранилище сертификатов:
   - **Использовать хранилище сертификатов Windows**. Это хранилище, в которое корневой сертификат "Лаборатории Касперского" добавляется при установке Kaspersky Endpoint Security.

- **Использовать хранилище сертификатов Mozilla**. Программы 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.

5. Сохраните внесенные изменения.

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*. Если доверенная программа использует защищенное соединение, вы можете выключить проверку защищенных соединений для этой программы. Например, вы можете выключить проверку защищенных соединений для программ облачных хранилищ, так как эти программы используют двухфакторную аутентификацию с собственным сертификатом.

Чтобы исключить веб-адрес из проверки защищенных соединений, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Проверка защищенных соединений** нажмите на кнопку **Доверенные адреса**.
4. Нажмите на кнопку **Добавить**.
5. Введите имя домена или IP-адрес, если вы хотите, чтобы программа Kaspersky Endpoint Security не проверяла 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 маски для IP-адресов.

   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 программы.

- 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 программы.

Чтобы просмотреть список доменов с ошибками проверки, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **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 программы, – *глобальные исключения*.

Чтобы просмотреть глобальные исключения из проверки защищенного трафика, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Проверка защищенных соединений** нажмите на ссылку **сайтах**.

   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.

Веб-Контроль

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

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).

Kaspersky Endpoint Security контролирует только HTTP- и HTTPS-трафик.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений.

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 программы). 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 программ" 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.

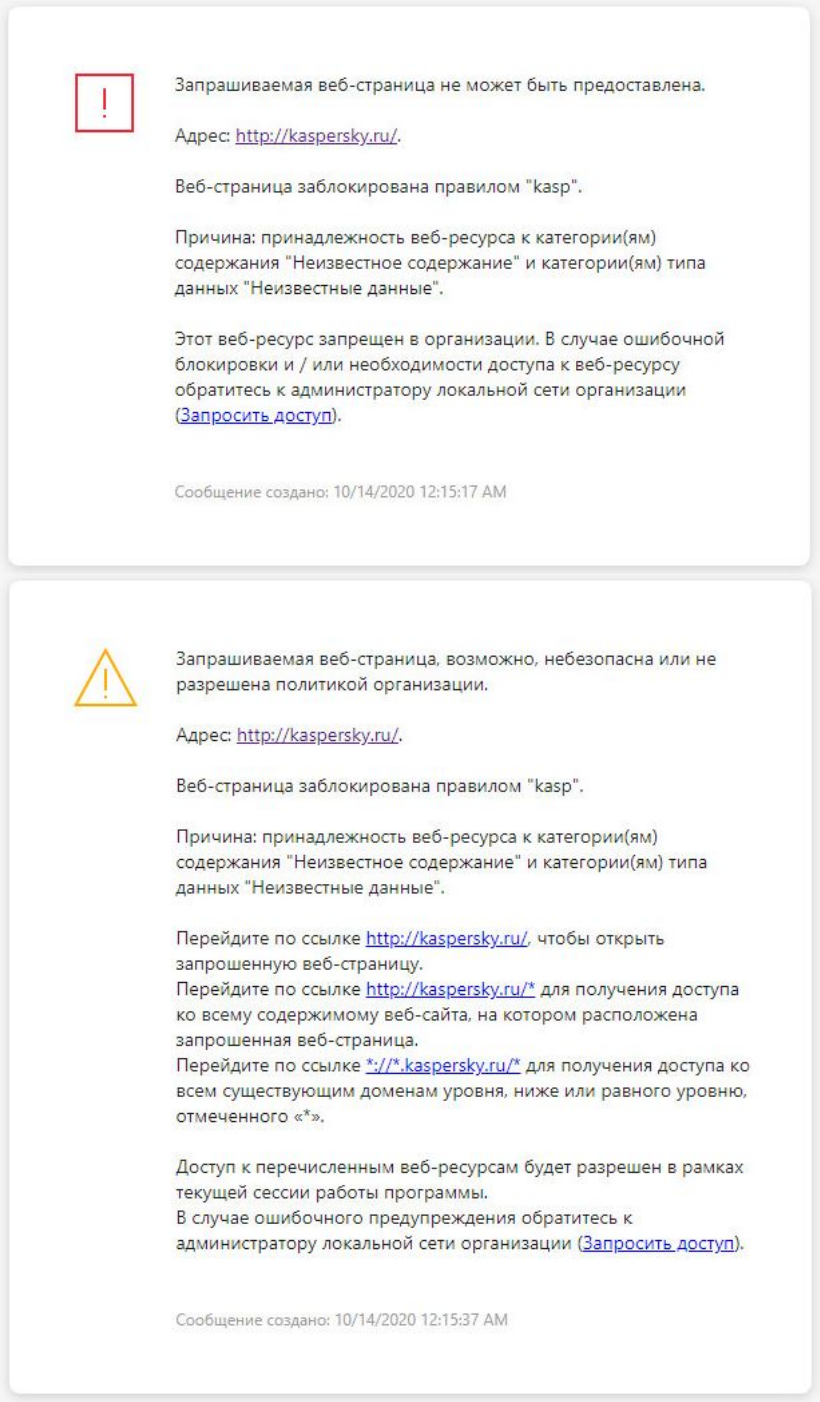
Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

- 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.



Включение и выключение Веб-Контроля

По умолчанию Веб-Контроль включен.

Чтобы включить или выключить Веб-Контроль, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. Используйте переключатель **Веб-Контроль**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

Действия с правилами доступа к веб-ресурсам

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 программы Kaspersky Endpoint Security список правил компонента Веб-Контроль не пуст. Предустановлены два правила:

- Правило "Сценарии и таблицы стилей", которое разрешает всем пользователям в любое время доступ к веб-ресурсам, адреса которых содержат названия файлов с расширением css, js, vbs. Например: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.
- "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.

Добавление правила доступа к веб-ресурсам

Чтобы добавить или изменить правило доступа к веб-ресурсам, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
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**. Если выбрано это значение, то Kaspersky Endpoint Security разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
   - **Запрещать**. Если выбрано это значение, то Kaspersky Endpoint Security запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
   - **Предупреждать**. Если выбрано это значение, то при попытке доступа к веб-ресурсам, удовлетворяющим правилу, Kaspersky Endpoint Security 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 изображения*).

   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 **Адреса** выберите нужный фильтр по адресам веб-ресурсов:

- **Ко всем адресам**. Веб-Контроль не фильтрует веб-ресурсы по адресам.
- **К отдельным адресам**. Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Для создания список адресов веб-ресурсов выполните следующие действия:

a. Нажмите на кнопку **Добавить адрес** или **Добавить группу адресов**.

b. В открывшемся окне сформируйте список адресов веб-ресурсов. Вы можете ввести веб-адрес или использовать маски. Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла.

c. Вернитесь в окно настройки правила доступа к веб-ресурсам.

Если Проверка защищенных соединений отключена, для протокола HTTPS доступна фильтрация только по имени сервера.

10. 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 веб-ресурсы только для отдельных пользователей. 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.

11. 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.

12. Сохраните внесенные изменения.

Назначение приоритета правилам доступа к веб-ресурсам

Вы можете назначить приоритет каждому правилу из списка правил, расположив их в определенном порядке.

Чтобы назначить правилам доступа к веб-ресурсам приоритет, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.
4. В открывшемся окне выберите правило, приоритет которого вы хотите изменить.
5. С помощью кнопок **Вверх** и **Вниз** переместите правило на нужную позицию в списке правил доступа к веб-ресурсам.
6. Сохраните внесенные изменения.

Включение и выключение правила доступа к веб-ресурсам

Чтобы включить или выключить правило доступа к веб-ресурсам, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.
4. В открывшемся окне выберите правило, которое вы хотите включить или выключить.
5. В графе **Состояние** выполните следующие действия:
   - Если вы хотите включить использование правила, выберите значение **Активно**.
   - Если вы хотите выключить использование правила, выберите значение **Не активно**.
6. Сохраните внесенные изменения.

Экспорт и импорт списка доверенных веб-адресов

Вы можете экспортировать список правил Веб-Контроля в файл в формате XML. 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Контроль безопасности** → **Веб-Контроль**.
6. 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 **Экспорт**.
   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. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл.
7. Для импорта списка правил Веб-Контроля выполните следующие действия:
   a. Нажмите на ссылку **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

   b. Нажмите на кнопку **Открыть**.

      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 правил Веб-Контроля в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите экспортировать или импортировать список правил.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
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 **Экспорт**.

   c. Подтвердите, что вы хотите экспортировать только выбранные правила, или экспортируйте весь список.

   d. Нажмите на кнопку **Экспорт**.

   Kaspersky Endpoint Security экспортирует список правил в XML-файл в папку для загрузки по умолчанию.
6. Для импорта списка правил в блоке **Список правил** выполните следующие действия:

   a. Нажмите на ссылку **Импорт**.

   В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

   b. Нажмите на кнопку **Открыть**.

   Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
7. Сохраните внесенные изменения.

Проверка работы правил доступа к веб-ресурсам

Чтобы оценить, насколько согласованы правила Веб-Контроля, вы можете проверить их работу. Для этого в рамках компонента Веб-Контроль предусмотрена функция "Диагностика правил".

Чтобы проверить работу правил доступа к веб-ресурсам, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
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.

Экспорт и импорт списка адресов веб-ресурсов

Если в правиле доступа к веб-ресурсам вы сформировали список адресов веб-ресурсов, вы можете экспортировать его в файл формата TXT. 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.

Чтобы импортировать или экспортировать список адресов веб-ресурсов в файл, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.

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 TXT, в который вы хотите экспортировать список адресов веб-ресурсов, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список адресов веб-ресурсов в TXT-файл.

6. Для импорта списка веб-ресурсов в блоке **Адреса** выполните следующие действия:

   a. Нажмите на кнопку **Импорт**.

      В открывшемся окне выберите TXT-файл, из которого вы хотите импортировать список веб-ресурсов.

   b. Нажмите на кнопку **Открыть**.

      Если на компьютере уже есть список адресов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из TXT-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.

Kaspersky Endpoint Security создает следующие события активности пользователя в интернете:

- блокировка веб-сайта (статус *Критические события*);
- посещение нерекомендованного веб-сайта (статус *Предупреждения*);
- посещение разрешенного веб-сайта (статус *Информационные сообщения*).

Перед включением мониторинга активности пользователей в интернете 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.

Чтобы внедрить в трафик скрипт взаимодействия с веб-страницами, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Обработка трафика** установите флажок **Внедрять в трафик скрипт взаимодействия**.
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 программы, журнала событий ОС, отчетов.

Чтобы настроить запись событий Веб-Контроля на компьютере пользователя, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Правила уведомлений**.
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 журнале** 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.

Чтобы включить запись событий посещения разрешенных веб-сайтов, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → Веб-Контроль**.
3. В блоке **Дополнительно** нажмите на кнопку **Дополнительные настройки**.
4. В открывшемся окне установите флажок **Записывать данные о посещении разрешенных страниц в журнал**.
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, в раскрывающемся списке **Действие** выбран элемент **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, если в параметрах правила, которое описывает этот веб-ресурс, в раскрывающемся списке **Действие** выбран элемент **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.

Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и сообщения для отправки администратору локальной сети организации предусмотрены шаблоны. Вы можете изменять их содержание.

Чтобы изменить шаблон сообщений Веб-Контроля, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. В блоке **Шаблоны** настройте шаблоны сообщений Веб-Контроля:
   - **Предупреждения**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу.
   - **Блокировка**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу.
   - **Сообщение администратору**. Поле ввода содержит шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно.
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-	Удовлетворяет	Комментарий

		ресурса	ли проверяемый адрес маске адреса	
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.

Миграция правил доступа к веб-ресурсам из предыдущих версий программы

При обновлении программы с версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и с более ранних версий до Kaspersky Endpoint Security 11.6.0 для Windows правила доступа к веб-ресурсам, основанные на категориях содержания веб-ресурсов, мигрируют по следующим правилам:

- Правила доступа к веб-ресурсам, основанные на одной или нескольких категориях содержания веб-ресурсов из списка "Чаты и форумы", "Веб-почта", "Социальные сети", становятся основанными на категории содержания веб-ресурсов "Общение в сети".
- Правила доступа к веб-ресурсам, основанные на одной или нескольких категориях содержания веб-ресурсов из списка "Интернет-магазины" и "Платежные системы", становятся основанными на категории содержания веб-ресурсов "Интернет-магазины, банки, платежные системы".
- Правила доступа к веб-ресурсам, основанные на категории содержания веб-ресурсов "Азартные игры", становятся основанными на категории содержания веб-ресурсов "Азартные игры, лотереи, тотализаторы".
- Правила доступа к веб-ресурсам, основанные на категории содержания веб-ресурсов "Браузерные игры", становятся основанными на категории содержания веб-ресурсов "Компьютерные игры".
- Правила доступа к веб-ресурсам, основанные на категориях содержания веб-ресурсов, не перечисленных в предыдущих пунктах списка, мигрируют без изменений.

Контроль устройств

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

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.

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 – .
  - 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). Таким образом, вы можете ограничить подключение всех устройств, 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.

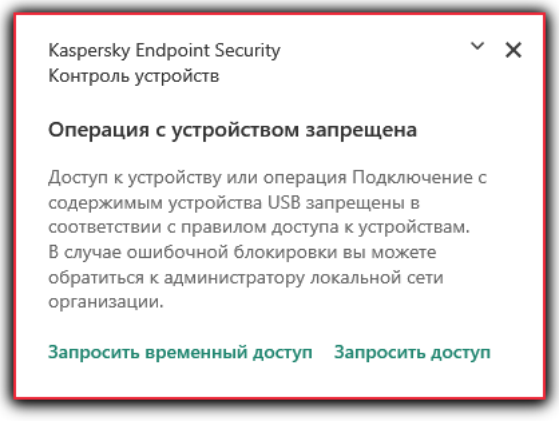
  - **Устройства по маске идентификатора**. Если вы используете несколько устройств с похожими идентификаторами, вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Kaspersky Endpoint Security не поддерживает символ `?` при вводе маски. Например, `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 программа Kaspersky Endpoint Security сохраняла события подключения / отключения устройства, разрешите доступ к соответствующему типу устройств (статус) или добавьте устройство в список доверенных.

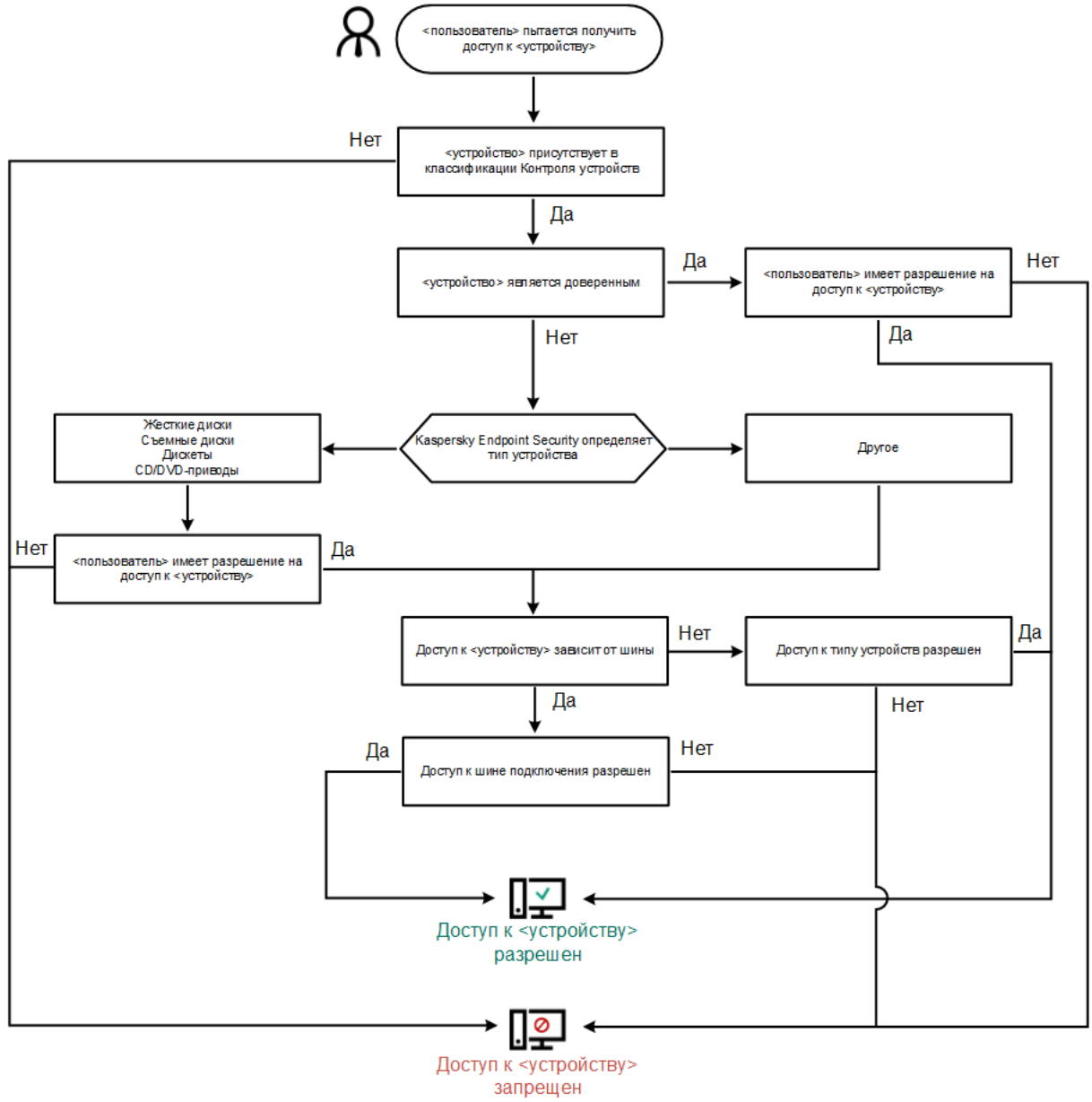
При подключении к компьютеру устройства, доступ к которому запрещен Контролем устройств, Kaspersky Endpoint Security заблокирует доступ и покажет уведомление (см. рис. ниже).



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 установленной программой Kaspersky Endpoint Security требуется запросить доступ к устройству, которое, по его мнению, было заблокировано ошибочно, передайте ему инструкцию по запросу доступа.

Включение и выключение Контроля устройств

По умолчанию Контроль устройств включен.

Чтобы включить или выключить Контроль устройств, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль устройств**.
3. Используйте переключатель **Контроль устройств**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Контроль устройств включен, программа передает в Kaspersky Security Center информацию о подключенных устройствах. Вы можете просмотреть список подключенных устройств в Kaspersky Security Center в папке **Оборудование**.

О правилах доступа

Правила доступа – набор параметров, которые определяют доступ пользователей к установленным или подключенным к компьютеру устройствам. 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	✓	✓	✓	✓	✓
Принтеры	✓	–	–	–	–
Дискеты	✓	✓	✓	✓	✓
CD/DVD-приводы	✓	✓	✓	✓	✓
Модемы	✓	–	–	–	–
Стримеры	✓	–	–	–	–
Мультифункциональные устройства	✓	–	–	–	–
Устройства чтения смарт-карт	✓	–	–	–	–
Windows CE USB ActiveSync устройства	✓	–	–	–	–
Внешние сетевые адаптеры	✓	–	–	–	–
Портативные устройства (MTP)	✓	✓	✓	✓	✓

Bluetooth	✓	–	–	–	–
Камеры и сканеры	✓	–	–	–	–

Правила доступа к мобильным устройствам

Мобильные устройства под управлением Android и iOS относятся к портативным устройствам (MTP). При подключении мобильного устройства к компьютеру операционная система определяет тип устройства. Если на компьютере установлены программы 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.

Доступ к ADB- или iTunes-устройствам имеет следующие особенности:

- Настроить расписание доступа к устройству невозможно. То есть, если доступ к устройствам ограничен правилами (статус), ADB- и iTunes-устройства доступны всегда.
- Настроить доступ к устройству для отдельных пользователей, а также настроить права доступа (чтение / запись) невозможно. То есть, если доступ к устройствам ограничен правилами (статус), ADB- и iTunes-устройства доступны всем пользователям со всеми правами.
- Настроить доступ к доверенным ADB- или iTunes-устройствам для отдельных пользователей невозможно. Если устройство доверенное, ADB- и iTunes-устройства доступны всем пользователям.
- Если вы установили программы 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.

По умолчанию правила доступа к устройствам разрешают полный доступ к устройствам всем пользователям в любое время, если разрешен доступ к шинам подключения для соответствующих типов устройств (статус).

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

Правила доступа к шинам определяют только разрешение (статус) или запрет (статус) на подключение устройств. Для всех шин подключения из классификации компонента Контроль устройств по умолчанию созданы правила, разрешающие доступ к шинам.

Изменение правила доступа к устройствам

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.

Чтобы изменить правило доступа к устройствам, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **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 запоминающим устройствам** выберите правило доступа, которое хотите изменить. В блоке находятся устройства с файловой системой, для которых вы можете настроить дополнительные параметры доступа. По умолчанию правило доступа к устройствам разрешает полный доступ к типу устройств всем пользователям в любое время.

   a. В блоке **Доступ** выберите доступ к устройству:

      - **Разрешать**.
      - **Запрещать**.
      - **Зависит от шины подключения**.

        Чтобы запретить или разрешить доступ к устройству, настройте доступ к шине подключения.

      - **Ограничивать правилами**.

        Этот вариант позволяет настроить права пользователей, разрешения, расписание для доступа к устройствам.

   b. В блоке **Права пользователей** нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила доступа к устройствам.

   c. Назначьте 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.

   d. Установите статус правила доступа к устройствам **Включено**.

   e. Настройте разрешения пользователей для доступа к устройствам: чтение, запись.

   f. Выберите пользователей или группы пользователей, к которым вы хотите применить правило доступа к устройству.

g. Настройте расписание доступа к устройствам для пользователей.

h. Нажмите на кнопку **Добавить**.

5. В блоке **Доступ к внешним устройствам** выберите правило и настройте доступ: **Разрешать**, **Запрещать**, **Зависит от шины подключения**. Если требуется, настройте доступ к шине подключения.

6. В блоке **Доступ к сетям Wi-Fi** перейдите по ссылке **Wi-Fi** и настройте доступ: **Разрешать**, **Запрещать**, **Запрещать с исключениями**. Если требуется, добавьте сети Wi-Fi в список доверенных.

7. Сохраните внесенные изменения.

Изменение правила доступа к шине подключения

Чтобы изменить правило доступа к шине подключения, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль устройств**.

3. В блоке **Настройки** 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**.

6. Сохраните внесенные изменения.

Добавление сети Wi-Fi в список доверенных

Вы можете разрешить пользователям подключаться к сетям Wi-Fi, которые вы считаете безопасными, например, к корпоративной сети Wi-Fi. Для этого нужно добавить эту сеть в список доверенных сетей Wi-Fi. Контроль устройств будет блокировать доступ ко всем сетям Wi-Fi, кроме тех, которые указаны в списке доверенных.

Чтобы добавить сеть Wi-Fi в список доверенных, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль устройств**.

3. В блоке **Настройки** нажмите на кнопку **Правила доступа для устройств и сетей 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.

5. В графе **Доступ** выберите **Запретить с исключениями**.
6. В блоке **Доверенная сеть Wi-Fi** нажмите на кнопку **Добавить**.
7. В открывшемся окне выполните следующие действия:
   a. В поле **Имя сети** укажите имя сети Wi-Fi, которую вы хотите добавить в список доверенных.
   b. В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации, используемый при подключении к доверенной сети Wi-Fi.
   c. В раскрывающемся списке **Тип шифрования** выберите тип шифрования, используемый для защиты трафика доверенной сети Wi-Fi.
   d. В поле **Комментарий** вы можете указать любую информацию о добавленной сети Wi-Fi.

   Сеть Wi-Fi считается доверенной, если ее параметры соответствуют всем параметрам, указанным в правиле.
8. Сохраните внесенные изменения.

Мониторинг использования съемных дисков

Чтобы включить мониторинг использования съемных дисков, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → Контроль устройств**.
3. В блоке **Настройки** нажмите на кнопку **Правила доступа для устройств и сетей Wi-Fi**.

   В открывшемся окне находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.
4. В блоке **Доступ к запоминающим устройствам** выберите элемент **Съемные диски**.
5. Нажмите на ссылку **Запись событий в журнал**.
6. В открывшемся окне перейдите на закладку **Запись событий в журнал**.
7. Включите переключатель **Запись событий в журнал**.
8. В блоке **Операции с файлами** выберите операции, которые вы хотите контролировать: **Запись**, **Удаление**.
9. В блоке **Фильтр по форматам файлов** выберите форматы файлов, информацию об операциях с которыми Контроль устройств должен записывать в журнал.
10. Выберите пользователей или группы пользователей, использование съемных дисков которых вы хотите контролировать.

11. 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 закладке **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 программы 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\environment];
   - для 32-битных операционных систем: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\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.

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 программы. 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 имеет следующие ограничения при работе с доверенными устройствами:

- Плагин управления Kaspersky Endpoint Security версий 11.0.0–11.2.0 не поддерживает работу со списком доверенных устройств программы Kaspersky Endpoint Security версии 11.3.0 и 11.4.0. Для работы со списком доверенных устройств обновить плагин управления до версии 11.3.0 и 11.4.0.

- Плагин управления Kaspersky Endpoint Security версий 11.3.0 и 11.4.0 не поддерживает работу со списком доверенных устройств программы Kaspersky Endpoint Security версии 11.2.0 и ниже. Для работы со списком доверенных устройств обновите программу до версии 11.3.0 или 11.4.0. Также вы можете отправить запрос с описанием ситуации в Службу технической поддержки через Kaspersky CompanyAccount.

- Для переноса списка доверенных устройств из Kaspersky Endpoint Security версии 11.2.0 в 11.3.0 отправьте запрос с описанием ситуации в Службу технической поддержки через Kaspersky CompanyAccount.

Добавление устройства в список доверенных из интерфейса программы

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей "Все").

Чтобы добавить устройство в список доверенных из интерфейса программы, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль устройств**.

3. В блоке **Настройки** 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.

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.

8. Сохраните внесенные изменения.

Добавление устройства в список доверенных из Kaspersky Security Center

Kaspersky Security Center получает информацию об устройствах, если на компьютерах установлена программа Kaspersky Endpoint Security и включен Контроль устройств. Добавить устройство в список доверенных, информации о котором в Kaspersky Security Center нет, невозможно.

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_*`.

Чтобы добавить устройства в список доверенных, выполните следующие действия:

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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Контроль безопасности** → **Контроль устройств**.
6. В правой части окна выберите закладку **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** и выберите способ добавления устройства в список доверенных.
9. Для фильтрации устройств в раскрывающемся списке **Тип устройств** выберите тип устройств (например, **Съемные диски**).
10. 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.
11. 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.
12. Нажмите на кнопку **Обновить**.

    В таблице отобразится список устройств, которые удовлетворяют заданным параметрам фильтрации.
13. Установите флажки напротив названий устройств, которые вы хотите добавить в список доверенных.
14. В поле **Комментарий** введите описание причины добавления устройств в список доверенных.
15. Справа от поля **Разрешать пользователям и / или группам пользователей** нажмите на кнопку **Выбрать**.
16. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.

    По умолчанию доступ к доверенным устройствам разрешен для группы "Все".

17. 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 список 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль устройств**.
3. В блоке **Настройки** 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. Нажмите на кнопку **Сохранить**.

      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 существующему** или **Импортировать и заменить существующий**.

b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных устройств.

c. Нажмите на кнопку **Открыть**.

Если на компьютере уже есть список доверенных устройств, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

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 добавляет устройство в список доверенных.

Вы можете добавить доверенное устройство в политике для группы администрирования или в локальных параметрах программы для отдельного компьютера.

3. Администратор обновляет параметры Kaspersky Endpoint Security на компьютере пользователя.

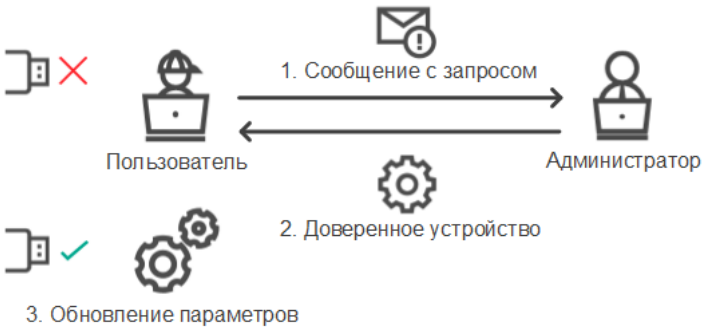


Схема предоставления доступа к устройству в онлайн-режиме

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 **Разрешить 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.

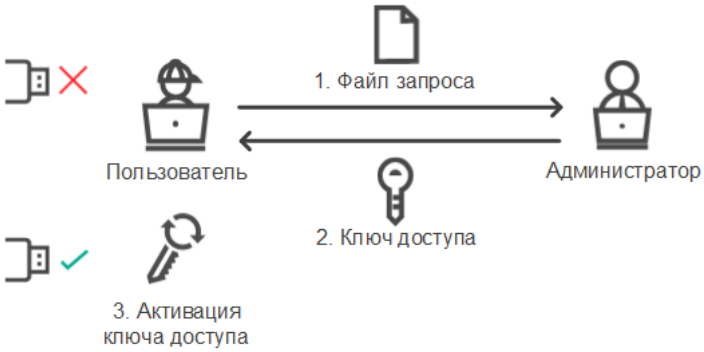


Схема предоставления доступа к устройству в офлайн-режиме

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.

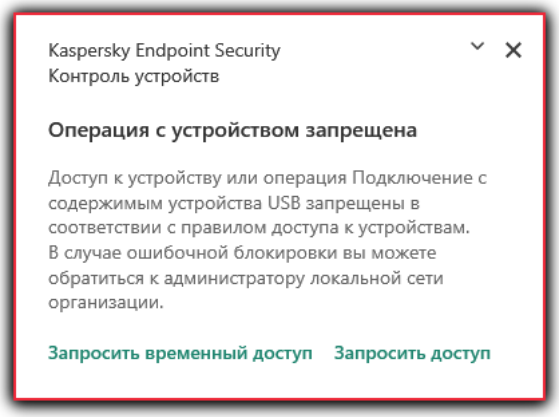
   Kaspersky Endpoint Security покажет уведомление блокировки доступа к устройству (см. рис. ниже).

2. Нажмите на ссылку **Запросить доступ**.

   Откроется окно **Сообщение для администратора**. В сообщении содержится информация о заблокированном устройстве.

3. Нажмите на кнопку **Отправить**.

Администратор получит сообщение с запросом на предоставление доступа, например, по электронной почте. Подробнее об обработке запросов пользователей см. в *справке Kaspersky Security Center*. После добавления устройства в список доверенных и обновления параметров Kaspersky Endpoint Security на компьютере пользователь получит доступ к устройству.



Уведомление Контроля устройств

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 **Разрешить 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 **Запрос доступа к устройству** со списком подключенных устройств.

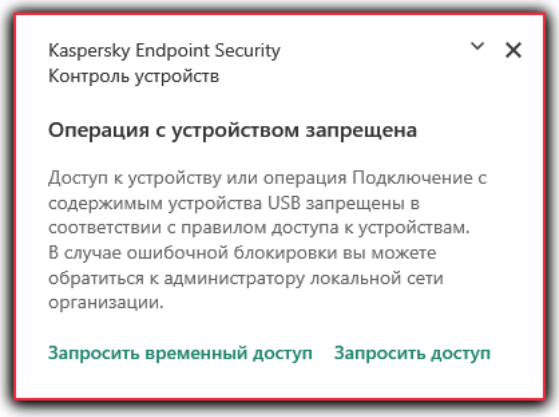
3. В списке подключенных устройств выберите устройство, к которому вы хотите получить доступ.

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

Чтобы администратору создать ключ доступа к заблокированному устройству, выполните следующие действия:

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 закладку **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 закладку **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.

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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → 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. Нажмите на кнопку **Открыть**.

   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. 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 сообщения о блокировке доступа к устройству или запрете операции над содержимым устройства, а также для сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

Чтобы изменить шаблоны сообщений Контроля устройств, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → Контроль устройств**.
3. В блоке **Шаблоны** настройте шаблоны сообщений Контроля устройств:

   - **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.
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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль устройств**.
3. В блоке **Настройки** 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль устройств**.
3. В блоке **Настройки** 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль устройств**.
3. В блоке **Настройки** 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 только для решений Kaspersky Endpoint Security для бизнеса Расширенный и Kaspersky Total Security для бизнеса. Подробнее о решениях Kaspersky Endpoint Security для бизнеса см. на *сайте "Лаборатории Касперского"*.

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена 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 офисной программы*). 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 программы. 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 **Срабатывание правил в обучающем режиме**.

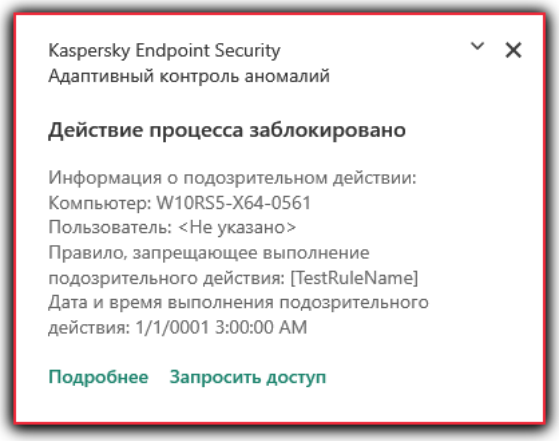
2. Анализ отчета о срабатывании правил.

   Администратор анализирует отчет о срабатываниях правил или содержание хранилища **Срабатывание правил в обучающем режиме**. Далее администратор может выбрать поведение Адаптивного контроля аномалий при срабатывании правила: блокировать или разрешить. Также администратор может продолжить отслеживать срабатывание правила и продлить работу программы в обучающем режиме. Если администратор не предпринимает никаких мер, программа также продолжит работать в обучающем режиме. Отсчет срока действия обучающего режима начинается заново.

Настройка Адаптивного контроля аномалий происходит в режиме реального времени. Настройка Адаптивного контроля аномалий 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 **Срабатывание правил в обучающем режиме**. Рекомендуется проверять отчет о срабатывании правил и содержимое хранилища **Срабатывание правил в обучающем режиме**.

При попытке вредоносной программы 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

Включение и выключение Адаптивного контроля аномалий

По умолчанию Адаптивный контроль аномалий включен.

Чтобы включить или выключить Адаптивный контроль аномалий, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → Адаптивный контроль аномалий**.
3. Используйте переключатель **Адаптивный контроль аномалий**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

Включение и выключение правила Адаптивного контроля аномалий

Чтобы включить или выключить правило Адаптивного контроля аномалий, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → 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 программ*) и разверните набор.
5. Выберите правило (например, Запуск *Windows PowerShell из офисных программ*).
6. Используйте переключатель в графе **Статус**, 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → 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 **Срабатывание правил в обучающем режиме** 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 данном примере `file.xlsx` – исходный объект, Excel – исходный процесс, `browser.exe` – целевой объект, Browser – целевой процесс.

Чтобы создать исключение для правила Адаптивного контроля аномалий, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → 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.

   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.
   - **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://<объект>`, где `<объект>` – 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.

   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.
    - **Целевой объект**. Команда запуска целевого процесса. Укажите команду по следующему шаблону `object://<команда>`, 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.

    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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → 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. Нажмите на кнопку **Сохранить**.
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. Нажмите на кнопку **Открыть**.

      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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **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 сообщения о блокировке потенциально опасных действий и сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

Чтобы изменить шаблон сообщения, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. В блоке **Шаблоны** настройте шаблоны сообщений Адаптивного контроля аномалий:

   - **Блокировка**. 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.
4. Сохраните внесенные изменения.

Просмотр отчетов Адаптивного контроля аномалий

Чтобы просмотреть отчеты Адаптивного контроля аномалий, выполните следующие действия:

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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В разделе **Контроль безопасности** выберите подраздел **Адаптивный контроль аномалий**.

   В правой части окна отобразятся параметры компонента Адаптивный контроль аномалий.
6. Выполните одно из следующих действий:

   - Если вы хотите просмотреть отчет о параметрах правил Адаптивного контроля аномалий, нажмите на кнопку **Отчет о состоянии правил**.
   - Если вы хотите просмотреть отчет о срабатываниях правил Адаптивного контроля аномалий, нажмите на кнопку **Отчет о срабатываниях правил**.
7. Запустится процесс формирования отчета.

Отчет отобразится в новом окне.

Контроль программ

Контроль программ управляет запуском программ на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании программ. Также Контроль программ снижает риск заражения компьютера, ограничивая доступ к программам.

Настройка Контроля программ состоит из следующих этапов:

1. Создание категорий программ.

   Администратор создает категории программ, которыми администратор хочет управлять. Категории программ предназначены для всех компьютеров сети организации независимо от групп администрирования. Для создания категории вы можете использовать следующие критерии: KL-категория (например, *Браузеры*), хеш файла, производитель программы и другие.
2. Создание правил Контроля программ.

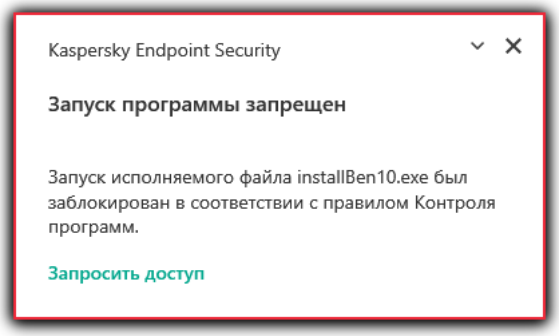
   Администратор создает правила Контроля программ в политике для группы администрирования. Правило включает в себя категории программ и статус запуска программ из этих категорий: запрещен или разрешен.
3. Выбор режима работы Контроля программ.

   Администратор выбирает режим работы с программами, которые не входят ни в одно из правил (списки запрещенных и разрешенных программ).

При попытке пользователя запустить запрещенную программу, Kaspersky Endpoint Security заблокирует запуск программы и покажет уведомление (см. рис. ниже).

Для проверки настройки Контроля программ предусмотрен *тестовый режим*. В этом режиме Kaspersky Endpoint Security выполняет следующие действия:

- разрешает запуск программ, в том числе запрещенных;
- показывает уведомление о запуске запрещенной программы и добавляет информацию в отчет на компьютере пользователя;
- отправляет данные о запуске запрещенных программ в Kaspersky Security Center.



Уведомление Контроля программ

Режимы работы Контроля программ

Компонент Контроль программ может работать в двух режимах:

- **Список запрещенных**. Режим, при котором Контроль программ разрешает пользователям запуск любых программ, кроме тех, которые запрещены в правилах Контроля программ.

  Этот режим работы Контроля программ установлен по умолчанию.

- **Список разрешенных**. Режим, при котором Контроль программ запрещает пользователям запуск любых программ, кроме тех, которые разрешены и не запрещены в правилах Контроля программ.

  Если разрешающие правила Контроля программ сформированы максимально полно, компонент запрещает запуск всех новых программ, не проверенных администратором локальной сети организации, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

  Вы можете ознакомиться с рекомендациями по настройке правил контроля программ в режиме списка разрешенных программ.

Настройка Контроля программ 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 программ.

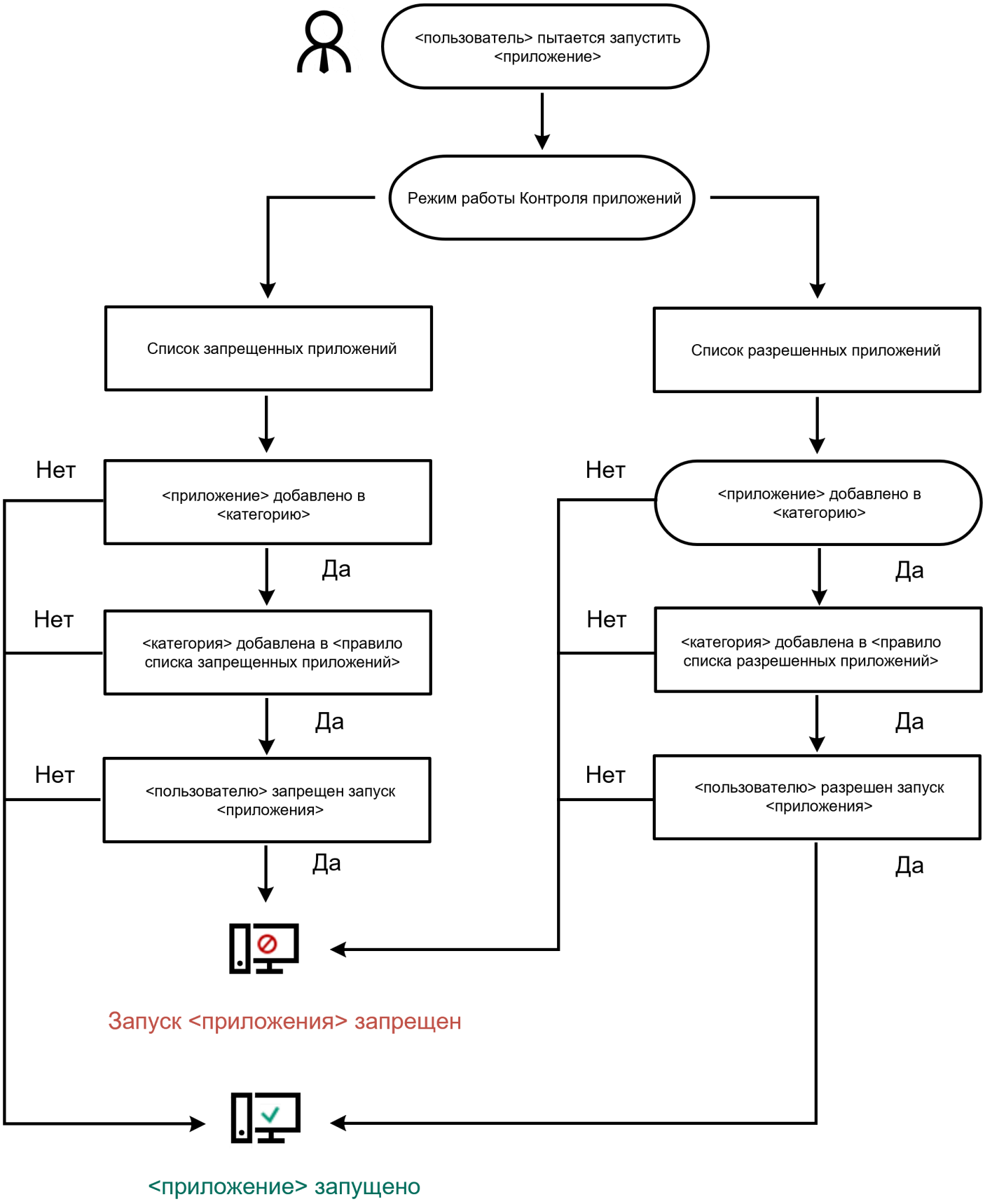
  Правила Контроля программ, сформированные в Консоли администрирования Kaspersky Security Center, основываются на созданных вами категориях программ, а не на включающих и исключающих условиях, как в локальном интерфейсе Kaspersky Endpoint Security.

- Получение информации о программах, которые установлены на компьютерах локальной сети организации.

Поэтому настройку работы компонента Контроль программ рекомендуется выполнять с помощью Kaspersky Security Center.

Алгоритм работы Контроля программ

Kaspersky Endpoint Security использует алгоритм для принятия решения о запуске программы (см. рис. ниже).



Алгоритм работы Контроля программ

Ограничения функциональности Контроля программ

Работа компонента Контроль программ ограничена в следующих случаях:

- При обновлении версии программы импорт параметров компонента Контроль программ не поддерживается.
- При обновлении версии программы импорт параметров компонента Контроль программ поддерживается только при обновлении версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше до Kaspersky Endpoint Security 11.6.0 для Windows.

  При обновлении версий программы, отличных от Kaspersky Endpoint Security 10 Service Pack 2 для Windows, для восстановления работоспособности Контроля программ необходимо заново настроить параметры работы компонента.

- При отсутствии соединения с серверами KSN Kaspersky Endpoint Security получает информацию о репутации программ и их модулей только из локальных баз.

  Список программ, для которых Kaspersky Endpoint Security определяет KL-категорию **Программы, доверенные согласно репутации в KSN**, при наличии соединения с серверами KSN может отличаться от списка программ, для которых Kaspersky Endpoint Security определяет KL-категорию **Программы, 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 установлена программа 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 программ, то компонент не блокирует скрипт, запущенный из этого интерпретатора.

  Если запуск хотя бы одного из скриптов, указанных в командной строке интерпретатора, запрещен правилами Контроля программ, то компонент блокирует все скрипты, указанные в командной строке интерпретатора.

- Компонент не контролирует запуск скриптов из интерпретаторов, не поддерживаемых программой 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.

Включение и выключение Контроля программ

По умолчанию Контроль программ выключен.

Чтобы включить или выключить Контроль программ выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль программ**.
3. Используйте переключатель **Контроль программ**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Контроль программ включен, программа передает в Kaspersky Security Center информацию о запущенных исполняемых файлах. Вы можете просмотреть список запущенных исполняемых файлов в Kaspersky Security Center в папке **Исполняемые файлы**. Для получения информации обо всех исполняемых файлах, а не только о запущенных файлах, запустите задачу *Инвентаризация*.

Выбор режима Контроля программ

Чтобы выбрать режим Контроля программ, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .

2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль программ**.

3. В блоке **Режим контроля запуска программ** выберите один из следующих вариантов:

   - **Список запрещенных**. Если выбран этот вариант, Контроль программ разрешает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям запрещающих правил Контроля программ.

   - **Список разрешенных**. Если выбран этот вариант, Контроль программ запрещает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям разрешающих правил Контроля программ.

     Для режима Список разрешенных программ изначально заданы правила **Программы ОС** и **Доверенные программы обновления**. Эти правила Контроля программ соответствуют KL-категориям. В KL-категорию "Программы ОС" входят программы, обеспечивающие нормальную работу операционной системы. В KL-категорию "Доверенные программы обновления" входят программы обновления наиболее известных производителей программного обеспечения. Вы не можете удалить эти правила. Параметры этих правил недоступны для изменения. По умолчанию правило **Программы ОС** включено, а правило **Доверенные программы обновления** выключено. Запуск программ, соответствующих условиям срабатывания этих правил, разрешен всем пользователям.

   Все правила, сформированные при выбранном режиме, сохраняются после смены режима для возможности их повторного использования. Чтобы вернуться к использованию этих правил, достаточно выбрать нужный режим.

4. В блоке **Действие при запуске запрещенных программ** выберите, какое действие компонент должен выполнять при попытке пользователя запустить программу, запрещенную правилами Контроля программ.

5. Установите флажок **Контролировать загрузку DLL-модулей**, если вы хотите, чтобы программа Kaspersky Endpoint Security контролировала загрузку DLL-модулей при запуске пользователями программ.

   Информация о модуле и программе, загрузившей этот модуль, будет сохранена в отчет.

   Kaspersky Endpoint Security контролирует только DLL-модули и драйверы, загруженные с момента установки флажка. Перезагрузите компьютер после установки флажка, если вы хотите, чтобы программа Kaspersky Endpoint Security контролировала все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security.

   При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в параметрах Контроля программ включено правило по умолчанию **Программы ОС** или другое правило, которое содержит KL-категорию "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 **Программы ОС** может привести к нестабильности операционной системы.

Рекомендуется включить защиту паролем для настройки параметров программы, чтобы иметь возможность выключить запрещающие правила, блокирующие запуск критически важных DLL-модулей и драйверов, не изменяя при этом параметры политики Kaspersky Security Center.

6. Сохраните внесенные изменения.

Действия с правилами Контроля программ в интерфейсе программы

Kaspersky Endpoint Security контролирует запуск программ пользователями с помощью правил. В правиле Контроля программ содержатся условия срабатывания и действия компонента Контроль программ при срабатывании правила (разрешение или запрещение пользователям запускать программу).

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 программе.

В правилах используются следующие типы условий:

- *Включающие условия*. Kaspersky Endpoint Security применяет правило к программе, если программа соответствует хотя бы одному включающему условию.
- *Исключающие условия*. Kaspersky Endpoint Security не применяет правило к программе, если программа 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 программы или путь к исполняемому файлу программы;
- метаданные: название исполняемого файла программы, версия исполняемого файла программы, название программы, версия программы, производитель программы;
- хеш исполняемого файла программы;
- сертификат: издатель, субъект, отпечаток;
- принадлежность программы к KL-категории;
- расположение исполняемого файла программы на съемном диске.

Для каждого критерия, используемого в условии, нужно указать его значение. Если параметры запускаемой программы соответствуют значениям критериев, указанных во включающем условии, правило срабатывает. В этом случае Контроль программ выполняет действие, прописанное в правиле. Если параметры программы соответствуют значениям критериев, указанных в исключающем условии, Контроль программ не контролирует запуск программы.

Решения компонента Контроль программ при срабатывании правила

При срабатывании правила Контроль программ в соответствии с правилом разрешает или запрещает пользователям (группам пользователей) запускать программы. Вы можете выбирать отдельных пользователей или группы пользователей, которым разрешен или запрещен запуск программ, для которых срабатывает правило.

Если в правиле не указан ни один пользователь, которому разрешен запуск программ, удовлетворяющих правилу, правило называется *запрещающим*.

Если в правиле не указан ни один пользователь, которому запрещен запуск программ, удовлетворяющих правилу, правило называется *разрешающим*.

Приоритет запрещающего правила выше приоритета разрешающего правила. Например, если для группы пользователей назначено разрешающее правило Контроля программы и для одного из пользователей этой группы назначено запрещающее правило Контроля программы, то этому пользователю будет запрещен запуск программы.

Статус работы правила

Правила Контроля программ могут иметь один из следующих статусов работы:

- **Вкл**. Статус означает, что правило используется во время работы компонента Контроль программ.
- **Выкл**. Статус означает, что правило не используется во время работы компонента Контроль программ.
- **Тест**. Статус означает, что Kaspersky Endpoint Security разрешает запуск программ, на которые распространяется действие правила, но заносит информацию о запуске этих программ в отчет.

Добавление правила Контроля программ

Чтобы добавить правило Контроля программ, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → Контроль программ**.
3. Нажмите на кнопку **Запрещенные программы** или **Разрешенные программы**.

   Откроется список правил Контроля программ.
4. Нажмите на кнопку **Добавить**.

   Откроется окно **Правило Контроля программ**.
5. На закладке **Общие настройки** задайте основные параметры правила:

   a. В поле **Название правила** введите название правила.

   b. В поле **Описание** введите описание правила.

   c. Задайте или измените список пользователей и / или групп пользователей, которым разрешено или запрещено запускать программы, удовлетворяющие условиям срабатывания правила. Для этого нажмите на кнопку **Добавить** в таблице **Субъекты и их права**.

По умолчанию в список пользователей добавлено значение **Все**. Действие правила распространяется на всех пользователей.

Если в таблице не указан ни один пользователь, правило не может быть сохранено.

d. В таблице **Субъекты и их права** определите право пользователей на запуск программ с помощью переключателя.

e. Установите флажок **Запретить остальным пользователям**, если вы хотите, чтобы программа запрещала запуск программ, удовлетворяющих условиям срабатывания правила, всем пользователям, которые не указаны в графе **Субъект** и не входят в группы пользователей, указанные в графе **Субъект**.

Если флажок **Запретить остальным пользователям** снят, Kaspersky Endpoint Security не контролирует запуск программ пользователями, которые не указаны в таблице **Субъекты и их права** и не входят в группы пользователей, указанные в таблице **Субъекты и их права**.

f. Установите флажок **Доверенные программы обновления**, если вы хотите, чтобы программы, удовлетворяющие условиям срабатывания правила, Kaspersky Endpoint Security считал доверенными программами обновления с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

6. На закладке **Условия** сформируйте или измените список включающих условий срабатывания правила.

7. На закладке **Исключения** сформируйте или измените список исключающих условий срабатывания правила.

   При миграции параметров Kaspersky Endpoint Security осуществляется также миграция списка исполняемых файлов, созданных доверенными программами обновления.

8. Сохраните внесенные изменения.

Добавление условия срабатывания в правило Контроля программ

Чтобы добавить новое условие срабатывания в правило Контроля программ, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → Контроль программ**.

3. Нажмите на кнопку **Запрещенные программы** или **Разрешенные программы**.

   Откроется список правил Контроля программ.

4. Выберите правило, для которого вы хотите добавить условие срабатывания.

   Откроются свойства правила Контроля программ.

5. Перейдите на закладку **Условия** или **Исключения** и нажмите на кнопу **Добавить**.

6. Выберите условия срабатывания правила Контроля программ:

- **Условия из свойств запускавшихся программ**. Вы можете выбрать программы, к которым будет применено правило Контроля программ, из списка запущенных программ. Kaspersky Endpoint Security также добавляет в этот список программы, 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 папке**.

- **Условия "KL-категория"**. *KL-категория* – сформированный специалистами "Лаборатории Касперского" список программ, обладающих общими тематическими признаками. Например, KL-категория "Офисные программы" включает в себя программы из пакетов Microsoft Office, Adobe® Acrobat® и другие.

- **Условие вручную**. Вы можете выбрать файл программы 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 программ применяется только к файлам, которые запускаются на съемном диске.

- **Условия из свойств файлов указанной папки**. Привило Контроля программ 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 папке**.

7. Сохраните внесенные изменения.

При добавлении условий учитывайте следующие особенности работы Контроля программ:

- 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**. 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 программ. Для этого нажмите на кнопку **Развернуть символьную ссылку**.

Изменение статуса правила Контроля программ

Чтобы изменить статус правила Контроля программ, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → Контроль программ**.

3. Нажмите на кнопку **Запрещенные программы** или **Разрешенные программы**.

   Откроется список правил Контроля программ.

4. В графе **Статус** откройте контекстное меню и выберите один из следующих пунктов:

   - **Включено**. Статус означает, что правило используется во время работы компонента Контроль программ.

- **Выключено**. Статус означает, что правило не используется во время работы компонента Контроль программ.

- **Тестирование**. Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск программ, на которые распространяется действие этого правила, но заносит информацию о запуске этих программ в отчет.

5. Сохраните внесенные изменения.

Управление правилами Контроля программ в Kaspersky Security Center

Kaspersky Endpoint Security контролирует запуск программ пользователями с помощью правил. В правиле Контроля программ содержатся условия срабатывания и действия компонента Контроль программ при срабатывании правила (разрешение или запрещение пользователям запускать программу).

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 программе.

В правилах используются следующие типы условий:

- *Включающие условия*. Kaspersky Endpoint Security применяет правило к программе, если программа соответствует хотя бы одному включающему условию.

- *Исключающие условия*. Kaspersky Endpoint Security не применяет правило к программе, если программа 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 программы или путь к исполняемому файлу программы;

- метаданные: название исполняемого файла программы, версия исполняемого файла программы, название программы, версия программы, производитель программы;

- хеш исполняемого файла программы;

- сертификат: издатель, субъект, отпечаток;

- принадлежность программы к KL-категории;

- расположение исполняемого файла программы на съемном диске.

Для каждого критерия, используемого в условии, нужно указать его значение. Если параметры запускаемой программы соответствуют значениям критериев, указанных во включающем условии, правило срабатывает. В этом случае Контроль программ выполняет действие, прописанное в правиле. Если параметры программы соответствуют значениям критериев, указанных в исключающем условии, Контроль программ не контролирует запуск программы.

Решения компонента Контроль программ при срабатывании правила

При срабатывании правила Контроль программ в соответствии с правилом разрешает или запрещает пользователям (группам пользователей) запускать программы. Вы можете выбирать отдельных пользователей или группы пользователей, которым разрешен или запрещен запуск программ, для которых срабатывает правило.

Если в правиле не указан ни один пользователь, которому разрешен запуск программ, удовлетворяющих правилу, правило называется *запрещающим*.

Если в правиле не указан ни один пользователь, которому запрещен запуск программ, удовлетворяющих правилу, правило называется *разрешающим*.

Приоритет запрещающего правила выше приоритета разрешающего правила. Например, если для группы пользователей назначено разрешающее правило Контроля программы и для одного из пользователей этой группы назначено запрещающее правило Контроля программы, то этому пользователю будет запрещен запуск программы.

Статус работы правила

Правила Контроля программ могут иметь один из следующих статусов работы:

- **Вкл**. Статус означает, что правило используется во время работы компонента Контроль программ.
- **Выкл**. Статус означает, что правило не используется во время работы компонента Контроль программ.

Тест. Статус означает, что Kaspersky Endpoint Security разрешает запуск программ, на которые распространяется действие правила, но заносит информацию о запуске этих программ в отчет.

Получение информации о программах, которые установлены на компьютерах пользователей

Для создания оптимальных правил Контроля программ рекомендуется получить представление о программах, используемых на компьютерах локальной сети организации. Для этого вы можете получить следующую информацию:

- производители, версии и локализации программ, которые используются в локальной сети организации;
- регулярность обновлений программ;
- политики использования программ, принятые в организации (это могут быть политики безопасности или административные политики);
- расположение хранилища дистрибутивов программ.

Чтобы получить информацию о программах, которые используются на компьютерах локальной сети организации, вы можете использовать данные, представленные в папках **Реестр программ** и **Исполняемые файлы**. Папки **Реестр программ** и **Исполняемые файлы** входят в состав папки **Управление программами** дерева Консоли администрирования Kaspersky Security Center.

Папка **Реестр программ** содержит список программ, которые обнаружил на клиентских компьютерах установленный на них Агент администрирования.

Папка **Исполняемые файлы** содержит список исполняемых файлов, которые когда-либо запускались на клиентских компьютерах или были обнаружены в процессе работы задачи инвентаризации для Kaspersky Endpoint Security.

Открыв окно свойств выбранной программы в папке **Реестр программ** или **Исполняемые файлы**, вы можете получить общую информацию о программе и о ее исполняемых файлах, а также просмотреть список компьютеров, на которых установлена эта программа.

*Чтобы открыть окно свойств программы в папке **Реестр программ**, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите **Дополнительно → Управление программами → Реестр программ**.
3. Выберите программу.
4. В контекстном меню программы выберите пункт **Свойства**.

*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 программами → Исполняемые файлы**.
3. Выберите исполняемый файл.
4. В контекстном меню исполняемого файла выберите пункт **Свойства**.

Создание категорий программ

Для удобства формирования правил Контроля программ вы можете создать категории программ.

Рекомендуется создать категорию "Программы для работы", которая включает в себя стандартный набор программ, используемых в организации. Если различные группы пользователей используют различные наборы программ для работы, вы можете создать отдельную категорию программ для работы каждой группы пользователей.

Чтобы создать категорию программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Дополнительно → Управление программами → Категории программ**.
3. В рабочей области нажмите на кнопку **Создать категорию**.

   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 программ:

- **Пополняемая вручную категория**. Если вы выбрали этот тип категории, то на шаге "Настройка условий для включения программ в категорию" и шаге "Настройка условий для исключения программ из категории" вы сможете задать критерии, по которым исполняемые файлы будут попадать в категорию.

- **Категория, в которую входят исполняемые файлы с выбранных устройств**. 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**. 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 программ.

Шаг 3. Настройка условий для включения программ в категорию

Этот шаг доступен, если вы выбрали тип категории **Пополняемая вручную категория**.

На этом шаге в раскрывающемся списке **Добавить** выберите условия для включения программ в категорию:

- **Из списка исполняемых файлов**. Добавьте программы из списка исполняемых файлов на клиентском устройстве в пользовательскую категорию.

- **Из свойств файла**. Укажите детальные данные исполняемых файлов в качестве условия добавления программ 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 программ 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 программ 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 программ 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 программ в пользовательскую категорию.

- **Контрольные суммы файлов msi-инсталлятора программы**. Выберите MSI-пакет. Kaspersky Security Center укажет хеши исполняемых файлов, упакованных в этот MSI-пакет, в качестве условия добавления программ в пользовательскую категорию.

- **KL-категория**. Укажите KL-категорию в качестве условия добавления программ в пользовательскую категорию. *KL-категория* – сформированный специалистами "Лаборатории Касперского" список программ, обладающих общими тематическими признаками. Например, KL-категория "Офисные программы" включает в себя программы из пакетов Microsoft Office, Adobe Acrobat и другие.

  Вы можете выбрать все KL-категории, чтобы сформировать расширенный список доверенных программ.

- **Папка программы**. Выберите папку на клиентском устройстве. Kaspersky Security Center добавит исполняемые файлы из этой папки в пользовательскую категорию.

- **Сертификаты из хранилища сертификатов**. Выберите сертификаты, которыми подписаны исполняемые файлы, в качестве условия добавления программ в пользовательскую категорию.

  Не рекомендуется использовать условия, в свойствах которых не указывается параметр **Отпечаток сертификата**.

- **Тип носителя**. Укажите тип запоминающего устройства (все жесткие и съемные диски или только съемные диски) в качестве условия добавления программ в пользовательскую категорию.

Шаг 4. Настройка условий для исключения программ из категории

Этот шаг доступен, если вы выбрали тип категории **Пополняемая вручную категория**.

Программы, указанные на этом шаге, исключаются из категории, даже если эти программы были указаны на шаге "Настройка условий для включения программ в категорию".

На этом шаге в раскрывающемся списке **Добавить** выберите условия для исключения программ из категории:

- **Из списка исполняемых файлов**. Добавьте программы из списка исполняемых файлов на клиентском устройстве в пользовательскую категорию.

- **Из свойств файла**. Укажите детальные данные исполняемых файлов в качестве условия добавления программ 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 программ 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 программ 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 программ 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 программ в пользовательскую категорию.

- **Контрольные суммы файлов msi-инсталлятора программы**. Выберите MSI-пакет. Kaspersky Security Center укажет хеши исполняемых файлов, упакованных в этот MSI-пакет, в качестве условия добавления программ в пользовательскую категорию.

- **KL-категория**. Укажите KL-категорию в качестве условия добавления программ в пользовательскую категорию. *KL-категория* – сформированный специалистами "Лаборатории Касперского" список программ, обладающих общими тематическими признаками. Например, KL-категория "Офисные программы" включает в себя программы из пакетов Microsoft Office, Adobe Acrobat и другие.

  Вы можете выбрать все KL-категории, чтобы сформировать расширенный список доверенных программ.

- **Папка программы**. Выберите папку на клиентском устройстве. Kaspersky Security Center добавит исполняемые файлы из этой папки в пользовательскую категорию.

- **Сертификаты из хранилища сертификатов**. Выберите сертификаты, которыми подписаны исполняемые файлы, в качестве условия добавления программ в пользовательскую категорию.

- **Тип носителя**. Укажите тип запоминающего устройства (все жесткие и съемные диски или только съемные диски) в качестве условия добавления программ 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 программ. Kaspersky Security Center добавит в категорию программ все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.

Также на этом шаге вы можете настроить следующие параметры:

- Алгоритм вычисления хеш-функции программой Kaspersky Security Center. Для выбора алгоритма необходимо установить хотя бы один из следующих флажков:

  - **Вычислять SHA-256 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 **Синхронизация данных с хранилищем Сервера администрирования**. Установите этот флажок, если вы хотите, чтобы Kaspersky Security Center периодически очищал категорию программ и добавлял в нее все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.

  Если флажок **Синхронизация данных с хранилищем Сервера администрирования** снят, то после создания категории программ Kaspersky Security Center не будет вносить в нее изменения.

- Поле **Период проверки (ч)**. В поле вы можете указать период времени в часах, по истечении которого Kaspersky Security Center очищает категорию программ и добавляет в нее все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.

  Поле доступно, если установлен флажок **Синхронизация данных с хранилищем Сервера администрирования**.

Шаг 6. Папка хранилища

Этот шаг доступен, если вы выбрали тип категории **Категория, в которую входят исполняемые файлы из указанной папки**.

На этом шаге нажмите на кнопку **Обзор** и укажите папку, в которой Kaspersky Security Center будет выполнять поиск исполняемых файлов для автоматического добавления в категорию программ.

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 программ включались динамически подключаемые библиотеки (файлы формата DLL).

  При включении файлов формата DLL в категорию программ возможно снижение производительности работы Kaspersky Security Center.

- Флажок **Включать в категорию данные о скриптах**. Установите этот флажок, если вы хотите, чтобы в категорию программ включались скрипты.

  При включении скриптов в категорию программ возможно снижение производительности работы Kaspersky Security Center.

- Алгоритм вычисления хеш-функции программой Kaspersky Security Center. Для выбора алгоритма необходимо установить хотя бы один из следующих флажков:

  - **Вычислять SHA-256 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 программ.

  Если флажок **Принудительно проверять папку на наличие изменений** снят, Kaspersky Security Center выполняет поиск исполняемых файлов в папке автоматического пополнения категории программ, только если в этой папке были изменены, добавлены или удалены файлы.

- Поле **Период проверки (ч)**. В поле вы можете указать период времени в часах, по истечении которого Kaspersky Security Center выполняет поиск исполняемых файлов в папке автоматического пополнения категории программ.

  Поле доступно, если установлен флажок **Принудительно проверять папку на наличие изменений**.

Шаг 7. Создание пользовательской категории

Чтобы завершить работу мастера установки программы, нажмите на кнопку **Готово**.

Добавление в категорию программ 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 программ исполняемые файлы из папки **Исполняемые файлы**, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите **Дополнительно** → **Управление программами** → **Исполняемые файлы**.
3. В рабочей области выберите исполняемые файлы, которые вы хотите добавить в категорию программ.
4. По правой клавише мыши откройте контекстное меню для выбранных исполняемых файлов и выберите пункт **Добавить в категорию**.

   Откроется окно **Выберите категорию программ**.
5. В окне **Выберите категорию программ** выполните следующие действия:
   - В верхней части окна выберите один из следующих вариантов:
     - **Создать категорию программ**. Выберите этот вариант, если вы хотите создать новую категорию программ и добавить в нее исполняемые файлы.
     - **Добавить правила в указанную категорию**. Выберите этот вариант, если вы хотите выбрать существующую категорию программ и добавить в нее исполняемые файлы.
   - В блоке **Тип правила** выберите один из следующих вариантов:
     - **Добавить в правила включения**. Выберите этот вариант, если вы хотите создать условия, добавляющие исполняемые файлы в категорию программ.
     - **Добавить в правила исключения**. Выберите этот вариант, если вы хотите создать условия, исключающие исполняемые файлы из категории программ.
   - В блоке **Тип информации о файле** 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)**.
6. Нажмите на кнопку **OK**.

Добавление в категорию программ исполняемых файлов, связанных с событиями

Чтобы добавить в категорию программ исполняемые файлы, связанные с событиями Контроля программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **События**.
3. Выберите выборку событий о работе компонента Контроль программ (Просмотр событий по результатам работы компонента Контроль программ, Просмотр событий по результатам тестовой работы компонента Контроля программ) в раскрывающемся списке **События выборки**.
4. Нажмите на кнопку **Запустить выборку**.
5. Выберите события, в связи с которыми вы хотите добавить в категорию программ исполняемые файлы.
6. По правой клавише мыши откройте контекстное меню для выбранных событий и выберите пункт **Добавить в категорию**.

   Откроется окно **Выберите категорию программ**.
7. В окне **Выберите категорию программ** выполните следующие действия:
   - В верхней части окна выберите один из следующих вариантов:
     - **Создать категорию программ**. Выберите этот вариант, если вы хотите создать новую категорию программ и добавить в нее исполняемые файлы.
     - **Добавить правила в указанную категорию**. Выберите этот вариант, если вы хотите выбрать существующую категорию программ и добавить в нее исполняемые файлы.
   - В блоке **Тип правила** выберите один из следующих вариантов:
     - **Добавить в правила включения**. Выберите этот вариант, если вы хотите создать условия, добавляющие исполняемые файлы в категорию программ.
     - **Добавить в правила исключения**. Выберите этот вариант, если вы хотите создать условия, исключающие исполняемые файлы из категории программ.
   - В блоке **Тип информации о файле** 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. Нажмите на кнопку **OK**.

Добавление и изменение правила Контроля программ с помощью Kaspersky Security Center

Чтобы добавить или изменить правило Контроля программ с помощью Kaspersky Security Center, выполните следующие действия:

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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Контроль безопасности** → **Контроль программ**.

   В правой части окна отобразятся параметры компонента Контроль программ.
6. Выполните одно из следующих действий:

   - Если вы хотите добавить правило, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить существующее правило, выберите правило в списке и нажмите на кнопку **Изменить**.

   Откроется окно **Правило Контроля программ**.
7. 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 программ.

   - Если вы хотите изменить существующую категорию, выполните следующие действия:

     a. Из раскрывающегося списка **Категория** выберите созданную категорию программ, которую вы хотите изменить.

     b. Нажмите на кнопку **Свойства**.

        Откроется окно **Свойства: <Название категории>**.

     c. Измените параметры выбранной категории программ.

     d. Нажмите на кнопку **ОК**.

     e. Из раскрывающегося списка **Категория** выберите созданную категорию программ, на основе которой вы хотите создать правило.

8. В таблице **Субъекты и их права** нажмите на кнопку **Добавить**.

   Откроется стандартное окно Microsoft Windows **Выбор: "Пользователи" или "Группы"**.

9. В окне **Выбор: "Пользователи" или "Группы"** задайте список пользователей и / или групп пользователей, для которых вы хотите настроить возможность запускать программы, принадлежащие к выбранной категории.

10. В таблице **Субъекты и их права** выполните следующие действия:

    - Если вы хотите разрешить пользователям и / или группам пользователей запуск программ, принадлежащих к выбранной категории, установите флажок **Разрешить** в нужных строках.

    - Если вы хотите запретить пользователям и / или группам пользователей запуск программ, принадлежащих к выбранной категории, установите флажок **Запретить** в нужных строках.

11. Установите флажок **Запретить остальным пользователям**, если вы хотите, чтобы программа запрещала запуск программ, принадлежащих к выбранной категории, всем пользователям, которые не указаны в графе **Субъект** и не входят в группы пользователей, указанные в графе **Субъект**.

12. Установите флажок **Доверенные программы обновления**, если вы хотите, чтобы программы, входящие в выбранную категорию программ, Kaspersky Endpoint Security считал доверенными программами 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 программами обновления.

13. Сохраните внесенные изменения.

Изменение статуса правила Контроля программ с помощью Kaspersky Security Center

Чтобы изменить статус правила Контроля программ, выполните следующие действия:

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 закладку **Политики**.

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

5. В окне политики выберите **Контроль безопасности** → **Контроль программ**.

   В правой части окна отобразятся параметры компонента Контроль программ.

6. 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 программ.

- **Выкл**. Статус означает, что правило не используется во время работы компонента Контроль программ.
- **Тест**. Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск программ, на которые распространяется действие правила, но заносит информацию о запуске этих программ в отчет.

  С помощью статуса **Тест** вы можете назначить действие, аналогичное элементу **Тестировать правила**, для части правил, при выбранном элементе **Применять правила** в раскрывающемся списке **Действие**.

7. Сохраните внесенные изменения.

Экспорт и импорт правил Контроля программ

Вы можете экспортировать список правил Контроля программ в файл в формате XML. Вы можете использовать функцию экспорта / импорта для резервного копирования списка правил Контроля программ или для миграции списка на другой сервер.

Экспорт и импорт правил Контроля программ имеет следующие особенности:

- Kaspersky Endpoint Security экспортирует список правил только для активного режима Контроля программ. То есть, если Контроль программ 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 программ для работы правил Контроля программ. При миграции списка правил Контроля программ на другой сервер вам также нужно выполнить миграцию списка категорий программ. Подробнее об экспорте / импорте категорий программ *см. в справке Kaspersky Security Center*.

Как экспортировать / импортировать список правил Контроля программ 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Контроль безопасности** → **Контроль программ**.
6. Для экспорта списка правил Контроля программ 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 **Экспорт**.
   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. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл.
7. Для импорта списка правил Контроля программ выполните следующие действия:
   a. Нажмите на ссылку **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.
   b. Нажмите на кнопку **Открыть**.

      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 правил Контроля программ в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите экспортировать или импортировать список правил.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль программ**.
5. Перейдите по ссылке **Настройки списков правил**.
6. Выберите список правил: списки запрещенных или разрешенных программ.
7. Для экспорта списка правил Контроля программ выполните следующие действия:
   a. Выберите правила, которые вы хотите экспортировать.
   b. Нажмите на кнопку **Экспорт**.
   c. Подтвердите, что вы хотите экспортировать только выбранные правила, или экспортируйте весь список.
   d. Нажмите на кнопку **Экспорт**.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл в папку для загрузки по умолчанию.
8. Для импорта списка правил Контроля программ выполните следующие действия:
   a. Нажмите на ссылку **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.
   b. Нажмите на кнопку **Открыть**.

      Если на компьютере уже есть список правил, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
9. Сохраните внесенные изменения.

Тестирование правил Контроля программ с помощью Kaspersky Security Center

Чтобы убедиться, что правила Контроля программ не блокируют программы, необходимые для работы, рекомендуется после создания правил включить тестирование правил Контроля программ и проанализировать их работу. При включении тестирования правил Контроля программ Kaspersky Endpoint Security не будет блокировать программы, запуск которых запрещен Контролем программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

Для анализа работы правил Контроля программ требуется изучить события по результатам работы компонента Контроль программ, приходящие в Kaspersky Security Center. Если для всех программ, 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 программ, кроме программ, запрещенных правилами.

Чтобы включить или выключить тестирование правил Контроля программ в Kaspersky Security Center, выполните следующие действия:

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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Контроль безопасности** → **Контроль программ**.

   В правой части окна отобразятся параметры компонента Контроль программ.
6. В раскрывающемся списке **Режим контроля** выберите один из следующих элементов:

   - **Список запрещенных**. Если выбран этот вариант, Контроль программ разрешает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям запрещающих правил Контроля программ.
   - **Список разрешенных**. Если выбран этот вариант, Контроль программ запрещает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям разрешающих правил Контроля программ.
7. Выполните одно из следующих действий:

   - Если вы хотите включить тестирование правил Контроля программ, в раскрывающемся списке **Действие** выберите элемент **Тестировать правила**.
   - Если вы хотите включить Контроль программ для управления запуском программ на компьютерах пользователей, в раскрывающемся списке **Действие** выберите элемент **Применять правила**.
8. Сохраните внесенные изменения.

Просмотр событий по результатам тестовой работы компонента Контроля программ

Чтобы просмотреть приходящие на Kaspersky Security Center события по результатам тестовой работы компонента Контроль программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **События**.

3. Нажмите на кнопку **Создать выборку**.

   Откроется окно **Свойства: <Название выборки>**.

4. Откройте раздел **События**.

5. Нажмите на кнопку **Сбросить все**.

6. В таблице **События** установите флажки **Запуск программы запрещен в тестовом режиме** и **Запуск программы разрешен в тестовом режиме**.

7. Нажмите на кнопку **ОК**.

8. В раскрывающемся списке **События выборки** выберите созданную выборку.

9. Нажмите на кнопку **Запустить выборку**.

Просмотр отчета о запрещенных программах в тестовом режиме

Чтобы просмотреть отчет о запрещенных программах в тестовом режиме, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **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 закладке **Отчеты** появится новый шаблон отчета.

5. Откройте отчет двойным щелчком мыши.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Просмотр событий по результатам работы компонента Контроль программ

Чтобы просмотреть приходящие в Kaspersky Security Center события по результатам работы компонента Контроль программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **События**.

3. Нажмите на кнопку **Создать выборку**.

   Откроется окно **Свойства: <Название выборки>**.

4. Откройте раздел **События**.

5. Нажмите на кнопку **Сбросить все**.

6. В таблице **События** установите флажок **Запуск программы запрещен**.

7. Нажмите на кнопку **ОК**.

8. В раскрывающемся списке **События выборки** выберите созданную выборку.

9. Нажмите на кнопку **Запустить выборку**.

Просмотр отчета о запрещенных программах

Чтобы просмотреть отчет о запрещенных программах, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **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**.

   После завершения работы мастера создания шаблона отчета в таблице на закладке **Отчеты** появится новый шаблон отчета.

5. Откройте отчет двойным щелчком мыши.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Тестирование правил Контроля программ

Чтобы убедиться, что правила Контроля программ не блокируют программы, необходимые для работы, рекомендуется после создания правил включить тестирование правил Контроля программ и проанализировать их работу.

Для анализа работы правил Контроля программ требуется изучить события по результатам работы компонента Контроль программ, приходящие в Kaspersky Security Center. Если для всех программ, 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.

Чтобы включить тестирование правил Контроля программ или выбрать блокирующее действие Контроля программ, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → Контроль программ**.

   Откроется список правил Контроля программ.

3. В графе **Статус** выберите пункт **Тестирование**.

   Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск программ, на которые распространяется действие этого правила, но заносит информацию о запуске этих программ в отчет.

4. Сохраните внесенные изменения.

Kaspersky Endpoint Security не будет блокировать программы, запуск которых запрещен компонентом Контроль программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

Мониторинг активности программ

Мониторинг активности программ – это инструмент, предназначенный для просмотра информации об активности программ на компьютере пользователя в режиме реального времени.

Для работы Мониторинга активности программ вам нужно установить компоненты Контроль программ и Предотвращение вторжений. Если эти компоненты не установлены, в главном окне программы раздел Мониторинг активности программ скрыт.

Чтобы запустить мониторинг активности программ,

в главном окне программы нажмите на кнопку **Больше функций** → **Мониторинг активности программ**.

Откроется окно **Активность программ**. В этом окне информация об активности программ на компьютере пользователя представлена на трех закладках:

- На закладке **Все программы** отображается информация о всех программах, установленных на компьютере.
- На закладке **Работающие** отображается информация о потреблении ресурсов компьютера каждой из программ в режиме реального времени. На этой закладке вы можете, а также перейти к настройке разрешений для отдельной программы.
- На закладке **Запускается при старте** отображается список программ, которые запускаются при старте операционной системы.

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 программ

Когда пользователь пытается запустить программу, запрещенную правилом Контроля программ, Kaspersky Endpoint Security выводит сообщение о блокировке запуска программы. Если блокировка запуска программы, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить сообщение администратору локальной сети организации.

Для сообщения о блокировке запуска программы и сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

Чтобы изменить шаблон сообщения, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → Контроль программ**.
3. В блоке **Шаблоны** настройте шаблоны сообщений Контроля программы:
   - **Блокировка**. Шаблон сообщения, которое появляется при срабатывании правила Контроля программ, блокирующего запуск программы.
   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка программы, по мнению пользователя, произошла ошибочно.
4. Сохраните внесенные изменения.

Лучшие практики по внедрению режима списка разрешенных программ

При планировании внедрения режима списка разрешенных программ рекомендуется выполнить следующие действия:

1. Произвести следующие виды группировок:
   - Группы пользователей. Группы пользователей, для которых необходимо разрешить использование различных наборов программ.
   - Группы администрирования. Одна или несколько групп компьютеров, к которым Kaspersky Security Center будет применять режим списка разрешенных программ. Создание нескольких групп компьютеров необходимо, если для этих групп используются различные параметры режима списка разрешенных.
2. Составить список программ, 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 программ

При настройке режима списка разрешенных программ рекомендуется выполнить следующие действия:

1. Создать категории программ, содержащие те программы, запуск которых необходимо разрешить.

   Вы можете выбрать один из следующих способов формирования категорий программ:

   - **Пополняемая вручную категория**. Вы можете вручную пополнять эту категорию, используя следующие условия:

     - Метаданные файла. Kaspersky Security Center добавляет в категорию программ все исполняемые файлы, сопровождающиеся указанными метаданными.
     - Хеш файла. Kaspersky Security Center добавляет в категорию программ 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 программ все исполняемые файлы, подписанные указанным сертификатом.
     - KL-категория. Kaspersky Security Center добавляет в категорию программ все программы, входящие в указанную KL-категорию.
     - Папка программы. Kaspersky Security Center добавляет в категорию программ все исполняемые файлы из этой папки.

       Использование условия "Папка программы" небезопасно, поскольку запуск любой программы из указанной папки будет разрешен. Правила, использующие категории программ с условием "Папка программы", 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 программ.
   - **Категория, в которую входят исполняемые файлы с выбранных устройств**. Вы можете указать компьютер, все исполняемые файлы которого будут автоматически попадать в создаваемую категорию программ.

     При использовании этого способа формирования категорий программ Kaspersky Security Center получает информацию о программах на компьютере из папки **Исполняемые файлы**.

2. Выбрать режим списка разрешенных программ для компонента Контроль программ.
3. Создать правила Контроля программ с использованием созданных категорий программ.

Для режима Список разрешенных программ изначально заданы правила **Программы ОС** и **Доверенные программы обновления**. Эти правила Контроля программ соответствуют KL-категориям. В KL-категорию "Программы ОС" входят программы, обеспечивающие нормальную работу операционной системы. В KL-категорию "Доверенные программы обновления" входят программы обновления наиболее известных производителей программного обеспечения. Вы не можете удалить эти правила. Параметры этих правил недоступны для изменения. По умолчанию правило **Программы ОС** включено, а правило **Доверенные программы обновления** выключено. Запуск программ, соответствующих условиям срабатывания этих правил, разрешен всем пользователям.

Операционная система и ее компоненты

4. Определить те программы, для которых необходимо разрешить автоматическую установку обновлений.

   Вы можете разрешить автоматическую установку обновлений одним из следующих способов:

   - Указать расширенный список разрешенных программ, разрешив запуск всех программ, входящих в любую из KL-категорий.
   - Указать расширенный список разрешенных программ, разрешив запуск всех программ, подписанных сертификатами.

     Чтобы разрешить запуск всех программ, подписанных сертификатами, вы можете создать категорию с условием на основе сертификата, в котором используется только параметр **Субъект** со значением *.
   - Для правила Контроля программ установить параметр **Доверенные программы обновления**. Если этот флажок установлен, то Kaspersky Endpoint Security будет считать программы, входящие в правило, доверенными программами обновления. Kaspersky Endpoint Security разрешает запуск программ, которые были установлены или обновлены программами, входящими в правило. При этом программы не должны попадать под действие запрещающих правил.

     При миграции параметров Kaspersky Endpoint Security осуществляется также миграция списка исполняемых файлов, созданных доверенными программами обновления.
   - Создать папку и поместить в нее исполняемые файлы программ, для которых вы хотите разрешить автоматическую установку обновлений. Далее создать категорию программ с условием "Папка программы" и указать путь к этой папке. Далее создать разрешающее правило и выбрать эту категорию.

     Использование условия "Папка программы" небезопасно, поскольку запуск любой программы из указанной папки будет разрешен. Правила, использующие категории программ с условием "Папка программы", рекомендуется применять только к тем пользователям, для которых необходимо разрешить автоматическую установку обновлений.

Тестирование режима списка разрешенных программ

Чтобы убедиться, что правила Контроля программ не блокируют программы, необходимые для работы, рекомендуется после создания правил включить тестирование правил Контроля программ и проанализировать их работу. При включении тестирования Kaspersky Endpoint Security не будет блокировать программы, запуск которых запрещен правилами Контроля программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

При тестировании режима списка разрешенных программ рекомендуется выполнить следующие действия:

1. Определить период тестирования (от нескольких дней до двух месяцев).
2. Включить тестирование правил Контроля программ.
3. Проанализировать результаты тестирования, используя события по результатам тестовой работы Компонента программ и отчеты о запрещенных программах в тестовом режиме.
4. По результатам анализа внести изменения в параметры режима списка разрешенных программ.

   В частности, по результатам тестирования вы можете добавить в категорию программ исполняемые файлы, связанные с событиями.

Поддержка режима списка разрешенных программ

После выбора блокирующего действия Контроля программ рекомендуется продолжать поддержку режима списка разрешенных программ, выполняя следующие действия:

- Анализировать работу правил Контроля программ, используя события по результатам работы Контроля программ и отчеты о запрещенных запусках.
- Анализировать запросы доступа к программам, 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 программ.
- Добавлять необходимые программы в категории, используемые в правилах Контроля программ.

Контроль сетевых портов

Во время работы Kaspersky Endpoint Security компоненты Веб-Контроль, Защита от почтовых угроз, Защита от веб-угроз 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 программ, 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.

Включение контроля всех сетевых портов

Чтобы включить контроль всех сетевых портов, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Настройки сети**.
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 нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **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 программ, с помощью которых устанавливается FTP-соединение.

Формирование списка программ, для которых контролируются все сетевые порты

Вы можете сформировать список программ, для которых Kaspersky Endpoint Security контролирует все сетевые порты.

В список программ, для которых Kaspersky Endpoint Security контролирует все сетевые порты, рекомендуется включить программы, которые принимают или передают данные по протоколу FTP.

Чтобы сформировать список программ, для которых контролируются все сетевые порты, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.
4. Установите флажок **Контролировать все порты для программ из списка, рекомендованного "Лабораторией Касперского"**.

   Если установлен этот флажок, Kaspersky Endpoint Security контролирует все порты для следующих программ:

   - Adobe 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 программ**.
6. Нажмите на кнопку **Выбрать**.

   Откроется список программ, сетевые порты которых контролирует Kaspersky Endpoint Security.
7. Используйте переключатель в графе **Статус**, чтобы включить или выключить контроль сетевых портов.
8. Если программа отсутствует в списке программ, добавьте ее следующим образом:

a. Нажмите на кнопку **Добавить**.

b. В открывшемся окне укажите путь к исполняемому файлу программы 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 программ, 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Общие настройки** → **Настройки сети**.
6. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.
7. 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.
8. 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 **Экспорт**.

   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. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список сетевых портов в XML-файл.
9. Для экспорта списка программ, порты которых контролирует Kaspersky Endpoint Security, выполните следующие действия:

   a. Установите флажок **Контролировать все порты для указанных программ**.

   b. В списке программ выберите программы, которые вы хотите экспортировать. Чтобы выбрать несколько записей, используйте клавиши **CTRL** или **SHIFT**.

      Если вы не выбрали ни одной программы, Kaspersky Endpoint Security экспортирует все программы.

   c. Нажмите на кнопку **Экспорт**.

   d. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список программ, а также выберите папку, в которой вы хотите сохранить этот файл.

   e. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список программ в XML-файл.
10. 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. Нажмите на кнопку **Открыть**.

Если на компьютере уже есть список сетевых портов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

11. Для импорта списка программ, порты которых контролирует Kaspersky Endpoint Security, выполните следующие действия:

a. В списке программ нажмите на кнопку **Импорт**.

В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список программ.

b. Нажмите на кнопку **Открыть**.

Если на компьютере уже есть список программ, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

12. Сохраните внесенные изменения.

[Как экспортировать /импортировать списки контролируемых портов в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства → Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите экспортировать или импортировать списки контролируемых портов.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
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. Нажмите на кнопку **Сохранить**.

   Kaspersky Endpoint Security экспортирует список сетевых портов в XML-файл.
6. Для экспорта списка программ, порты которых контролирует Kaspersky Endpoint Security, выполните следующие действия:

   a. В блоке **Контролируемые порты** установите флажок **Контролировать все порты для указанных программ**.

   b. Перейдите по ссылке **Выбрано N программ**.

   c. В списке программ выберите программы, которые вы хотите экспортировать.

   d. Нажмите на кнопку **Экспорт**.

   e. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список программ, а также выберите папку, в которой вы хотите сохранить этот файл.

   f. Нажмите на кнопку **Сохранить**.

   Kaspersky Endpoint Security экспортирует список программ 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. Нажмите на кнопку **Открыть**.

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 программ, порты которых контролирует Kaspersky Endpoint Security, выполните следующие действия:

a. В списке программ нажмите на кнопку **Импорт**.

В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список программ.

b. Нажмите на кнопку **Открыть**.

Если на компьютере уже есть список программ, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

9. Сохраните внесенные изменения.

Managed Detection and Response

В Kaspersky Endpoint Security версии 11.6.0 добавлен компонент Managed Detection and Response. Компонент обеспечивает взаимодействие с решением Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию. Подробную информацию о работе решения *см. в справке Kaspersky Managed Detection and Response*.

При взаимодействии с Kaspersky Managed Detection and Response программа позволяет выполнять следующие функции:

- Активация Managed Detection and Response с помощью конфигурационного файла BLOB.
- Выполнение команд от Kaspersky Managed Detection and Response.
- Отправка данных телеметрии для обнаружения угроз в Kaspersky Managed Detection and Response.

Интеграция с Kaspersky Managed Detection and Responce

Интеграция с Kaspersky Managed Detection and Response состоит из следующих этапов:

1. **Настройка Локального Kaspersky Security Network**

   Если вы используете Kaspersky Security Center Cloud Console, этот шаг нужно пропустить. Kaspersky Security Center Cloud Console автоматически настраивает Локальный Kaspersky Security Network при установке плагина MDR.

   Локальный KSN обеспечивает обмен данными между компьютерами и выделенными серверами Kaspersky Security Network, а не Глобальным KSN.

   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 Локального Kaspersky 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 Локальный Kaspersky Security Network из 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:

   ```
   avp.com KSN /private <имя файла>
   ```

   где `<имя файла>` – имя конфигурационного файла с параметрами Локального KSN (формат файла PKCS7 или PEM).

   Пример:

   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

В результате Kaspersky Endpoint Security будет использовать Локальный KSN для определения репутации файлов, программ и веб-сайтов. В параметрах политики в разделе **Kaspersky Security Network** будет указан статус работы *Сеть KSN: Локальный KSN*.

Для работы Managed Detection and Response необходимо включить расширенный режим KSN.

2 **Активация 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*.

Как активировать Managed Detection and Response 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Расширения защиты** → **Detection and Response**.
6. Установите флажок **Managed Detection and Response**.
7. В блоке **Настройка** нажмите на кнопку **Импорт** и выберите BLOB-файл, полученный в Консоли Kaspersky Managed Detection and Response. Файл имеет расширение P7.
8. Сохраните внесенные изменения.

Как активировать Managed Detection and Response в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Расширения защиты** → **Detection and Response**.
5. Включите переключатель **Managed Detection and Response**.
6. Нажмите на кнопку **Импорт** и выберите BLOB-файл, полученный в Консоли Kaspersky Managed Detection and Response. Файл имеет расширение P7.
7. Сохраните внесенные изменения.

[Как активировать Managed Detection and Response из 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:

   - Если настройка параметров программы не защищена паролем:

     `avp.com MDRLICENSE /ADD <имя файла>`

     где `<имя файла>` – имя конфигурационного файла BLOB для активации Managed Detection and Response (формат файла P7).

   - Если настройка параметров программы защищена паролем:

     `avp.com MDRLICENSE /ADD <имя файла> /login=<имя пользователя> /password=<пароль>`

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 программы*. 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**.

Для работы Managed Detection and Response должны быть включены следующие компоненты:

- Kaspersky Security Network (расширенный режим).
- Анализ поведения.

Эти компоненты должны быть включены обязательно. В противном случае Kaspersky Managed Detection and Response не работает, так как не получает необходимые данные телеметрии.

Дополнительно Kaspersky Managed Detection and Response использует данные полученные от других компонентов программы. Включение этих компонентов не является обязательным. К компонентам, которые предоставляют дополнительные данные, относятся следующие компоненты:

- Защита от веб-угроз.
- Защита от почтовых угроз.
- Сетевой экран.

Миграция из Kaspersky Endpoint Agent на Kaspersky Endpoint Security для Windows

Программа Kaspersky Endpoint Security версии 11 или выше поддерживает работу с решением MDR. Kaspersky Endpoint Security версий 11 – 11.5.0 только отправляет данные телеметрии для обнаружения угроз в Kaspersky Managed Detection and Response. Kaspersky Endpoint Security версии 11.6.0 выполняет все функции встроенного агента (Kaspersky Endpoint Agent).

Если вы используете Kaspersky Endpoint Security 11 – 11.5.0, для работы с решением MDR нужно обновить базы до актуальной версии. Также требуется установить Kaspersky Endpoint Agent.

Если вы используете Kaspersky Endpoint Security 11.6.0 или выше, для работы с решением MDR нужно выбрать компонент Managed Detection and Response при установке программы. Устанавливать Kaspersky Endpoint Agent при этом не требуется.

Для миграции из Kaspersky Endpoint Agent на Kaspersky Endpoint Security для Windows вам нужно выполнить следующие действия:

1. Настройте интеграцию с Kaspersky Managed Detection and Response в политике Kaspersky Endpoint Security.
2. Выключите компонент Managed Detection and Response в политике Kaspersky Endpoint Agent.

Если политика Kaspersky Endpoint Security также применяется к компьютерам, на которых установлена программа Kaspersky Endpoint Security 11 – 11.5.0, необходимо сначала создать отдельную политику Kaspersky Endpoint Agent для этих компьютеров. В новой политике необходимо настроить интеграцию с Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent обеспечивает взаимодействие программы 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.

Полную информацию о Kaspersky Endpoint Agent для Windows 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*.

Kaspersky Endpoint Agent входит в комплект поставки Kaspersky Endpoint Security. Вы можете установить Kaspersky Endpoint Agent при установке Kaspersky Endpoint Security. Для этого вам нужно выбрать компонент Endpoint Agent при установке программы (например, в инсталляционном пакете). После установки программы с компонентом Endpoint Agent в список установленных программ будут добавлены Kaspersky Endpoint Security и Kaspersky Endpoint Agent. После удаления Kaspersky Endpoint Security, программа Kaspersky Endpoint Agent также будет удалена автоматически.

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 **Устройства** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Security для Windows (11.6.0)**.

   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 **Выбор устройств, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.

   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 по кнопке **Готово**.

   В списке задач отобразится новая задача.

6. Нажмите на задачу Kaspersky Endpoint Security **Удаление данных**.

   Откроется окно свойств задачи.

7. Выберите закладку **Параметры программы**.

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, например, выключить компьютер перед уходом в отпуск. В этом случае срок отсутствия связи может быть превышен и данные будут удалены. Также учитывайте график работы автономных пользователей. Подробнее о работе с автономными компьютерами и автономными пользователями *см. в справке Kaspersky Security Center*.

   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 программ. Например, программы 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 закладок. 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. Нажмите на кнопку **Сохранить**.

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, программа не пытается удалить его снова. Для завершения удаления данных повторите запуск задачи.

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 программы).

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 программе следующими способами:

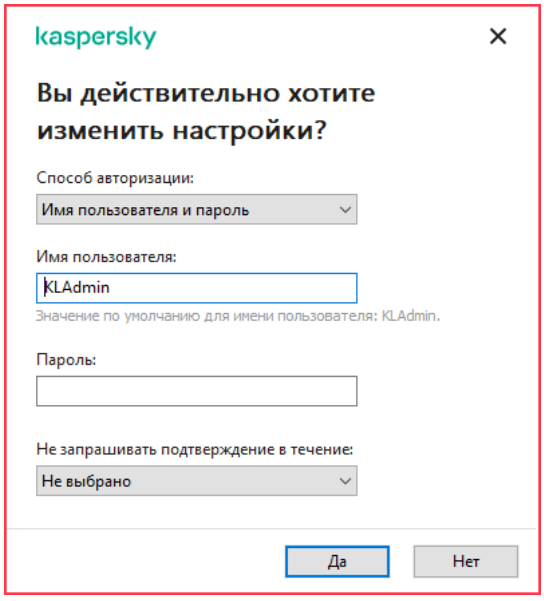
- Ввод имени пользователя и пароля.

  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.

- 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 программы). По истечении срока действия временного пароля или истечении сессии программа возвращает параметры Kaspersky Endpoint Security в прежнее состояние.

При попытке пользователя выполнить действие, защищенное паролем, Kaspersky Endpoint Security предложит пользователю ввести имя пользователя и пароль или временный пароль (см. рис. ниже).



Запрос пароля для доступа к Kaspersky Endpoint Security

Имя пользователя и пароль

Для доступа к Kaspersky Endpoint Security необходимо ввести данные доменной 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.

- **Группа "Все"**. Стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети. Пользователи из группы "Все" могут получить доступ к программе 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.

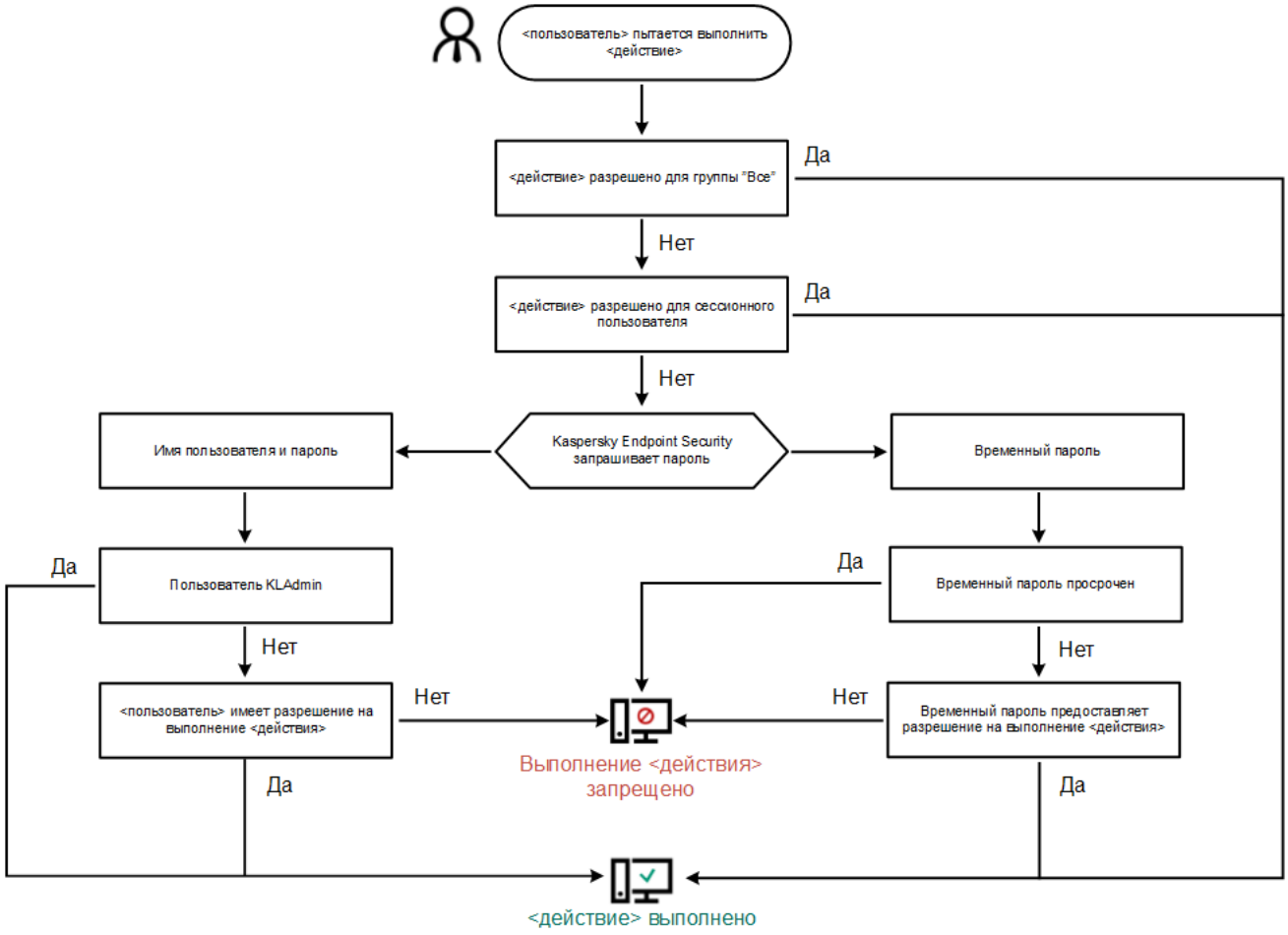
- **Сессионный пользователь**. Учетная запись пользователя, который запустил сессию Windows. Вы можете сменить сессионного пользователя во время ввода пароля (флажок **Запомнить пароль на текущую сессию**). В этом случае Kaspersky Endpoint Security назначает сессионным пользователем, учетные данные которого 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.

Алгоритм работы Защиты паролем

Kaspersky Endpoint Security принимает решение о выполнении действия, защищенного паролем, по следующему алгоритму (см. рис. ниже).



Алгоритм работы Защиты паролем

Включение Защиты паролем

Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы программы).

Чтобы включить Защиту паролем, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

   В окне параметров программы выберите раздел **Интерфейс**.

2. Используйте переключатель **Защита паролем**, чтобы включить или выключить компонент.

3. 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.

4. Настройте разрешения для всех пользователей внутри корпоративной сети:

   a. В таблице **Разрешения** 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 программы** снят, вы можете завершить работу программы 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.

c. Нажмите на кнопку **OK**.

5. Сохраните внесенные изменения.

После включения Защиты паролем программа ограничит доступ пользователей к Kaspersky Endpoint Security в соответствии в 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

Вы можете предоставить доступ к Kaspersky Endpoint Security для отдельных пользователей или групп. Например, если группе "Все" запрещено завершать работу программы, вы можете предоставить отдельному пользователю разрешение **Завершение работы программы**. В результате вы можете завершить работу программы только с помощью учетной записи этого пользователя или учетной записи KLAdmin.

> Вы можете использовать данные учетной записи для доступа к программе, только если компьютер в домене. Если компьютер не в домене, вы можете использовать учетную запись KLAdmin или временный пароль.

Чтобы предоставить разрешение для отдельных пользователей или групп, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

В окне параметров программы выберите раздел **Интерфейс**.

2. В таблице **Защита паролем** нажмите на кнопку **Добавить**.

3. В открывшемся окне нажмите на кнопку **Выбрать пользователя**.

Откроется стандартное окно Windows для выбора пользователей или групп.

4. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.

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 программы** снят, вы можете завершить работу программы 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 программе 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.

Чтобы предоставить пользователю разрешение на выполнение запрещенного действия с помощью временного пароля, выполните следующие действия:

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 закладку **Устройства**.

4. Откройте свойства компьютера двойным щелчком мыши.

5. В окне свойств компьютера выберите раздел **Программы**.

6. В списке установленных на компьютере программ "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows** и откройте свойства программы двойным щелчком мыши.

7. В окне параметров программы выберите раздел **Общие настройки → Интерфейс**.

8. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

   Откроется окно **Защита паролем**.

9. В блоке **Временный пароль** нажмите на кнопку **Настройка**.

   Откроется окно **Создание временного пароля**.

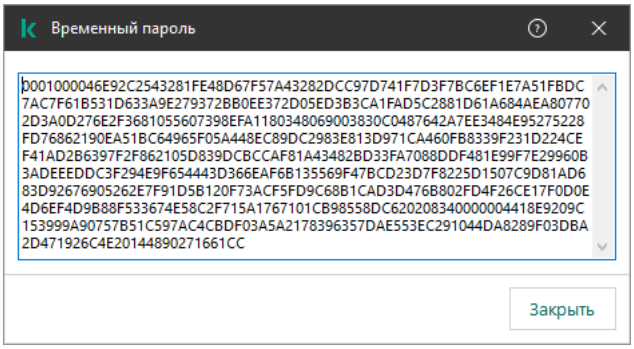
10. В поле **Дата истечения** установите срок действия временного пароля.

11. В таблице **Область действия временного пароля** установите флажки напротив тех действий, которые будут доступны пользователю после ввода временного пароля.

12. Нажмите на кнопку **Создать**.

    Откроется окно с временным паролем (см. рис. ниже).

13. Скопируйте и передайте пользователю пароль.



Временный пароль

Особенности разрешений Защиты паролем

Разрешения Защиты паролем имеют ряд особенностей и ограничений.

Настройка параметров программы

Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты открыты).

Завершение работы программы

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 KLAdmin, 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 программы пользователь должен иметь разрешение **Настройка параметров программы**.
- 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 KLAdmin, 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 программы пользователь должен иметь разрешение **Настройка параметров программы**.

- 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 KLAdmin, 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 программы

Если вы предоставили разрешение на удаление, изменение и восстановление программы 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 программу.

Восстановление доступа к данным на зашифрованных устройствах

Вы можете восстановить доступ к данным на зашифрованных устройствах только с помощью учетной записи KLAdmin. Разрешить это действие другому пользователю невозможно.

Просмотр отчетов

Особенностей и ограничений нет.

Восстановление из резервного хранилища

Особенностей и ограничений нет.

Доверенная зона

Доверенная зона – это сформированный администратором системы список объектов и программ, 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 программ, установленных на компьютере. Включение объектов и программ в доверенную зону может потребоваться, например, если Kaspersky Endpoint Security блокирует доступ к какому-либо объекту или программе, в то время как вы уверены, что этот объект или программа 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 программ.

Создание исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Endpoint Security не проверяет объект на вирусы и другие программы, представляющие угрозу.

Исключения из проверки позволяют работать с легальными программами, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы злоумышленниками. Подробную информацию о легальных программах, 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 программы могут быть заблокированы. Чтобы избежать блокирования, для используемых программ 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 программу Radmin, предназначенную для удаленного управления компьютерами. Такая активность программы рассматривается Kaspersky Endpoint Security как подозрительная и может быть заблокирована. Чтобы исключить блокировку программы, нужно сформировать исключение из проверки, где указать название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского".

Если у вас на компьютере установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Endpoint Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из проверки, настроив Kaspersky Endpoint Security способом, описанным в этом документе.

Исключения из проверки могут использоваться в ходе работы следующих компонентов и задач программы, заданных администратором системы:

- Анализ поведения.
- Защита от эксплойтов.
- Предотвращение вторжений.
- Защита от файловых угроз.
- Защита от веб-угроз.
- Защита от почтовых угроз.

- Задачи проверки.

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 папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Общие настройки** → **Исключения**.
6. В блоке **Исключения из проверки и доверенные программы** нажмите на кнопку **Настройка**.
7. В окне **Доверенная зона** выберите закладку **Исключения из проверки**.

   Откроется окно со списком исключений.
8. 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.
9. 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. Если локальный список сформирован, после выключения функции Kaspersky Endpoint Security продолжает исключать из проверки файлы из списка.
10. Нажмите на кнопку **Добавить**.
11. Если вы хотите исключить из проверки файл или папку, выполните следующие действия:

    a. В блоке **Свойства** установите флажок **Файл или папка**.

    b. По ссылке **выберите файл или папку**, расположенной в блоке **Описание исключения из проверки**, откройте окно **Имя файла или папки**.

    c. 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 папке `Folder` и вложенных папках. 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.

d. Нажмите на кнопку **OK** в окне **Имя файла или папки**.

Ссылка на добавленный файл или папку появится в блоке **Описание исключения из проверки** окна **Исключение из проверки**.

12. Если вы хотите исключить из проверки объекты с определенным названием, выполните следующие действия:

a. В блоке **Свойства** установите флажок **Название объекта**.

b. По ссылке **введите название объекта**, расположенной в блоке **Описание исключения из проверки**, откройте окно **Название объекта**.

c. 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`.

d. Нажмите на кнопку **OK** в окне **Название объекта**.

Ссылка на добавленное название объекта появится в блоке **Описание исключения из проверки** окна **Исключение из проверки**.

13. Если вы хотите исключить из проверки отдельный файл, выполните следующие действия:

a. В блоке **Свойства** установите флажок **Хеш объекта**.

b. По ссылке введите хеш объекта откройте окно **Хеш объекта**.

c. 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.

d. Нажмите на кнопку **OK** в окне **Хеш объекта**.

Ссылка на добавленный объект появится в блоке **Описание исключения из проверки** окна **Исключение из проверки**.

14. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

15. Определите компоненты Kaspersky Endpoint Security, в работе которых должно быть использовано исключение из проверки:

a. По ссылке **любые**, расположенной в блоке **Описание исключения из проверки**, активируйте ссылку **выберите компоненты**.

b. По ссылке **выберите компоненты** откройте окно **Компоненты защиты**.

c. Установите флажки напротив тех компонентов, на работу которых должно распространяться исключение из проверки.

d. Нажмите на кнопку **OK** в окне **Компоненты защиты**.

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.

16. Вы можете в любое время остановить работу исключения с помощью флажка.

17. Сохраните внесенные изменения.

Как создать исключение из проверки в Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства → Политики и профили политик**.

2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите добавить исключение.

   Откроется окно свойств политики.

3. Выберите закладку **Параметры программы**.

4. Перейдите в раздел **Общие настройки → Исключения**.

5. В блоке **Исключения из проверки и доверенные программы** перейдите по ссылке **Исключения из проверки**.

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. Если локальный список сформирован, после выключения функции Kaspersky Endpoint Security продолжает исключать из проверки файлы из списка.

8. Нажмите на кнопку **Добавить**.

9. Выберите способ добавления исключения: **Файл или папка**, **Название объекта** или **Хеш объекта**.

10. 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 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 папке `Folder` и вложенных папках. 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.

11. Если вы хотите исключить из проверки тип объектов, в поле **Объект** 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 файла** введите хеш файла.

    Если файл изменится, хеш файла тоже будет изменен. В результате измененный файл не будет добавлен в исключения.

13. В блоке **Компоненты защиты** 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. Вы можете в любое время остановить работу исключения с помощью переключателя.

16. Сохраните внесенные изменения.

Как создать исключение из проверки в интерфейсе программы

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Исключения** перейдите по ссылке **Настроить исключения**.
4. Нажмите на кнопку **Добавить**.
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 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 папке `Folder` и вложенных папках. 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.
6. Если вы хотите исключить из проверки тип объектов, в поле **Объект** 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 файла** 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**.

    Вы можете в любое время остановить работу исключения с помощью переключателя.
11. Сохраните внесенные изменения.

Примеры масок пути:
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\, но не в подпапках папки C:\dir\;
- маска `C:\dir\` будет включать все пути к файлам в папке C:\dir\, но не в подпапках папки C:\dir\;
- 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\.

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.

Запуск и остановка работы исключения из проверки

Чтобы запустить или остановить работу исключения из проверки, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Исключения** перейдите по ссылке **Настроить исключения**.
4. В списке исключений из проверки выберите нужное исключение.
5. Используйте переключатель рядом с объектом, чтобы включить или исключить объект из проверки.
6. Сохраните внесенные изменения.

Формирование списка доверенных программ

Список доверенных программ – это список программ, у которых Kaspersky Endpoint Security не контролирует файловую и сетевую активность (в том числе и вредоносную), а также обращения этих программ к системному реестру. По умолчанию Kaspersky Endpoint Security проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и создаваемый ими сетевой трафик. Kaspersky Endpoint Security исключает из проверки программу, добавленную в список доверенных программ.

Например, если вы считаете объекты, используемые программой Microsoft Windows Блокнот, безопасными и не требующими проверки, то есть доверяете этой программе, вам следует добавить программу Microsoft Windows Блокнот в список доверенных программ, чтобы не проверять объекты, используемые этой программой.

Кроме того, некоторые действия, которые Kaspersky Endpoint Security классифицирует как подозрительные, могут быть безопасны в рамках функциональности ряда программ. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием программ автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких программ и отключить контроль их активности, рекомендуется добавить их в список доверенных программ.

Исключение доверенных программ из проверки позволяет избежать проблемы совместимости Kaspersky Endpoint Security с другими программами (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky Endpoint Security и другой антивирусной программой), а также увеличить производительность компьютера, что особенно важно при использовании серверных программ.

В то же время исполняемый файл и процесс доверенной программы по-прежнему проверяются на наличие в них вирусов и других программ, представляющих угрозу. Для полного исключения программы из проверки Kaspersky Endpoint Security следует пользоваться исключениями из проверки.

Как добавить программу в список доверенных 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Общие настройки** → **Исключения**.
6. В блоке **Исключения из проверки и доверенные программы** нажмите на кнопку **Настройка**.
7. В окне **Доверенная зона** выберите закладку **Доверенные программы**.

   Откроется окно со списком доверенных программ.
8. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных программ для всех компьютеров организации. Списки доверенных программ родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные программы родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных программ родительской политики невозможно.
9. Установите флажок **Разрешить использование локальных доверенных программ**, если вы хотите чтобы у пользователя была возможность создать локальный список доверенных программ. Таким образом, кроме общего списка доверенных программ, сформированного в политике, пользователь может создавать собственный локальный список доверенных программ. 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 программ, сформированный в политике. Если локальный список сформирован, после выключения функции Kaspersky Endpoint Security продолжает исключать из проверки доверенные программы из списка.
10. Нажмите на кнопку **Добавить**.
11. В открывшемся окне введите путь к исполняемому файлу доверенной программы.

    Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

    > Kaspersky Endpoint Security не поддерживает переменную среды `%userprofile%` при формировании списка доверенных программ 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 программу.
12. Настройте дополнительные параметры доверенной программы (см. таблицу ниже).
13. Вы можете в любое время исключить программу из доверенной зоны с помощью флажка.
14. Сохраните внесенные изменения.

[Как добавить программу в список доверенных в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите добавить программу в список доверенных.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Общие настройки** → **Исключения**.
5. В блоке **Исключения из проверки и доверенные программы** перейдите по ссылке **Доверенные программы**.

   Откроется окно со списком доверенных программ.
6. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных программ для всех компьютеров организации. Списки доверенных программ родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные программы родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных программ родительской политики невозможно.
7. Установите флажок **Разрешить использование локальных доверенных программ**, если вы хотите чтобы у пользователя была возможность создать локальный список доверенных программ. Таким образом, кроме общего списка доверенных программ, сформированного в политике, пользователь может создавать собственный локальный список доверенных программ. 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 программ, сформированный в политике. Если локальный список сформирован, после выключения функции Kaspersky Endpoint Security продолжает исключать из проверки доверенные программы из списка.
8. Нажмите на кнопку **Добавить**.
9. В открывшемся окне введите путь к исполняемому файлу доверенной программы.

   Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

   > Kaspersky Endpoint Security не поддерживает переменную среды `%userprofile%` при формировании списка доверенных программ 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 программу.
10. Настройте дополнительные параметры доверенной программы (см. таблицу ниже).
11. Вы можете в любое время [исключить программу из доверенной зоны] с помощью флажка.
12. Сохраните внесенные изменения.

[Как добавить программу в список доверенных в интерфейсе программы](#)

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Исключения** перейдите по ссылке **Указать доверенные программы**.
4. В открывшемся окне нажмите на кнопку **Добавить**.
5. Выберите исполняемый файл доверенной программы.

   Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

   > Kaspersky Endpoint Security поддерживает переменные среды. При этом Kaspersky Endpoint Security конвертирует путь в локальном интерфейсе программы. То есть, если вы ввели путь к файлу `%userprofile%\Documents\File.exe`, в локальном интерфейсе программы для пользователя Fred123 будет добавлена запись `C:\Users\Fred123\Documents\File.exe`. Соответственно, Kaspersky Endpoint Security игнорирует доверенную программу `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 программу.

6. В окне свойств доверенной программы настройте дополнительные параметры (см. таблицу ниже).
7. Вы можете в любое время [исключить программу из доверенной зоны](#) с помощью переключателя.
8. Сохраните внесенные изменения.

Параметры доверенной программы

Параметр	Описание
Не проверять открываемые файлы	Kaspersky Endpoint Security исключает из проверки все файлы, открываемые с помощью программы. Например, если вы используете программы резервного копирования файлов, функция позволит снизить потребление ресурсов компьютера Kaspersky Endpoint Security.
Не контролировать активность программы	Kaspersky Endpoint Security не контролирует файловую и сетевую активности программы в операционной системе. Контроль за активностью программы выполняют следующие компоненты: [Анализ поведения](#), [Защита от эксплойтов](#), [Предотвращение вторжений](#), [Откат вредоносных действий](#) и [Сетевой экран](#).
Не наследовать ограничения родительского процесса (программы)	Kaspersky Endpoint Security не применяет ограничения к процессу, которые настроены для родительского процесса. Родительский процесс запускает программа, для которой настроены [права программы](#) (Предотвращение вторжений) и [сетевые правила программы](#) (Сетевой экран).
Не контролировать активность	Kaspersky Endpoint Security не контролирует файловую и сетевую активности программ, которые запускает программа.

дочерних программ	
Разрешить взаимодействие с интерфейсом Kaspersky Endpoint Security	Самозащита Kaspersky Endpoint Security блокирует все попытки управления службами программы с удаленного компьютера. Если флажок установлен, то программе удаленного доступа к компьютеру разрешено управлять параметрами Kaspersky Endpoint Security через интерфейс Kaspersky Endpoint Security.
Не блокировать взаимодействие с компонентом AMSI-защита *(доступен только в консоли Kaspersky Security Center)*	Kaspersky Endpoint Security не контролирует запросы доверенной программы на проверку объектов компонентом AMSI-защита.
Не проверять зашифрованный трафик / Не проверять весь трафик	Kaspersky Endpoint Security исключает из проверки сетевой трафик, инициируемый программой. Вы можете исключить из проверки весь трафик или только зашифрованный трафик. Также вы можете исключить из проверки отдельные IP-адреса или номера портов.
Комментарий	Если необходимо, вы можете ввести краткий комментарий к доверенной программе. Комментарий позволяет упростить поиск и сортировку доверенных программ.
Статус	Статус доверенной программы: • **Активно** – программа в доверенной зоне. • **Неактивно** – программа исключена из доверенной зоны.

Включение и выключение действия правил доверенной зоны на программу из списка доверенных программ

Чтобы включить или выключить действие правил доверенной зоны на программу из списка доверенных программ, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Исключения** перейдите по ссылке **Указать доверенные программы**.
4. В списке доверенных программ выберите нужную доверенную программу.
5. Используйте переключатель в графе **Статус**, чтобы включить или исключить доверенную программу из проверки.
6. Сохраните внесенные изменения.

Использование доверенного системного хранилища сертификатов

Использование системного хранилища сертификатов позволяет исключать из антивирусной проверки программы, подписанные доверенной цифровой подписью. Kaspersky Endpoint Security автоматически помещает такие программы в группу *Доверенные*.

Чтобы начать использовать доверенное системное хранилище сертификатов, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В раскрывающемся списке **Доверенное системное хранилище сертификатов** выберите, какое системное хранилище Kaspersky Endpoint Security должен считать доверенным.
4. Сохраните внесенные изменения.

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\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 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Отчеты и хранилище**.
3. В блоке **Резервное хранилище** установите флажок **Хранить объекты не более N дней**, если хотите ограничить срок хранения копий файлов в резервном хранилище. В поле справа от флажка **Хранить объекты не более N дней** 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 таким образом, чтобы не превышался его максимальный размер.

Чтобы настроить максимальный размер резервного хранилища, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Отчеты и хранилище**.
3. В блоке **Резервное хранилище** установите флажок **Ограничить размер хранилища до N МБ**, если вы хотите ограничить размер резервного хранилища. Укажите максимальный размер резервного хранилища.
4. Сохраните внесенные изменения.

Восстановление файлов из резервного хранилища

Если в файле обнаружен вредоносный код, Kaspersky Endpoint Security блокирует файл, присваивает ему статус *Заражен*, 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 вылечен 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 Microsoft Windows 8 (подробную информацию о восстановлении приложения Windows Store читайте в *Справочной системе к Microsoft Windows 8*).

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 программы нажмите на кнопку **Больше функций** → **Хранилище**.

   Откроется окно **Резервное хранилище**.
2. В таблице в окне **Резервное хранилище** выберите один или несколько файлов резервного хранилища.
3. Нажмите на кнопку **Восстановить**.

Kaspersky Endpoint Security восстановит файлы из выбранных резервных копий в папки их исходного размещения.

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 программы. 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 программы нажмите на кнопку **Больше функций** → **Хранилище**.

   Откроется окно **Резервное хранилище**.

2. Выберите резервные копии файлов, которые вы хотите удалить из резервного хранилища, и нажмите на кнопку **Удалить**. Также вы можете удалить все файлы из резервного хранилища по кнопке **Удалить все**.

Kaspersky Endpoint Security удалит выбранные резервные копии файлов из резервного хранилища.

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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Интерфейс**.
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 **Журналах приложений и служб** в разделе **Журнал событий Kaspersky**. События, напротив которых установлен флажок в графе **Сохранять в журнале событий Windows**, отображаются в **Журналах Windows** в разделе **Приложение**. Чтобы открыть журналы событий, выберите **Пуск → Панель управления → Администрирование → Просмотр событий**.

6. Сохраните внесенные изменения.

Настройка отображения и доставки уведомлений

Чтобы настроить отображение и доставку уведомлений, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Интерфейс**.

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 **OK**.

8. Если вы включили уведомления по почте, настройте параметры доставки электронных сообщений:

   a. Нажмите на кнопку **Настройка почтовых уведомлений**.

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 программы в области уведомлений

Чтобы настроить отображение предупреждений о состоянии программы в области уведомлений, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .

2. В окне параметров программы выберите раздел **Интерфейс**.

3. В блоке **Отображать состояние программы 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 программы в области уведомлений будет меняться на или в зависимости от важности предупреждения.

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 программы в целом сохраняется в отчетах.

Отчеты хранятся в папке `C:\ProgramData\Kaspersky Lab\KES\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 **Системный аудит**. Содержит информацию о событиях, возникающих в процессе взаимодействия пользователя с программой, а также в ходе работы программы 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 Kaspersky Endpoint Security.

Критические события. События критической важности, указывающие на проблемы в работе 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 программы нажмите на кнопку **Больше функций** → **Отчеты**.
2. В левой части окна **Отчеты** 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. По умолчанию события в отчете отсортированы по возрастанию значений в ячейках графы **Дата события**.
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 нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Отчеты и хранилище**.
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 не превышался максимальный размер файла отчета.

Чтобы настроить максимальный размер файла отчета, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Отчеты и хранилище**.
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 программы нажмите на кнопку **Больше функций** → **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. В поле **Имя файла** введите название файла отчета.
7. В поле **Тип файла** 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 нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Отчеты и хранилище**.
3. В блоке **Отчеты** нажмите на кнопку **Очистить**.
4. Если включена Защита паролем, Kaspersky Endpoint Security может запросить учетные данные пользователя. Программа запрашивает учетные данные, если у пользователя нет необходимого расширения.

Kaspersky Endpoint Security удалит все отчеты для всех компонентов и задач программы.

Самозащита Kaspersky Endpoint Security

Kaspersky Endpoint Security обеспечивает защиту компьютера от вредоносных программ, которые пытаются заблокировать работу Kaspersky Endpoint Security или удалить программу с компьютера. Набор доступных технологий самозащиты Kaspersky Endpoint Security зависит от разрядности операционной системы (см. таблицу ниже).

Технологии самозащиты Kaspersky Endpoint Security

Технология	Описание	Компьютер на базе x86	Компьютер на базе x64
Механизм самозащиты	Технология блокирует доступ к следующим компонентам программы: • файлы в папке установки Kaspersky Endpoint Security • раздел реестра с ключами программы • процессы, которые запускает программа.	✓	✓
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 ограничивает управление Kaspersky Endpoint Security с помощью специальных программ удаленного администрирования (например, программы TeamViewer или RemotelyAnywhere).	✓	– (кроме Windows 7)

Включение и выключение механизма самозащиты

По умолчанию механизм самозащиты Kaspersky Endpoint Security включен.

Чтобы включить или выключить механизм самозащиты, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Общие**.
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 программы). 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 программы. Поддержка AM-PPL позволяет делегировать функции защиты процессов операционной системе. Таким образом, вы увеличиваете быстродействие программы и уменьшаете потребление ресурсов компьютера.

Сервис AM-PPL доступен 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 программы.

   Механизм самозащиты предотвращает изменение и удаление процессов программы в памяти компьютера, в том числе изменение статуса AM-PPL.

2. Запустите интерпретатор командной строки cmd от имени администратора.

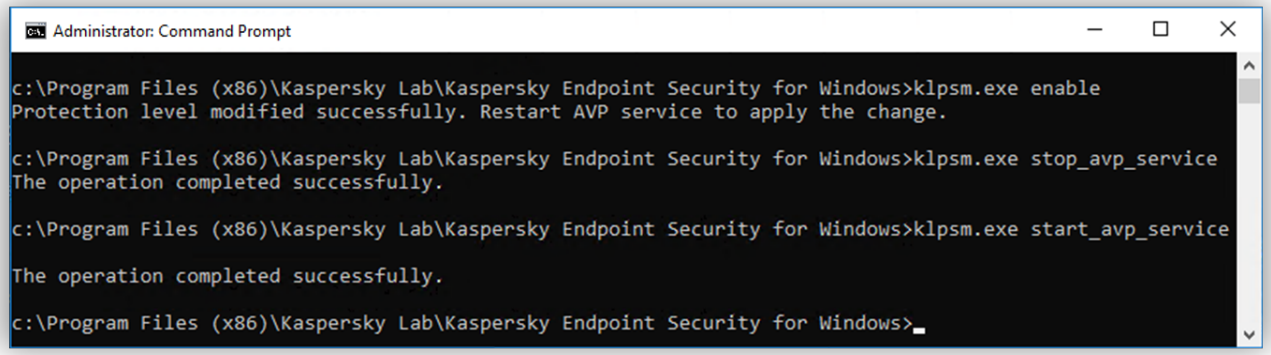
3. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.

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 программы.



Включение поддержки технологии AM-PPL

Включение и выключение защиты от внешнего управления

Защита от внешнего управления позволяет запретить управление Kaspersky Endpoint Security с помощью программ удаленного администрирования (например, программы TeamViewer или RemotelyAnywhere). Технология выполняет следующие функции:

- Защита от изменения настроек Kaspersky Endpoint Security.
- Защита от управления службами Kaspersky Endpoint Security (например, служба `AVP`).
- Защита от остановки процессов программы.

Защита от внешнего управления доступна только для компьютеров под управлением 32-разрядных операционных систем. Для компьютеров под управлением 64-разрядных операционных систем технология недоступна.

Чтобы включить или выключить защиту от внешнего управления, выполните следующие действия:

1. В главном окне программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Расширенные настройки** → **Общие**.
3. Используйте флажок **Разрешить управление настройками Kaspersky Endpoint Security через программы удаленного управления**, чтобы включить или выключить защиту от изменения настроек Kaspersky Endpoint Security. Если вы используете программы удаленного администрирования, вам нужно разрешить управление настройками Kaspersky Endpoint Security и добавить программы в список доверенных. Недоверенным программам удаленного администрирования изменение настроек Kaspersky Endpoint Security запрещено, даже если установлен флажок **Разрешить управление настройками Kaspersky Endpoint Security через программы удаленного управления**. Этот флажок недоступен, если снят флажок **Включить самозащиту**.
4. Используйте флажок **Включить возможность внешнего управления системными службами**, чтобы включить или выключить защиту служб Kaspersky Endpoint Security от внешнего управления.

   Для завершения работы программы из командной строки необходимо, чтобы защита от внешнего управления службами Kaspersky Endpoint Security была выключена.

5. Сохраните внесенные изменения.

В результате, если механизмы защиты от внешнего управления включены, Kaspersky Endpoint Security блокирует наведение курсора на окно программы. При попытке удаленного пользователя остановить работу службы программы отображается системное окно с ошибкой.

Обеспечение работы программ удаленного администрирования

Нередко возникают ситуации, когда при использовании механизма защиты от внешнего управления возникает необходимость применить программы удаленного администрирования.

Чтобы обеспечить работу программ удаленного администрирования, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Угрозы и исключения**.

3. В блоке **Исключения** перейдите по ссылке **Указать доверенные программы**.

4. В открывшемся окне нажмите на кнопку **Добавить**.

5. Выберите исполняемый файл программы удаленного администрирования.

   Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.

6. Установите флажок **Не контролировать активность программы**.

7. Сохраните внесенные изменения.

Производительность Kaspersky Endpoint Security и совместимость с другими программами

Производительность Kaspersky Endpoint Security

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 программа обнаруживает в ходе работы. Kaspersky Endpoint Security всегда проверяет операционную систему на наличие вирусов, червей и троянских программ. Вы не можете выключить проверку этих типов объектов. Такие программы могут нанести значительный вред компьютеру пользователя. Чтобы обеспечить большую безопасность компьютера, вы можете расширить список обнаруживаемых типов объектов, включив контроль действий легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Использование режима энергосбережения

Во время работы на портативных компьютерах потребление программами 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 обновления;
- 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 программа возобновляет выполнение задач шифрования.

Передача ресурсов компьютера другим программам

Потребление ресурсов компьютера Kaspersky Endpoint Security может сказываться на производительности других программ. Чтобы решить проблему совместной работы при увеличении нагрузки на процессор и дисковые подсистемы, Kaspersky Endpoint Security может приостанавливать выполнение задач по расписанию и уступать ресурсы другим программам.

Однако существует ряд программ, которые запускаются в момент высвобождения ресурсов процессора и работают в фоновом режиме. Чтобы проверка не зависела от работы таких программ, не следует уступать им ресурсы операционной системы.

По мере необходимости вы можете запускать эти задачи вручную.

Применение технологии лечения активного заражения

Современные вредоносные программы 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 программ, 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 программ.

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 программы 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 вирусов* в удобное для пользователей сервера время.

Выбор типов обнаруживаемых объектов

Чтобы выбрать типы обнаруживаемых объектов, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Типы обнаруживаемых объектов** установите флажки для типов объектов, которые должен обнаруживать Kaspersky Endpoint Security:
   - **Вирусы, черви**

Подкатегория: вирусы и черви (Viruses_and_Worms)

Степень угрозы: высокая

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-	IM-клиентов	Распространяются через IM-клиенты.

Worm		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 программы

Подкатегория: троянские программы (Trojan_programs)

Степень угрозы: высокая

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-	Троянские	"Берут в заложники" информацию на компьютере

Ransom	программы, требующие выкупа	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,	Троянские программы, крадущие пароли (Password Stealing Ware); крадут учетные записи пользователей,

	крадущие пароли	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 программы

Подкатегория: рекламные программы (Adware)

Степень угрозы: средняя

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.

- Программы 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.
Dialer	Программы автодозвона	Могут устанавливать телефонные соединения через модем в скрытом режиме.
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.

- Другие программы, 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.
Dialer	Программы автодозвона	Могут устанавливать телефонные соединения через модем в скрытом режиме.
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

Kaspersky Endpoint Security проверяет упакованные объекты и модуль-распаковщик в составе самораспаковывающихся архивов SFX (self-extracting archive).

Чтобы скрыть опасные программы от обнаружения антивирусом, злоумышленники упаковывают их с помощью специальных упаковщиков или многократно упаковывают один объект.

Вирусные аналитики "Лаборатории Касперского" отобрали упаковщики, которые злоумышленники используют чаще всего.

Если Kaspersky Endpoint Security обнаружил в объекте такой упаковщик, то скорее всего он содержит вредоносную программу или программу, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.

Kaspersky Endpoint Security выделяет следующие программы:

- *Упакованные файлы, которые могут нанести вред* – используются для упаковки вредоносных программ: вирусов, червей, троянских программ.
- *Многократно упакованные файлы* (степень угрозы средняя) – объект упакован трижды одним или несколькими упаковщиками.

- **Множественно упакованные файлы**

Kaspersky Endpoint Security проверяет упакованные объекты и модуль-распаковщик в составе самораспаковывающихся архивов SFX (self-extracting archive).

Чтобы скрыть опасные программы от обнаружения антивирусом, злоумышленники упаковывают их с помощью специальных упаковщиков или многократно упаковывают один объект.

Вирусные аналитики "Лаборатории Касперского" отобрали упаковщики, которые злоумышленники используют чаще всего.

Если Kaspersky Endpoint Security обнаружил в объекте такой упаковщик, то скорее всего он содержит вредоносную программу или программу, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.

Kaspersky Endpoint Security выделяет следующие программы:

- *Упакованные файлы, которые могут нанести вред* – используются для упаковки вредоносных программ: вирусов, червей, троянских программ.
- *Многократно упакованные файлы* (степень угрозы средняя) – объект упакован трижды одним или несколькими упаковщиками.

4. Сохраните внесенные изменения.

Включение и выключение технологии лечения активного заражения

Если Kaspersky Endpoint Security не может остановить выполнение вредоносной программы, вы можете использовать технологию лечения активного заражения. По умолчанию технология лечения активного заражения выключена, так как технология использует значительные ресурсы компьютера. Таким образом, вы можете включать технологию лечения активного заражения только при работе с активными угрозами.

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 *Антивирусная проверка*. Для работы технологии на рабочих станциях это условие не является обязательным.

Чтобы включить или выключить технологию лечения активного заражения, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Общие**.
3. В блоке **Режим защиты** используйте флажок **Применять технологию лечения активного заражения**, 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.

Включение и выключение режима энергосбережения

Чтобы включить или выключить режим энергосбережения, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Производительность** используйте флажок **Откладывать задачи по расписанию при работе от аккумулятора**, чтобы включить или выключить режим энергосбережения.

   Если включен режим энергосбережения, при работе от аккумулятора не запускаются следующие задачи, даже если для них задан запуск по расписанию:

   - задача обновления;
   - задача полной проверки;
   - задача проверки важных областей;
   - задача выборочной проверки;
   - задача проверки целостности.
4. Сохраните внесенные изменения.

Включение и выключение режима передачи ресурсов другим программам

Чтобы включить или выключить режим передачи ресурсов другим программам, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Общие**.

3. В блоке **Производительность** используйте флажок **Уступать ресурсы другим программам**, чтобы включить или выключить режим передачи ресурсов другим программам.

   При включенном режиме передачи ресурсов другим программам Kaspersky Endpoint Security откладывает выполнение задач, если для них задан запуск по расписанию и их выполнение замедляет работу других программ:

   - задача обновления;
   - задача полной проверки;
   - задача проверки важных областей;
   - задача выборочной проверки;
   - задача проверки целостности.

   По умолчанию режим передачи ресурсов другим программам включен.

4. Сохраните внесенные изменения.

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.

  Для этого требуется сохранить конфигурационный файл в той же папке, где находится дистрибутив.

- Выполнить удаленную установку Kaspersky Endpoint Security через Kaspersky Security Center с заранее заданными параметрами.

- Перенести параметры работы Kaspersky Endpoint Security с одного компьютера на другой.

Чтобы создать конфигурационный файл, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Управление настройками**.
3. Нажмите на кнопку **Экспортировать**.
4. 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.

5. Нажмите на кнопку **Сохранить**.

Чтобы импортировать параметры работы Kaspersky Endpoint Security из конфигурационного файла, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Управление настройками**.
3. Нажмите на кнопку **Импортировать**.
4. В открывшемся окне укажите путь к конфигурационному файлу.
5. Нажмите на кнопку **Открыть**.

Все значения параметров Kaspersky Endpoint Security будут установлены в соответствии с выбранным конфигурационным файлом.

Восстановление параметров программы по умолчанию

Вы в любое время можете восстановить настройки Kaspersky Endpoint Security, рекомендуемые "Лабораторией Касперского". В результате восстановления настроек для всех компонентов защиты будет установлен уровень безопасности **Рекомендуемый**.

Чтобы восстановить параметры программы по умолчанию, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Управление настройками**.
3. Нажмите на кнопку **Восстановление**.
4. Нажмите на кнопку **Сохранить**.

Обмен сообщениями между пользователем и администратором

Компоненты Контроль программ, Контроль устройств, Веб-Контроль и Адаптивный контроль аномалий предоставляют пользователям локальной сети организации, на компьютерах которых установлена программа 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 программ запретил запуск программы.

  Шаблон сообщения с запросом разрешения на запуск заблокированной программы доступен в интерфейсе Kaspersky Endpoint Security в разделе Контроль программ.

- 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 установленной программой Kaspersky Endpoint Security действующей политики Kaspersky Security Center и связи с Сервером администрирования Kaspersky Security Center. Возможны следующие сценарии:

- Если на компьютере с установленной программой 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 установленной программой 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 установленной программой 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 закладку **События**.

   В рабочей области Kaspersky Security Center отображаются все события, произошедшие во время работы программы Kaspersky Endpoint Security, в том числе и сообщения администратору, приходящие от пользователей локальной сети организации.

3. Чтобы настроить фильтр событий, в раскрывающемся списке **События выборки** выберите элемент **Запросы пользователей**.

4. Выберите сообщение администратору.

5. Нажмите на кнопку **Открыть окно свойств события** в правой части рабочей области Консоли администрирования.

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 программ к данным. Kaspersky Endpoint Security использует алгоритм шифрования Advanced Encryption Standard (AES).

Если срок действия лицензии истек, то программа не шифрует новые данные, а старые зашифрованные данные остаются зашифрованными и доступными для работы. В этом случае для шифрования новых данных требуется активировать программу по новой лицензии, которая допускает использование шифрования.

В случае истечения срока действия лицензии, нарушения Лицензионного соглашения, удаления лицензионного ключа, удаления программы Kaspersky Endpoint Security или компонентов шифрования с компьютера пользователя не гарантируется, что файлы, зашифрованные ранее, останутся зашифрованными. Это связано с тем, что некоторые программы, 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 программами. После применения политики программа 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 программами.
- **Шифрование съемных дисков**. Вы можете указать правило шифрования по умолчанию, в соответствии с которым программа 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 программа выполняет одно из следующих действий:
  - Если известна только модель устройства, программа применяет правило шифрования, созданное для съемных дисков с данной моделью устройства, если такое правило есть.
  - Если известен только идентификатор устройства, программа применяет правило шифрования, созданное для съемных дисков с данным идентификатором устройства, если такое правило есть.
  - Если известны и модель устройства, и идентификатор устройства, программа 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, программа применяет его. Если не заданы правила шифрования ни для

данного идентификатора устройства, ни для данной модели устройства, программа применяет правило шифрования по умолчанию.

- Если неизвестны ни модель устройства, ни идентификатор устройства, программа применяет правило шифрования по умолчанию.

Программа 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 любой программы 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. Программа 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 *Управления 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 установлена программа 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 **Шифровать только занятое пространство**. 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 зашифрованными файлам, Работа с зашифрованными устройствами при отсутствии доступа к ним).

Ограничения функциональности шифрования

Шифрование данных имеет следующие ограничения:

- В процессе шифрования программа 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 12 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 программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для серверов, то доступно только полнодисковое шифрование с помощью технологии Шифрование диска BitLocker. Если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций, то функциональность шифрования данных доступна в полном объеме.

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 программа 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 Express Cache.
- 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 Think Center 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 программой.

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 программа Kaspersky Endpoint Security зашифровала 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 программы. Смена длины ключа через обновление программы доступна при выполнении следующих условий:

- На компьютере установлена программа 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 программу дистанционно с помощью инсталляционного пакета.

Невозможно сменить длину ключа шифрования с помощью дистрибутива той же версии программы, которая установлена на вашем компьютере, без предварительного удаления программы.

Шифрование диска Kaspersky

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 программа 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 программа в автоматическом режиме выполняет все необходимые проверки. Если проверка на совместимость проходит успешно, то после загрузки операционной системы и запуска программы 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 программой 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

Программа поддерживает шифрование SSD-дисков, гибридных SSHD-дисков и дисков с функцией Intel Smart Response. Программа 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

Полнодисковое шифрование с помощью технологии Шифрование 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.

Чтобы выполнить полнодисковое шифрование с помощью технологии Шифрование диска Kaspersky, выполните следующие действия:

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 закладку **Политики**.

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

5. В окне политики выберите **Шифрование данных → Полнодисковое шифрование**.

6. 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.

7. В раскрывающемся списке **Режим шифрования** выберите действие **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 установлена программа.

   Если некоторые жесткие диски нужно исключить из шифрования, сформируйте их список.

8. Настройте правила добавления учетных записей Агента аутентификации при шифровании диска. Агент позволяет пользователю пройти аутентификацию для доступа к зашифрованным дискам и для загрузки операционной системы. Для автоматического добавления учетных записей Агента аутентификации настройте следующие параметры:

   - **Автоматически создавать учетные записи Агента аутентификации для пользователей при применении шифрования на компьютере**. Если флажок установлен, программа 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, программа 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, программа 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 дискам.

   Если вы выключили автоматическое создание учетных записей Агента аутентификации, вы можете вручную добавить учетные записи Агента аутентификации с помощью задачи *Управление учетными записями*. Также с помощью задачи вы можете изменить параметры учетных записей Агента аутентификации, которые были созданы автоматически.

9. Для удобства пользования вы можете сохранить имя пользователя в память Агента аутентификации, чтобы пользователь при следующем входе в систему вводил только пароль. Для этого установите флажок **Сохранить введенное в Агенте аутентификации имя пользователя**.

10. Выберите один из следующих способов шифрования:

- Если вы хотите применить шифрование только к тем секторам жесткого диска, которые заняты файлами, установите флажок **Шифровать только занятое пространство**.

  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 вы хотите применить шифрование ко всему жесткому диску, снимите флажок **Шифровать только занятое пространство**.

  Если устройство было зашифровано ранее с использованием функции **Шифровать только занятое пространство**, после применения политики в режиме **Шифровать все жесткие диски** секторы, не занятые файлами, по-прежнему не будут зашифрованы.

11. Если в ходе шифрования компьютера возникла проблема несовместимости с аппаратным обеспечением, вы можете установить флажок **Использовать 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.

    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.

12. 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 программы.

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.

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. 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 закладку **Политики**.

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

5. В окне политики выберите **Шифрование данных → Полнодисковое шифрование**.

6. В раскрывающемся списке **Технология шифрования** выберите вариант **Шифрование диска Kaspersky**.

   В таблице **Не шифровать следующие жесткие диски** отобразятся записи о жестких дисках, которые программа не будет шифровать. Если вы ранее не сформировали список жестких дисков для исключения из шифрования, эта таблица пуста.

7. Если вы хотите добавить жесткие диски в список жестких дисков, которые программа не будет шифровать, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Добавление устройств из списка Kaspersky Security Center**.

   b. В окне **Добавление устройств из списка Kaspersky Security Center** 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 **ОК**.

   Выбранные жесткие диски отобразятся в таблице **Не шифровать следующие жесткие диски**.

8. Если вы хотите удалить жесткие диски из таблицы исключений, выберите одну или несколько строк в таблице **Не шифровать следующие жесткие диски** и нажмите на кнопку **Удалить**.

   Чтобы выбрать несколько строк в таблице, выделяйте их, удерживая клавишу **CTRL**.

9. 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Полнодисковое шифрование**.
6. В раскрывающемся списке **Технология шифрования** выберите вариант **Шифрование диска Kaspersky**.

   В таблице **Не шифровать следующие жесткие диски** отобразятся записи о жестких дисках, которые программа не будет шифровать.
7. 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 ссылку **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. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список исключений в XML-файл.
8. 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. Нажмите на кнопку **Открыть**.

      Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
9. Сохраните внесенные изменения.

[Как экспортировать / импортировать список исключений жестких дисков из шифрования в Web Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите экспортировать или импортировать список исключений.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Шифрование данных** → **Полнодисковое шифрование**.
5. Выберите технологию **Шифрование диска Kaspersky** и перейдите по ссылке для настройки параметров.

   Откроются параметры шифрования.
6. Перейдите по ссылке **Исключения**.
7. Для экспорта списка исключений выполните следующие действия:
   a. Выберите исключения, которые вы хотите экспортировать.
   b. Нажмите на кнопку **Экспорт**.
   c. Подтвердите, что вы хотите экспортировать только выбранные исключения, или экспортируйте весь список.
   d. 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.
   e. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список исключений в XML-файл.
8. 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. Нажмите на кнопку **Открыть**.

      Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.
9. 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.

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.

Технология единого входа несовместима со сторонними поставщиками учетных данных.

Как включить использование технологии единого входа 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Общие настройки шифрования**.
6. В блоке **Настройки паролей** нажмите на кнопку **Настройка**.
7. В открывшемся окне на закладке **Агент аутентификации** установите флажок **Использовать технологию единого входа (SSO)**.
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.

Как включить использование технологии единого входа в Web Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите включить использование технологии единого входа.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Шифрование данных** → **Полнодисковое шифрование**.
5. Выберите технологию **Шифрование диска Kaspersky** и перейдите по ссылке для настройки параметров.

   Откроются параметры шифрования.
6. В блоке **Настройки паролей** установите флажок **Использовать технологию единого входа (SSO)**.
7. Нажмите на кнопку **OK**.

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. После этого Kaspersky Endpoint Security заменит пароль учетной записи Агента аутентификации на пароль учетной записи 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 Консоли администрирования перейдите в папку **Сервер администрирования → 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 (11.6.0) → 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 **Устройства** → **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 **Программа** выберите **Kaspersky Endpoint Security для Windows (11.6.0)**.
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 **Выбор устройств, 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 по кнопке **Готово**. 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 **Параметры**.

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. SID – Security Identifier).

   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 **Шифрование всего носителя, управление учетными записями**.

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 программа требовала 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 программа требовала 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. Выполните одно из следующих действий:

    - Выберите вариант **Разрешать аутентификацию**, если вы хотите, чтобы программа разрешала доступ к аутентификации в Агенте аутентификации пользователю, работающему под учетной записью, указанной в команде.

- Выберите вариант **Запрещать аутентификацию**, если вы хотите, чтобы программа запрещала 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 **Устройства → Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Управление учетными записями Агента аутентификации**.

   Откроется окно свойств задачи.

3. Выберите закладку **Параметры программы**.

4. В списке учетных записей Агента аутентификации нажмите на кнопку **Добавить**.

   Запустится мастер управления учетными записями Агента аутентификации.

5. Выберите тип команды **Добавление учетной записи**.

6. Выберите учетную запись пользователя. Вы можете выбрать учетную запись из списка доменных учетных записей или ввести имя учетной записи вручную. Нажмите на кнопку **Далее**.

   Kaspersky Endpoint Security определяет идентификатор безопасности учетной записи (англ. SID – Security Identifier). Это нужно для проверки учетной записи. Если вы ввели имя пользователя неверно, Kaspersky Endpoint Security завершит выполнение задачи с ошибкой.

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.

   - **Разрешить 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.

   - **Разрешить 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**.

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 **Параметры**.
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. SID – Security Identifier).

   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**, программа Kaspersky Endpoint Security изменила имя пользователя на указанное в поле ниже.
7. Установите флажок **Изменить параметры 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 программа требовала 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**, программа Kaspersky Endpoint Security изменила значение параметра смены пароля на установленное ниже.
10. Установите значение параметра смены пароля при аутентификации в Агенте аутентификации.
11. Установите флажок **Изменить параметры 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 программа требовала 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**, программа Kaspersky Endpoint Security изменила 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 **Устройства → Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Управление учетными записями Агента аутентификации**.

   Откроется окно свойств задачи.

3. Выберите закладку **Параметры программы**.

4. В списке учетных записей Агента аутентификации нажмите на кнопку **Добавить**.

   Запустится мастер управления учетными записями Агента аутентификации.

5. Выберите тип команды **Изменение учетной записи**.

6. Выберите учетную запись пользователя. Вы можете выбрать учетную запись из списка доменных учетных записей или ввести имя учетной записи вручную. Нажмите на кнопку **Далее**.

   Kaspersky Endpoint Security определяет идентификатор безопасности учетной записи (англ. SID – Security Identifier). Это нужно для проверки учетной записи. Если вы ввели имя пользователя неверно, Kaspersky Endpoint Security завершит выполнение задачи с ошибкой.

7. Установите флажки напротив тех параметров, которые вы хотите изменить.

8. 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.

   - **Разрешить 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.

   - **Разрешить 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.

9. Сохраните внесенные изменения.

10. 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 **Параметры**.
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. SID – Security Identifier).

   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 **Устройства → Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Управление учетными записями Агента аутентификации**.

   Откроется окно свойств задачи.

3. Выберите закладку **Параметры программы**.

4. В списке учетных записей Агента аутентификации нажмите на кнопку **Добавить**.

   Запустится мастер управления учетными записями Агента аутентификации.

5. Выберите тип команды **Удаление учетной записи**.

6. Выберите учетную запись пользователя. Вы можете выбрать учетную запись из списка доменных учетных записей или ввести имя учетной записи вручную.

7. Сохраните внесенные изменения.

8. 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 папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

3. В рабочей области выберите закладку **Устройства**.

4. Откройте свойства компьютера двойным щелчком мыши.

5. В окне свойств компьютера выберите раздел **Задачи**.

   Откроется список локальных задач.

6. Выберите задачу **Управление учетными записями Агента аутентификации**.

7. В свойствах задачи выберите раздел **Параметры**.

   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.

[Как просмотреть список учетных записей Агента аутентификации через Web Console]

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите просмотреть список учетных записей Агента аутентификации.

   Откроются свойства компьютера.
3. В окне свойств компьютера выберите раздел **Задачи**.

   Откроется список локальных задач.
4. Выберите задачу **Управление учетными записями Агента аутентификации**.
5. В свойствах задачи выберите закладку **Параметры программы**.

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;
- Aladdin-RD JaCarta PKI;
- 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных → Полнодисковое шифрование**.

6. В раскрывающемся списке **Технология шифрования** выберите ту технологию, с помощью которой были зашифрованы жесткие диски.

7. 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.

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 программы.

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").

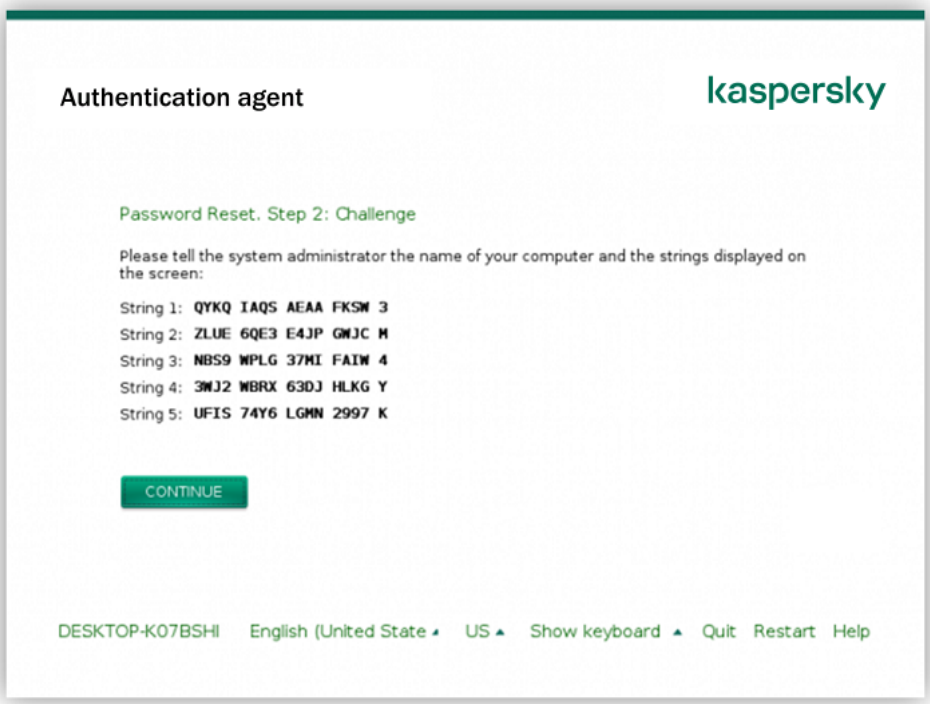
Восстановление доступа к системному жесткому диску

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 папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. На закладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите закладку **Агент аутентификации**.
7. 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 программой.
8. В раскрывающемся списке **Учетная запись** выберите имя учетной записи Агента аутентификации пользователя, запросившего восстановление доступа к диску.
9. В раскрывающемся списке **Жесткий диск** выберите зашифрованный жесткий диск, доступ к которому необходимо восстановить.
10. 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.

[Как получить блоки ответа для системного жесткого диска, защищенного технологией Шифрование диска Kaspersky, в Web Console]

1. В главном окне Web Console выберите **Устройства** → **Управляемые 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 папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. На закладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите закладку **Шифрование данных**.
7. На закладке **Шифрование данных** нажмите на кнопку **Обзор**.
8. 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.

Как получить файл ключа доступа к зашифрованному несистемному жесткому диску в Web Console

1. В главном окне Web Console выберите **Устройства** → **Управляемые 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.

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.

Подробнее о безопасном обновлении операционной системы вы можете узнать в базе знаний Службы технической поддержки.

Автоматическое обновление операционной системы доступно при выполнении следующих условий:

1. Обновление ОС через WSUS (Windows Server Update Services).
2. На компьютере установлена операционная система Windows 10 версия 1607 (RS1) и выше.
3. На компьютере установлена программа Kaspersky Endpoint Security версии 11.2.0 и выше.

При выполнении всех условий вы можете обновлять операционную систему обычным способом.

Если вы используете технологию Шифрование диска Kaspersky (FDE) и на компьютере установлена программа Kaspersky Endpoint Security для Windows версий 11.1.0 и 11.1.1, для обновления Windows 10 не нужно расшифровывать жесткие диски.

Для обновления операционной системы вам нужно выполнить следующие действия:

1. Перед обновлением системы скопируйте драйверы cm_km.inf, cm_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf, klfdefsf.sys в локальную папку. Например, C:\fde_drivers.

2. Запустите установку обновления системы с ключом `/ReflectDrivers`, указав папку с сохраненными драйверами:

   ```
   setup.exe /ReflectDrivers C:\fde_drivers
   ```

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 программы до Kaspersky Endpoint Security для Windows 11.6.0 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 программы 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.

Выбор уровня трассировки Агента аутентификации

Программа записывает служебную информацию о работе Агента аутентификации, а также информацию о действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.

Чтобы выбрать уровень трассировки Агента аутентификации, выполните следующие действия:

1. Сразу после запуска компьютера с зашифрованными жесткими дисками по кнопке **F3** вызовите окно для настройки параметров Агента аутентификации.

2. В окне настройки параметров Агента аутентификации выберите уровень трассировки:

   - **Disable debug logging (default)**. Если выбран этот вариант, то программа не записывает информацию о событиях работы Агента аутентификации в файл трассировки.

   - **Enable debug logging**. Если выбран этот вариант, то программа записывает информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.

   - **Enable verbose logging**. Если выбран этот вариант, то программа 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 **Enable debug logging**. Высокий уровень детализации записей может замедлять загрузку Агента аутентификации и операционной системы.

   - **Enable debug logging and select serial port**. Если выбран этот вариант, то программа 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.

   - **Enable verbose debug logging and select serial port**. Если выбран этот вариант, то программа 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 **Enable debug logging and select serial port**. Высокий уровень детализации записей может замедлять загрузку Агента аутентификации и операционной системы.

Запись в файл трассировки Агента аутентификации выполняется в случае, если на компьютере есть зашифрованные жесткие диски или выполняется полнодисковое шифрование.

Файл трассировки Агента аутентификации не передается в "Лабораторию Касперского", как другие файлы трассировки программы. 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. 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 закладку **Политики**.

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

5. В окне политики выберите **Шифрование данных** → **Общие настройки шифрования**.

6. Нажмите на кнопку **Справка** в блоке **Шаблоны**.

   Откроется окно **Справочные тексты Агента аутентификации**.

7. Выполните следующие действия:

   - Выберите закладку **Аутентификация**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе ввода учетных данных.

   - Выберите закладку **Смена пароля**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе смены пароля для учетной записи Агента аутентификации.

   - Выберите закладку **Восстановление пароля**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе восстановления пароля для учетной записи Агента аутентификации.

8. 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.

9. 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 программы Kaspersky Endpoint Security обнаруживает объекты и данные, оставшиеся на системном жестком диске после тестовой работы Агента аутентификации, то удаление программы 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 программа 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 данные о несовместимости программы 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.

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 диска BitLocker создает мастер-ключ. Kaspersky Endpoint Security отправляет мастер-ключ 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 информацию о шифровании диска в Kaspersky Security Center. При этом Kaspersky Endpoint Security не отправит мастер-ключ в Kaspersky Security Center, и восстановить доступ к диску с помощью Kaspersky Security Center будет невозможно. Для корректной работы BitLocker с Kaspersky Security Center расшифруйте диск и зашифруйте диск повторно с помощью политики. Расшифровать диск вы можете локально или с помощью политики.

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).

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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Полнодисковое шифрование**.
6. В раскрывающемся списке **Технология шифрования** выберите элемент **Шифрование диска BitLocker**.
7. 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.

8. Настройте дополнительные параметры шифрования диска BitLocker (см. таблицу ниже).
9. Сохраните внесенные изменения.

Как запустить шифрование диска BitLocker через Web Console и Cloud Console

1. В главном окне Web Console выберите **Устройства → Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите запустить шифрование диска BitLocker.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Шифрование данных → Полнодисковое шифрование**.
5. В блоке **Управление шифрованием** выберите элемент **Шифрование диска BitLocker**.
6. Перейдите на ссылке **Шифрование диска BitLocker**.

   Откроется окно с параметрами шифрования диска BitLocker.
7. 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.
8. Настройте дополнительные параметры шифрования диска BitLocker (см. таблицу ниже).
9. Нажмите на кнопку **OK**.

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 программы.

После применения политики в зависимости от настроек аутентификации программа 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).

Параметры компонента Шифрование диска BitLocker

Параметр	Описание
Включить использование проверки подлинности BitLocker, требующей предзагрузочного ввода с клавиатуры на планшетах	Флажок включает / выключает 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 программа 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.
Настройки аутентификации	**Использовать 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).

Использовать 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.
  Вы можете разрешить пользователю использовать расширенный PIN-код. *Расширенный PIN-код* кроме цифр позволяет использовать другие символы: заглавные и строчные латинские буквы, специальные символы и пробел.

- **Использовать доверенный платформенный модуль (TPM), если он недоступен, то пароль**. Если флажок установлен, 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.

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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных → Полнодисковое шифрование**.
6. В раскрывающемся списке **Технология шифрования** выберите элемент **Шифрование диска BitLocker**.
7. В раскрывающемся списке **Режим шифрования** выберите элемент **Расшифровывать все жесткие диски**.
8. Сохраните внесенные изменения.

Как расшифровать жесткий диск, защищенный BitLocker, через Web Console и Cloud Console

1. В главном окне Web Console выберите закладку **Устройства → Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите расшифровать жесткие диски.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Шифрование данных → Полнодисковое шифрование**.
5. Выберите технологию **Шифрование диска BitLocker** и перейдите по ссылке для настройки параметров.

   Откроются параметры шифрования.
6. В раскрывающемся списке **Режим шифрования** выберите элемент **Расшифровывать все жесткие диски**.
7. Нажмите на кнопку **OK**.

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 программы.

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 в 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.

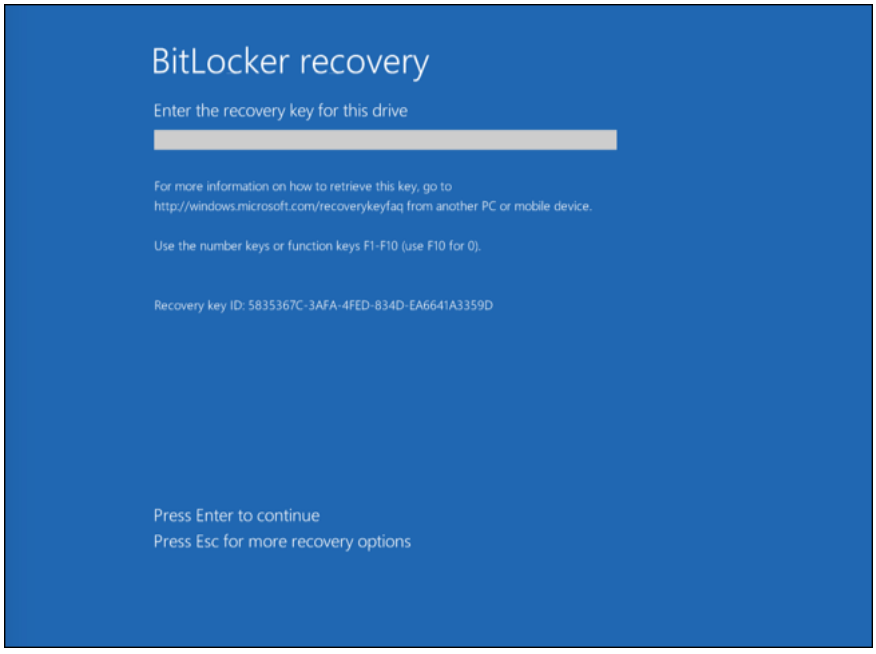
Восстановление доступа к жесткому диску, зашифрованному BitLocker, состоит из следующих этапов:

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.
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 папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. На закладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите закладку **Доступ к системному диску с защитой BitLocker**.
7. 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.

[Как просмотреть ключ восстановления для системного диска, зашифрованного BitLocker, в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Управляемые 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 мастер-ключ 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 устройства**.
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 (11.6.0)**.
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**.

[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 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**.

   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.

Шифрование файлов на локальных дисках компьютера

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена 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 программ. 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 блокирует копирование зашифрованных файлов в облачное хранилище OneDrive, если эти файлы не добавлены в правило расшифровки.

Чтобы зашифровать файлы на локальных дисках компьютера, выполните следующие действия:

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 закладку **Политики**.

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

5. В окне политики выберите **Шифрование данных → Шифрование файлов**.

6. В правой части окна выберите закладку **Шифрование**.

7. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.

8. На закладке **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 программ. Например, программы 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).

   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. Вы можете использовать набор `\..\` (например, `C:\Users\..\UserFolder\`). Набор `\..\` обозначает переход к родительской папке.
      - 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.

9. 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 программ к зашифрованным файлам

Чтобы сформировать правила доступа программ к зашифрованным файлам, выполните следующие действия:

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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных → Шифрование файлов**.
6. 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 программы будут иметь доступ ко всем зашифрованным файлам.

7. В правой части окна выберите закладку **Правила для программ**.
8. Если вы хотите выбрать программы исключительно из списка Kaspersky Security Center, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы из списка Kaspersky**

Security Center.

a. Задайте фильтры для вывода списка программ в таблице. Для этого укажите значения параметров **Программа**, **Производитель**, **Период добавления**, а также флажков из блока **Группа**.

b. Нажмите на кнопку **Обновить**.

c. В таблице отобразится список программ, удовлетворяющих заданным фильтрам.

d. В графе **Программы** установите флажки напротив тех программ в таблице, для которых вы хотите сформировать правила доступа к зашифрованным файлам.

e. В раскрывающемся списке **Правило для программ** выберите правило, которое будет определять доступ программ к зашифрованным файлам.

f. В раскрывающемся списке **Действие для программ, выбранных ранее** выберите действие, которое выполняет Kaspersky Endpoint Security над правилами доступа к зашифрованным файлам, сформированными для указанных выше программ ранее.

g. Нажмите на кнопку **OK**.

Информация о правиле доступа программ к зашифрованным файлам отобразится в таблице на закладке **Правила для программ**.

9. Если вы хотите выбрать программы вручную, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы вручную**.

a. В поле ввода введите имя или список имен исполняемых файлов программ с их расширениями.

Вы можете также добавить имена исполняемых файлов программ из списка Kaspersky Security Center, нажав на кнопку **Добавить из списка Kaspersky Security Center**.

b. Если требуется, в поле **Описание** введите описание списка программ.

c. В раскрывающемся списке **Правило для программ** выберите правило, которое будет определять доступ программ к зашифрованным файлам.

d. Нажмите на кнопку **OK**.

Информация о правиле доступа программ к зашифрованным файлам отобразится в таблице на закладке **Правила для программ**.

10. Сохраните внесенные изменения.

Шифрование файлов, создаваемых и изменяемых отдельными программами

Вы можете создать правило, согласно которому Kaspersky Endpoint Security будет шифровать все файлы, создаваемые и изменяемые указанными в правиле программами.

Файлы, созданные или измененные указанными программами до применения правила шифрования, не будут зашифрованы.

Чтобы настроить шифрование файлов, создаваемых и изменяемых отдельными программами, выполните следующие действия:

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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных → Шифрование файлов**.
6. 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.

7. В правой части окна выберите закладку **Правила для программ**.
8. Если вы хотите выбрать программы исключительно из списка Kaspersky Security Center, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы из списка Kaspersky Security Center**.

   Откроется окно **Добавление программ из списка Kaspersky Security Center**.

   Выполните следующие действия:

   a. Задайте фильтры для вывода списка программ в таблице. Для этого укажите значения параметров **Программа**, **Производитель**, **Период добавления**, а также флажков из блока **Группа**.

   b. Нажмите на кнопку **Обновить**.

      В таблице отобразится список программ, удовлетворяющих заданным фильтрам.

   c. В графе **Программы** установите флажки напротив тех программ в таблице, создаваемые файлы которых вы хотите шифровать.

   d. В раскрывающемся списке **Правило для программ** выберите элемент **Шифровать все создаваемые файлы**.

   e. В раскрывающемся списке **Действие для программ, выбранных ранее** выберите действие, которое выполняет Kaspersky Endpoint Security над правилами шифрования файлов, сформированными для указанных выше программ ранее.

   f. Нажмите на кнопку **ОК**.

   Информация о правиле шифрования файлов, создаваемых и изменяемых выбранными программами, отобразится в таблице на закладке **Правила для программ**.

9. Если вы хотите выбрать программы вручную, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы вручную**.

   Откроется окно **Добавление / изменение названий исполняемых файлов программ**.

   Выполните следующие действия:

a. В поле ввода введите имя или список имен исполняемых файлов программ с их расширениями.

   Вы можете также добавить имена исполняемых файлов программ из списка Kaspersky Security Center, нажав на кнопку **Добавить из списка Kaspersky Security Center**.

b. Если требуется, в поле **Описание** введите описание списка программ.

c. В раскрывающемся списке **Правило для программ** выберите элемент **Шифровать все создаваемые файлы**.

d. Нажмите на кнопку **ОК**.

Информация о правиле шифрования файлов, создаваемых и изменяемых выбранными программами, отобразится в таблице на закладке **Правила для программ**.

10. Сохраните внесенные изменения.

Формирование правила расшифровки

Чтобы сформировать правило расшифровки, выполните следующие действия:

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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных → Шифрование файлов**.
6. В правой части окна выберите закладку **Расшифровка**.
7. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.
8. На закладке **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.

9. 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных → Шифрование файлов**.
6. В правой части окна выберите закладку **Шифрование**.
7. 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**.

   Вы можете удалять сразу несколько элементов из списка для шифрования. Для этого, удерживая клавишу **CTRL**, левой клавишей мыши выберите нужные элементы 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.
8. Сформируйте список файлов для расшифровки.
9. 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных → Общие настройки шифрования**.
6. В блоке **Настройки паролей** нажмите на кнопку **Настройка**.
7. В открывшемся окне выберите закладку **Зашифрованные архивы**.
8. 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 **Устройства → Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите включить проверку сложности паролей.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Шифрование данных → Шифрование файлов**.
5. В блоке **Настройки пароля для зашифрованных архивов** настройте параметры сложности пароля при создании зашифрованных архивов.

Вы можете создавать зашифрованные архивы на компьютерах с установленной программой 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).

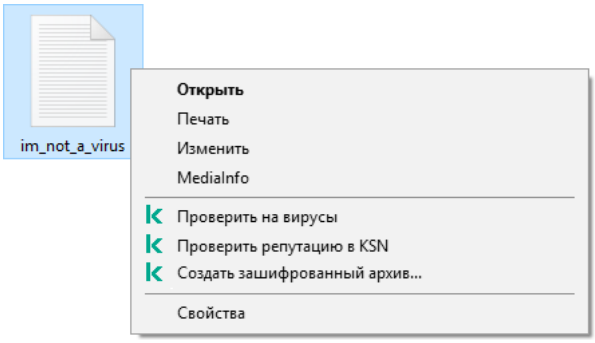
3. В открывшемся окне выберите место для сохранения зашифрованного архива на съемном диске, задайте имя и нажмите на кнопку **Сохранить**.

4. В открывшемся окне задайте пароль и повторите его.

   Пароль должен соответствовать критериям сложности, заданным в политике.

5. 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) – .



Создание зашифрованного архива

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 зашифрованными 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.

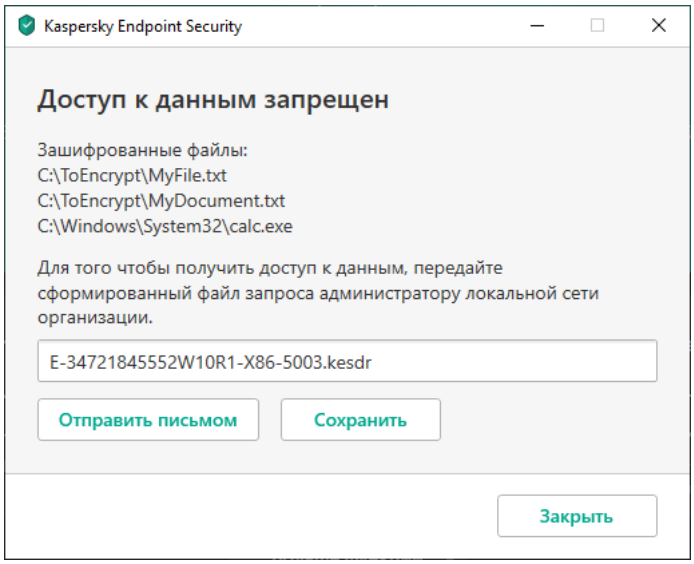
  Пользователь может работать с зашифрованными файлами при следующих условиях:

  - Файлы помещены в зашифрованные архивы, созданные на компьютере с установленной программой 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 папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. На закладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите закладку **Шифрование данных**.
7. На закладке **Шифрование данных** нажмите на кнопку **Обзор**.
8. 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.

Как получить файл ключа доступа к зашифрованным данным в Web Console

1. В главном окне Web Console выберите **Устройства** → **Управляемые 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных → Общие настройки шифрования**.
6. В блоке **Шаблоны** нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны**.
7. Выполните следующие действия:

   - Если вы хотите изменить шаблон сообщения пользователя, выберите закладку **Сообщение пользователя**. Когда пользователь обращается к зашифрованному файлу при отсутствии на компьютере ключа доступа к зашифрованным файлам, открывается окно **Доступ к данным запрещен**. При нажатии на кнопку **Отправить по электронной почте** окна **Доступ к данным запрещен** 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 закладку **Сообщение администратора**. Это сообщение автоматически формируется при нажатии на кнопку **Отправить по электронной почте** окна **Запрос доступа к зашифрованным файлам** и приходит к пользователю после предоставления ему доступа к зашифрованным файлам.
8. Измените шаблоны сообщений.

   Вы можете использовать кнопку **По умолчанию** и раскрывающийся список **Переменная**.

9. Сохраните внесенные изменения.

Шифрование съемных дисков

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена 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 файловых систем FAT32 и NTFS. Если к компьютеру подключен съемный диск с неподдерживаемой файловой системой, шифрование съемного диска завершится с ошибкой и Kaspersky Endpoint Security установит для этого съемного диска право доступа "только чтение".

Чтобы зашифровать съемные диски, выполните следующие действия:

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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных → Шифрование съемных дисков**.
6. 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. Программа 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.
7. 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 установлена программа Kaspersky Endpoint Security.
8. 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.
9. Если вы хотите настроить шифрование для отдельных съемных дисков, задайте правила шифрования.
10. 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.

11. Сохраните внесенные изменения.

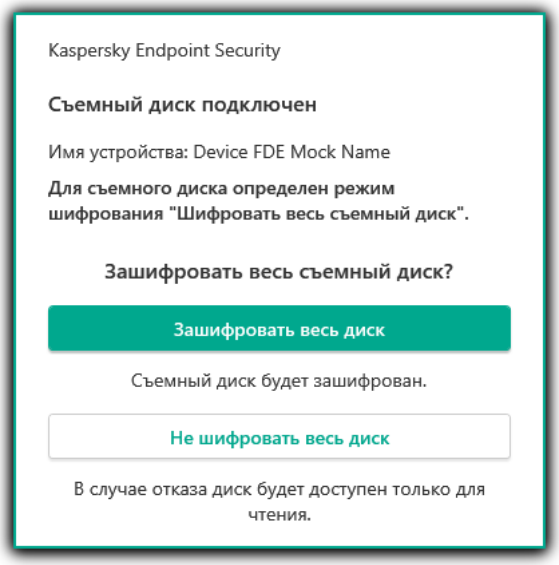
В результате применения политики, если пользователь подключает съемный диск или съемный диск уже подключен, Kaspersky Endpoint Security запрашивает подтверждение для выполнения операции шифрования (см. рис. ниже).

Программа 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". Программа 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 другой программой. 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. 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 закладку **Политики**.

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

5. В окне политики выберите **Шифрование данных → Шифрование съемных дисков**.

6. 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**.

7. В раскрывающемся списке **Режим шифрования для выбранных устройств** выберите действие, которое выполняет Kaspersky Endpoint Security с файлами, хранящимися на выбранных съемных дисках.

8. 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.

9. 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.

10. 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**.

11. 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных → Шифрование съемных дисков**.
6. 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 **Экспорт**.
   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. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список правил в XML-файл.
7. Для импорта списка правил шифрования для съемных дисков, выполните следующие действия:
   a. Нажмите на ссылку **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

   b. Нажмите на кнопку **Открыть**.

      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 правил шифрования для съемных дисков в Web Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите экспортировать или импортировать список правил шифрования для съемных дисков.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Шифрование данных** → **Шифрование съемных дисков**.
5. В блоке **Правила шифрования выбранных устройств** перейдите по ссылку **Правила шифрования**.

   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 **Экспорт**.
   c. Подтвердите, что вы хотите экспортировать только выбранные правила, или экспортируйте весь список.
   d. Нажмите на кнопку **Экспорт**.

      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 **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.
   b. Нажмите на кнопку **Открыть**.

      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.

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 установлена программа Kaspersky Endpoint Security.

Портативный режим удобно использовать в следующих случаях:

- Нет связи между компьютером и Сервером администрирования Kaspersky Security Center.

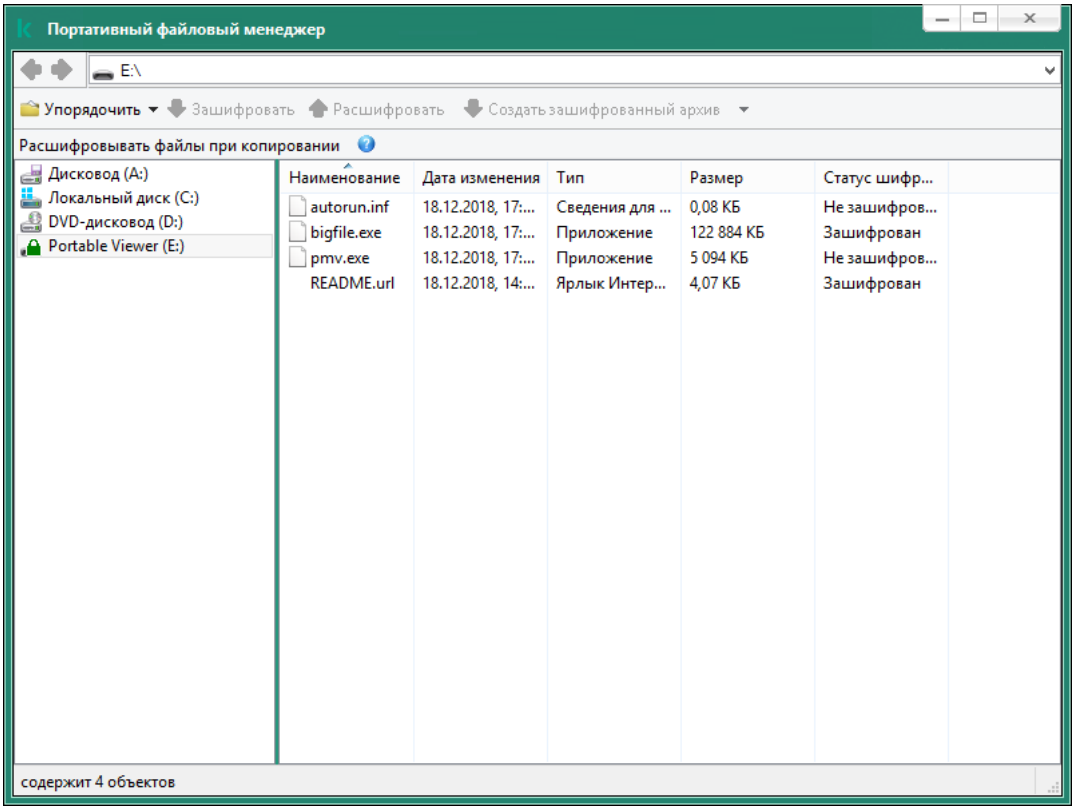
- Изменилась инфраструктура со сменой Сервера администрирования Kaspersky Security Center.
- На компьютере не установлена программа Kaspersky Endpoint Security.

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 установлена программа Kaspersky Endpoint Security (см. рис. ниже). Если на компьютере установлена программа 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 установлена программа Kaspersky Endpoint Security. Если на компьютере выключен автозапуск программ, 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных** → **Шифрование съемных дисков**.
6. 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.

7. Установите флажок **Портативный режим**.
8. Если нужно, добавьте правила шифрования для отдельных съемных дисков.
9. Сохраните внесенные изменения.
10. После применения политики подключите съемный диск к компьютеру.
11. Подтвердите операцию шифрования съемного диска.

    Откроется окно создания пароля для портативного файлового менеджера.

12. Задайте пароль, соответствующий требованиям к уровню сложности, и подтвердите его.
13. Нажмите на кнопку **OK**.

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.

Как включить поддержку портативного режима для работы с зашифрованными файлами на съемных дисках в Web Console

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите включить поддержку портативного режима.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Шифрование данных** → **Шифрование съемных дисков**.
5. В блоке **Управление шифрованием** 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.
11. Задайте пароль, соответствующий требованиям к уровню сложности, и подтвердите его.
12. Нажмите на кнопку **OK**.

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 установлена программа 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 установлена программа Kaspersky Endpoint Security, программа 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.

- Если компьютер находится внутри корпоративной сети и на компьютере установлена программа 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.

Восстановление пароля для работы в портативном режиме

Если вы забыли пароль для работы в портативном режиме, вам нужно подключить съемный диск к компьютеру с установленной программой 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 установлена программа 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 программа 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 папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. На закладке **Устройства** выделите компьютер пользователя, запросившего восстановление доступа к зашифрованным данным, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
6. В открывшемся окне выберите закладку **Шифрование данных**.
7. На закладке **Шифрование данных** нажмите на кнопку **Обзор**.
8. 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.

Как получить файл доступа к зашифрованным данным в Web Console

1. В главном окне Web Console выберите **Устройства** → **Управляемые 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. 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 закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Шифрование данных → Шифрование съемных дисков**.
6. Если вы хотите расшифровать все зашифрованные файлы, хранящиеся на съемных дисках, в раскрывающемся списке **Режим шифрования** выберите действие **Расшифровывать весь съемный диск**.
7. 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.
      Откроется контекстное меню кнопки **Задать правило**.
   c. В контекстном меню кнопки **Задать правило** выберите пункт **Расшифровывать все файлы**.
8. Сохраните внесенные изменения.

В результате, если пользователь подключает съемный диск или он уже подключен, Kaspersky Endpoint Security расшифровывает съемный диск. Программа 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 другой программой. 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.

Возможны следующие статусы шифрования:

- *Не задана политика шифрования*. Для компьютера не назначена политика шифрования Kaspersky Security Center.
- *В процессе применения политики*. На компьютере выполняется шифрование и / или расшифровка данных.
- *Ошибка*. Во время шифрования и / или расшифровки данных на компьютере возникла ошибка.
- *Требуется перезагрузка*. Для инициализации или завершения шифрования или расшифровки данных на компьютере требуется перезагрузка операционной системы.
- *Соответствует политике*. Шифрование данных на компьютере выполнено в соответствии с параметрами шифрования, указанными в примененной к компьютеру политике Kaspersky Security Center.
- *Отменено пользователем*. Пользователь отказался подтвердить выполнение операции шифрования файлов на съемном диске.

Просмотр статусов шифрования

Чтобы просмотреть статус шифрования данных компьютера, выполните следующие действия:

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 закладку **Устройства**.

   На закладке **Устройства** в рабочей области отображаются свойства компьютеров выбранной группы администрирования.
4. На закладке **Устройства** рабочей области сдвиньте полосу прокрутки до упора вправо.
5. Если графа **Статус шифрования** не отображается, выполните следующие действия:

   a. По правой клавиши мыши откройте контекстное меню для заголовочной части таблицы.

   b. В контекстном меню в выпадающем списке **Вид** выберите **Добавить или удалить графы**.

   Откроется окно **Добавление или удаление граф**.

   c. В окне **Добавление или удаление граф** установите флажок **Статус шифрования**.

   d. Нажмите на кнопку **ОК**.

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.

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 – <Имя компьютера>**.
3. В рабочей области, расположенной справа от дерева Консоли администрирования, выберите закладку **Статистика**.
4. Создайте новую страницу с информационными панелями со статистикой шифрования данных. Для этого выполните следующие действия:
   a. На закладке **Статистика** нажмите на кнопку **Настроить вид**.
      Откроется окно **Свойства: Статистика**.
   b. В окне **Свойства: Статистика** нажмите на кнопку **Добавить**.
      Откроется окно **Свойства: Новая страница**.
   c. В разделе **Общие** окна **Свойства: Новая страница** введите название страницы.
   d. В разделе **Информационные панели** нажмите на кнопку **Добавить**.
      Откроется окно **Новая информационная панель**.
   e. В окне **Новая информационная панель** в группе **Состояние защиты** выберите элемент **Шифрование устройств**.
   f. Нажмите на кнопку **ОК**.
      Откроется окно **Свойства: Шифрование устройств**.
   g. Измените при необходимости параметры информационной панели. Для этого воспользуйтесь разделами **Вид** и **Устройства** окна **Свойства: Шифрование устройств**.
   h. Нажмите на кнопку **ОК**.
   i. Повторите пункты d – h инструкции, при этом в окне **Новая информационная панель** в группе **Состояние защиты** выберите элемент **Шифрование съемных дисков**.
      Добавленные информационные панели отобразятся в списке **Информационные панели** окна **Свойства: Новая страница**.
   j. В окне **Свойства: Новая страница** нажмите на кнопку **ОК**.
      Название созданной на предыдущих шагах страницы с информационными панелями отобразится в списке **Страницы** окна **Свойства: Статистика**.
   k. В окне **Свойства: Статистика** нажмите на кнопку **Закрыть**.
5. На закладке **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 папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, где находится компьютер пользователя, для которого вы хотите просмотреть список ошибок шифрования файлов.

3. В рабочей области выберите закладку **Устройства**.

4. На закладке **Устройства** выделите в списке компьютер и по правой клавише мыши вызовите контекстное меню.

5. В контекстном меню компьютера выберите пункт **Свойства**. В открывшемся окне **Свойства: <название компьютера>** выберите раздел **Защита**.

6. В разделе **Защита** окна **Свойства: <название компьютера>** 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

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 закладку **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 следующих пунктов:

   - **Отчет о статусе шифрования управляемых устройств**.
   - **Отчет о статусе шифрования запоминающих устройств**.
   - **Отчет об ошибках шифрования файлов**.
   - **Отчет о блокировании доступа к зашифрованным файлам**.

   После завершения работы мастера создания шаблона отчета в таблице на закладке **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 программы 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.

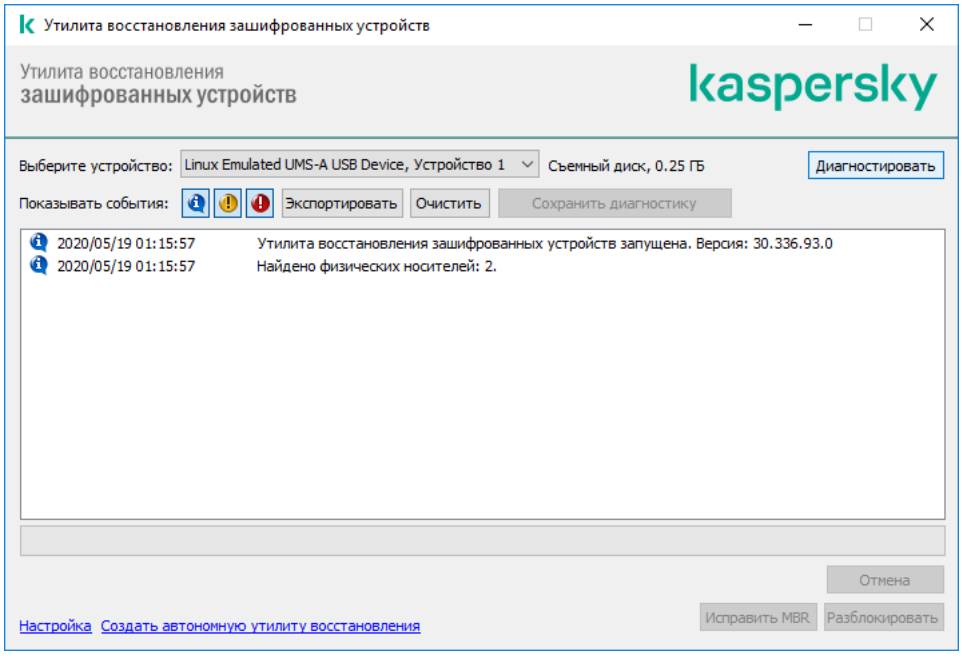
Перед восстановлением данных на зашифрованных устройствах рекомендуется вывести компьютер, на котором будет выполняться процедура, из-под действия политики Kaspersky Security Center или отключить шифрование в параметрах политики Kaspersky Security Center. Это позволяет предотвратить повторное шифрование 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 программы нажмите на кнопку **Поддержка**.
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 программы Kaspersky Endpoint Security.

2. В окне утилиты восстановления в раскрывающемся списке **Выберите устройство** 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 устройства**.
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 (11.6.0)**.

   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 (11.6.0)**.

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 программой.

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 Control выберите **Операции → Шифрование и защита данных → Зашифрованные устройства**.

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 программой.

   c. Нажмите на кнопку **Выбрать файл** и выберите файл запроса, полученного от пользователя (файл с расширением fdertc).

   d. Нажмите на кнопку **Сохранить ключ** и 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).

Управление программой из командной строки

Вы можете управлять Kaspersky Endpoint Security из командной строки. Вы можете просмотреть список команд для управления программой с помощью команды `HELP`. Чтобы получить справку по синтаксису конкретной команды, введите `HELP <команда>`.

Специальные символы в команде нужно экранировать. Для экранирования символов &, |, (,), <, >, ^ используйте символ ^ (например, чтобы использовать символ `&` введите `^&`). Для экранирования символа `%`, введите `%%`.

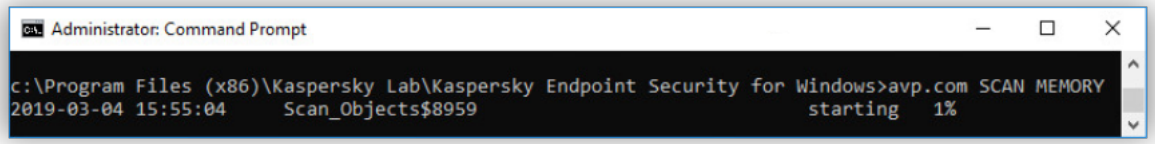
Команды AVP

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.
3. Используйте следующий шаблон для выполнения команды:

```
avp.com <команда> [параметры]
```

В результате Kaspersky Endpoint Security выполнит команду (см. рис. ниже).



Управление программой из командной строки

SCAN. Антивирусная проверка

Запустить задачу антивирусной проверки.

Синтаксис команды

```
SCAN [<область проверки>] [<действие при обнаружении угрозы>] [<типы файлов>]
[<исключения из проверки>] [/R[A]:<файл отчета>] [<технологии проверки>] [/C:<файл с
параметрами антивирусной проверки>]
```

Область проверки	

<файлы для проверки>	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 *Полная проверка*. 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.
/MEMORY	Проверить память ядра.
/STARTUP	Проверить объекты, загрузка которых осуществляется при запуске операционной системы.
/MAIL	Проверить почтовый ящик Outlook.
/REMDRIVES	Проверить съемные диски.
/FIXDRIVES	Проверить жесткие диски.
/NETDRIVES	Проверить сетевые диски.
/QUARANTINE	Проверить файлы в резервном хранилище Kaspersky Endpoint Security.
/@:<список файлов.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; блокировать, 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.
	Лечить; удалять, если лечение невозможно. Если выбран этот вариант действия, то

`/i2`	Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет. Этот вариант действия выбран по умолчанию.
`/i3`	Лечить обнаруженные зараженные файлы. Если лечение невозможно, удалять зараженные файлы. Также удалять составные файлы (например, архивы), если вылечить или удалить зараженный файл невозможно.
`/i4`	Удалять зараженные файлы. Также удалять составные файлы (например, архивы), если удалить зараженный файл невозможно.
`/i8`	Запрашивать действие у пользователя сразу после обнаружения угрозы.
`/i9`	Запрашивать действие у пользователя после выполнения проверки.

Типы файлов	
`/fe`	Файлы, проверяемые по расширению. Если выбран этот параметр, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
`/fi`	Файлы, проверяемые по формату. Если выбран этот параметр, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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:b`	Исключение из проверки почтовых баз, входящих и исходящих сообщений электронной почты.
`-e:<маска файла>`	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:<секунды>`	Исключение из проверки файлов, длительность проверки которых превышает установленное значение в секундах.
`-es:<мегабайты>`	Исключение из проверки файлов, размер которых превышает установленное значение в мегабайтах.

Режим сохранения событий в файл отчета	
`/R:<файл отчета>`	Сохранять только критические события в файл отчета.
`/RA:<файл отчета>`	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 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 программе 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:<файл с параметрами антивирусной проверки>`	Файл с параметрами задачи антивирусной проверки. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: `[<область проверки>] [<действие при обнаружении угрозы>] [<типы файлов>] [<исключения из проверки>] [/R[A]:<файл отчета>] [<технологии проверки>]`.

Пример:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Обновление баз и модулей программы

Запустить задачу *Обновление*.

Синтаксис команды

```
UPDATE [local] ["<источник обновления>"] [/R[A]:<файл отчета>] [/C:<файл с параметрами обновления>]
```

Параметры задачи обновления	
`local`	Запуск задачи *Обновление*, созданной автоматически после установки программы. Вы можете изменить параметры задачи *Обновление* в локальном интерфейсе программы или в консоли Kaspersky Security Center. Если этот параметр не установлен, Kaspersky Endpoint Security запускает задачу *Обновление* с параметрами по умолчанию или с параметрами, заданными в команде. Таким образом, вы можете настроить параметры задачи Обновление, следующим образом: • `UPDATE` – запуск задачи *Обновление* с параметрами по умолчанию: источник обновления – серверы обновлений "Лаборатории Касперского", учетная запись – System, и другие.

	• `UPDATE local` – запуск задачи *Обновление*, созданной автоматически после установки (предустановленная задача). • `UPDATE <параметры обновления>` – запуск задача *Обновление* с параметрами, заданными вручную (см. ниже).

Источник обновления	
`"<источник обновления>"`	Адрес HTTP-, FTP-сервера или папки общего доступа с пакетом обновлений. Вы можете указать только один источник обновления. Если источник обновлений не указан, Kaspersky Endpoint Security использует источник по умолчанию – серверы обновлений "Лаборатории Касперского".

Режим сохранения событий в файл отчета	
`/R:<файл отчета>`	Сохранять только критические события в файл отчета.
`/RA:<файл отчета>`	Сохранять все события в файл отчета.

Дополнительные параметры	
`/C:<файл с параметрами обновления>`	Файл с параметрами задачи *Обновление*. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: `["<источник обновления>"] [/R[A]:<файл отчета>]`.

Пример:
```
avp.com UPDATE local

avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Откат последнего обновления

Откатить последние обновления антивирусных баз. Это позволяет вернуться к использованию предыдущей версии баз и модулей программы при необходимости, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасную программу.

Синтаксис команды

```
ROLLBACK [/R[A]:<файл отчета>]
```

Режим сохранения событий в файл отчета	
`/R:<файл отчета>`	Сохранять только критические события в файл отчета.
`/RA:<файл отчета>`	Сохранять все события в файл отчета.

Пример:
```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Трассировка

Включить / выключить трассировку. Файлы трассировки хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы. Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке %ProgramData%\Kaspersky Lab\KES\Traces. По умолчанию трассировка выключена.

Синтаксис команды

```
TRACES on|off [<уровень трассировки>] [<дополнительные параметры>]
```

Уровень трассировки	
`<уровень трассировки>`	Уровень детализации трассировки. Возможные значения: • `100` (критический). Только сообщения о неустранимых ошибках. • `200` (высокий). Сообщения о всех ошибках, включая неустранимые. • `300` (диагностический). Сообщения о всех ошибках, а также предупреждения. • `400` (важный). Сообщения о всех ошибках, предупреждения, а также дополнительная информация. • `500` (обычный). Сообщения о всех ошибках, предупреждениях, а также подробная информация о работе программы в нормальном режиме (значение по умолчанию). • `600` (низкий). Все сообщения.

Дополнительные параметры	
`all`	Выполнить команду с параметрами `dbg`, `file` и `mem`.
`dbg`	Использовать функцию OutputDebugString и сохранять файл трассировки. Функция OutputDebugString отправляет символьную строку отладчику программы для вывода на экран. Подробнее см. на *сайте MSDN*.
`file`	Сохранить один файл трассировки (без ограничений по размеру).
`rot`	Сохранить результаты трассировки в ограниченное число файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера.
`mem`	Записывать результаты трассировки в файлы дампов.

Примеры:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`

- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

START. Запуск профиля

Запустить выполнение профиля (например, запустить обновление баз или включить компонент защиты).

Синтаксис команды

```
START <профиль> [/R[A]:<файл отчета>]
```

Профиль	
`<профиль>`	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	
`/R:<файл отчета>`	Сохранять только критические события в файл отчета.
`/RA:<файл отчета>`	Сохранять все события в файл отчета.

Пример:

```
avp.com START Scan_Objects
```

STOP. Остановка профиля

Остановить выполняемый профиль (например, остановить проверку съемных дисков или выключить компонент защиты).

Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешения **Выключение компонентов защиты**, **Выключение компонентов контроля**.

Синтаксис команды

```
STOP <профиль> /login=<имя пользователя> /password=<пароль>
```

Профиль	
`<профиль>`	Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей вы можете узнать по команде `HELP STOP`.

Авторизация	
`/login=<имя пользователя>`	Учетные данные пользователя с необходимыми

`/password=<пароль>`	разрешениями Защиты паролем.

STATUS. Статус профиля

Показать информацию о состоянии профилей программы (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".

Синтаксис команды

```
STATUS [<профиль>]
```

STATISTICS. Статистика выполнения профиля

Показать статистическую информацию о профиле программы (например, время проверки или количество обнаруженных угроз). Список доступных профилей вы можете узнать по команде `HELP STATISTICS`.

Синтаксис команды

```
STATISTICS <профиль>
```

RESTORE. Восстановление файлов

Восстановить файл из резервного хранилища в папку его исходного размещения. Если по указанному пути уже существует файл с таким же именем, к имени файла добавляется суффикс "-copy". 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\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.

Синтаксис команды

```
RESTORE [/REPLACE] <имя файла> /login=<имя пользователя> /password=<пароль>
```

Дополнительные параметры	
`/REPLACE`	Переписать существующий файл.
`<имя файла>`	Имя восстанавливаемого файла.

Авторизация	
`/login=<имя пользователя>` `/password=<пароль>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

Пример:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Экспорт параметров программы

Экспортировать параметры Kaspersky Endpoint Security в файл. Файл будет размещен в папке C:\Windows\SysWOW64.

Синтаксис команды

```
EXPORT <профиль> <имя файла>
```

Профиль	
`<профиль>`	Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей вы можете узнать по команде `HELP EXPORT`.

Файл для экспорта	
`<имя файла>`	Имя файла, в который должны быть экспортированы параметры профиля. 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.

Примеры:

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

IMPORT. Импорт параметров программы

Импортировать параметры 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 параметров программы**.

Синтаксис команды

```
IMPORT <имя файла> /login=<имя пользователя> /password=<пароль>
```

Файл для импорта	
`<имя файла>`	Имя файла, из которого должны быть импортированы параметры программы. 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=<имя пользователя> /password=<пароль>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем.

Пример:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. Применение файла ключа

Применить файл ключа для активации Kaspersky Endpoint Security. Если программа уже активирована, ключ будет добавлен в качестве резервного.

Синтаксис команды

```
ADDKEY <имя файла> [/login=<имя пользователя> /password=<пароль>]
```

Файл ключа	
`<имя файла>`	Имя файла ключа.

Авторизация	
`/login=<имя пользователя> /password=<пароль>`	Данные учетной записи пользователя. Данные учетные записи нужно вводить, только если включена Защита паролем.

Пример:

```
avp.com ADDKEY file.key
```

LICENSE. Лицензирование

Выполнить операции с лицензионными ключами программы Kaspersky Endpoint Security.

Для выполнения команды удаления лицензионного ключа должна быть включена Защита паролем. Пользователь должен иметь разрешение **Удаление ключа**.

Синтаксис команды

```
LICENSE <операция> [/login=<имя пользователя> /password=<пароль>]
```

Операция	
`/ADD <имя файла>`	Применить файл ключа для активации Kaspersky Endpoint Security. Если программа уже активирована, ключ будет добавлен в качестве резервного.
`/ADD <код активации>`	Активировать Kaspersky Endpoint Security с помощью кода активации. Если программа уже активирована, ключ будет добавлен в качестве резервного.
`/REFRESH <имя файла>`	Продлить срок действия лицензии с помощью файла ключа. В результате будет добавлен резервный ключ, который станет активным по истечении срока действия лицензии. Добавить активный ключ с помощью этой команды невозможно.
`/REFRESH <код активации>`	Продлить срок действия лицензии с помощью кода активации. В результате будет добавлен резервный ключ, который станет активным по истечении срока действия лицензии. Добавить активный ключ с помощью этой команды невозможно.
`/DEL /login=<имя пользователя> /password=<пароль>`	Удалить лицензионный ключ. Также будет удален резервный ключ.

Авторизация	
`/login=<имя пользователя> /password=<пароль>`	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 /login=KLAdmin /password=!Password1`

RENEW. Покупка лицензии

Перейти на веб-сайт "Лаборатории Касперского" для покупки лицензии или продления ее срока действия.

PBATESTRESET. Сбросить результаты проверки перед шифрованием диска

Сбросить результаты проверки поддержки полнодискового шифрования (FDE) по технологиям Шифрование диска Kaspersky и BitLocker.

Перед запуском полнодискового шифрования программа выполняет ряд проверок на возможность шифрования компьютера. Если полнодисковое шифрование невозможно, Kaspersky Endpoint Security сохраняет информацию о несовместимости. При следующей попытке шифрования программа 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 программой при предыдущей проверке.

EXIT. Завершение работы программы

Завершить работу Kaspersky Endpoint Security. Программа будет выгружена из оперативной памяти компьютера.

Для выполнения команды должна быть включена Защита паролем. Пользователь должен иметь разрешение **Завершение работы программы**.

Синтаксис команды

```
EXIT /login=<имя пользователя> /password=<пароль>
```

EXITPOLICY. Выключение политики

Выключает политику 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**.

Синтаксис команды

```
EXITPOLICY /login=<имя пользователя> /password=<пароль>
```

STARTPOLICY. Включение политики

Включить политику Kaspersky Security Center на компьютере. Параметры программы будут настроены в соответствии с политикой.

DISABLE. Выключение защиты

Выключить Защиту от файловых угроз на компьютере с истекшей лицензией на Kaspersky Endpoint Security. Выполнить команду на компьютере с неактивированной программой или с действующей лицензией невозможно.

SPYWARE. Обнаружение шпионского ПО

Включить / выключить обнаружение шпионского ПО. По умолчанию обнаружение шпионского ПО включено.

Синтаксис команды

```
SPYWARE on|off
```

MDRLICENSE. Активация MDR

Выполнить операции с конфигурационным файлом 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 ( ).

Синтаксис команды

```
MDRLICENSE <операция> [/login=<имя пользователя> /password=<пароль>]
```

Операция	
`/ADD <имя файла>`	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=<имя пользователя>`	Учетные данные пользователя с необходимыми

/password=<пароль>	разрешениями Защиты паролем.

Пример:

- avp.com MDRLICENSE /ADD file.key
- avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1

KSN. Переключение Глобальный / Локальный KSN

Выбор решения Kaspersky Security Network для определения репутации файлов или сайтов. Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения KSN:

- *Глобальный KSN* – это решение, которое используют большинство программ "Лаборатории Касперского". Участники KSN получают информацию от Kaspersky Security Network, 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 Security Network.
- *Локальный KSN* – это решение, позволяющее пользователям компьютеров, на которые установлена программа Kaspersky Endpoint Security или другие программы "Лаборатории Касперского", получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в KSN со своих компьютеров. Локальный KSN 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.

Синтаксис команды

KSN /global | /**private** <имя файла>

Конфигурационный файл Локального KSN	
<имя файла>	Имя конфигурационного файла с параметрами прокси-сервера KSN. Файл имеет разрешение PKCS7 или PEM.

Пример:

avp.com KSN /global

avp.com KSN /private C:\ksn_config.pkcs7

Команды KESCLI

Команды KESCLI позволяют получать информацию о состоянии защиты компьютера с помощью компонента OPSWAT, а также выполнять стандартные задачи (например, антивирусная проверка, обновление баз).

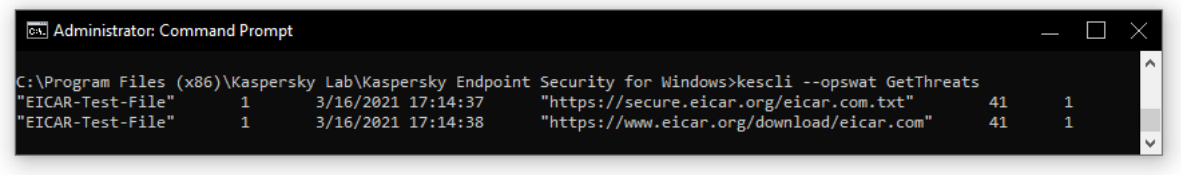
Вы можете просмотреть список команд KESCLI с помощью команды `--help` или сокращенной команды `-h`.

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.
3. Используйте следующий шаблон для выполнения команды:

```
kescli <команда> [параметры]
```

В результате Kaspersky Endpoint Security выполнит команду (см. рис. ниже).



Управление программой из командной строки

Scan. Антивирусная проверка

Запустить задачу антивирусной проверки.

Синтаксис команды

```
--opswat Scan <область проверки> <действие при обнаружении угрозы>
```

Вы можете проверить статус выполнения задачи *Полная проверка* с помощью команды `GetScanState` и посмотреть дату и время последнего выполнения проверки с помощью команды `GetLastScanTime`.

Область проверки	
`<файлы для проверки>`	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

	Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет. 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

Получить информацию о статусе выполнения задачи *Полная проверка*.

- `1` – проверка выполняется.
- `0` – проверка не запущена.

Синтаксис команды
```
--opswat GetScanState
```

Пример:
```
kescli --opswat GetScanState
```

GetLastScanTime. Определения времени выполнения проверки

Получить информацию о дате и времени последнего выполнения задачи *Полная проверка*.

Синтаксис команды
```
--opswat GetLastScanTime
```

Пример:
```
kescli --opswat GetLastScanTime
```

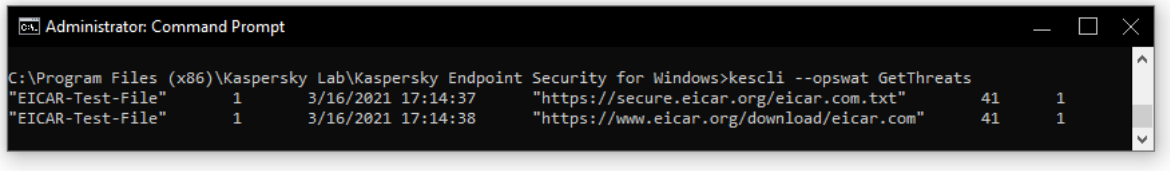
GetThreats. Получение данных об обнаруженных угрозах

Получить список обнаруженных угроз (*Отчет об угрозах*). Отчет содержит информацию об угрозах и вирусной активности за 30 дней до момента создания отчета.

Синтаксис команды
```
--opswat GetThreats
```

В результате выполнение команды Kaspersky Endpoint Security отправит ответ в следующем формате:

`<имя обнаруженного объекта>` `<тип объекта>` `<дата и время обнаружения>` `<путь к файлу>` `<действие при обнаружении угрозы>` `<уровень опасности угрозы>`



Управление программой из командной строки

Тип объекта	
`0`	Неизвестно (`Unknown`).
`1`	Вирусы (`Virware`).
`2`	Троянские программы (`Trojware`).
`3`	Вредоносные программы (`Malware`).
`4`	Рекламные программы (`Adware`).
`5`	Программы автодозвона (`Pornware`).
`6`	Программы, 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 программы (`Software`).
`22`	Скрытые файлы (`Hidden`).
`23`	Программа, требующая 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`	Вредоносная программы, обнаруженная с помощью Kaspersky Security Network (`Urgent`).
`100`	Неизвестная ссылка (`Suspic URL`).
`110`	Другая вредоносная программа (`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 программы

Запустить задачу *Обновление*. Kaspersky Endpoint Security использует источник по умолчанию – серверы обновлений "Лаборатории Касперского".

Синтаксис команды

```
--opswat UpdateDefinitions
```

Вы можете просмотреть дату и время выполнения последней задачи *Обновление* с помощью команды `GetDefinitionsetState`.

Пример:

```
kescli --opswat UpdateDefinitions
```

GetDefinitionState. Определение времени выполнения обновления

Получить информацию о дате и времени последнего выполнения задачи *Обновление*.

Синтаксис команды

```
--opswat GetDefinitionState
```

Пример:

```
kescli --opswat GetDefinitionState
```

EnableRTP. Включение защиты

Включить компоненты защиты Kaspersky Endpoint Security на компьютере: Защита от файловых угроз, Защита от веб-угроз, Защита от почтовых угроз, Защита от сетевых угроз, Предотвращение вторжений.

Синтаксис команды

```
--opswat EnableRTP
```

Вы можете проверить статус работы Защиты от файловых угроз с помощью команды `GetRealTimeProtectionState`.

Пример:

```
kescli --opswat EnableRTP
```

GetRealTimeProtectionState. Статус Защиты от файловых угроз

Получить информацию о статусе работы компонента Защита от файловых угроз:

- 1 – компонент включен.

- `0` – компонент выключен.

Синтаксис команды

```
--opswat GetRealTimeProtectionState
```

Пример:
`kescli --opswat GetRealTimeProtectionState`

Version. Определение версии программы

Определить версию программы Kaspersky Endpoint Security для Windows.

Синтаксис команды

```
--Version
```

Вы также можете использовать сокращенную команду `-v`.

Пример:
`kescli -v`

Коды ошибок

При работе с программой 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	Лицензионный ключ для Kaspersky Endpoint Security уже используется на этом компьютере.
0947901D	Срок действия лицензии истек. 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 или срок годности лицензионного ключа.
89479007	Файл ключа не указан.
89479008	Невозможно применить 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.
89479014	Цифровая подпись файла не соответствует цифровой подписи "Лаборатории Касперского".
89479015	Невозможно использовать ключ для некоммерческой лицензии в качестве ключа для коммерческой лицензии.
89479016	Чтобы использовать бета-версию программы, требуется лицензия на бета-тестирование.
89479017	Файл ключа не подходит для данной программы.
89479018	Ключ заблокирован "Лабораторией Касперского".
89479019	Программа уже использовалась по пробной лицензии. Невозможно снова добавить ключ для пробной лицензии.
8947901A	Файл ключа поврежден.
8947901B	Цифровая подпись не найдена, повреждена или не соответствует цифровой 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	Ошибка в служебных данных о лицензионном ключе.
89479023	Невозможно применить недействительный файл ключа для добавления резервного ключа.
89479025	Ошибка при отправке запроса на сервер активации. Возможные причины: ошибка соединения с интернетом или временные проблемы на сервере активации. Попробуйте активировать программу с помощью кода активации позже. В случае повторения ошибки обратитесь к вашему интернет-провайдеру.
89479026	Ошибка в ответе от сервера 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	Файл ключа не подходит для данной программы или истек срок действия лицензии.

	Невозможно активировать Kaspersky Endpoint Security с помощью файла ключа для другой программы.
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	Сервер активации возвратил ошибку 404.
89479030	Сервер активации возвратил ошибку 405.
89479031	Сервер активации возвратил ошибку 406.
89479032	Требуется аутентификация на прокси-сервере. Проверьте параметры сети.
89479033	Время ожидания запроса истекло.
89479034	Сервер активации возвратил ошибку 409.
89479035	Сервер активации возвратил ошибку 410.
89479036	Сервер активации возвратил ошибку 411.
89479037	Сервер активации возвратил ошибку 412.
89479038	Сервер активации возвратил ошибку 413.
89479039	Сервер активации возвратил ошибку 414.
8947903A	Сервер активации возвратил ошибку 415.
8947903C	Внутренняя ошибка сервера.
8947903D	Функциональность не поддерживается.
8947903E	Некорректный ответ от шлюза. Проверьте параметры сети.
8947903F	Служба недоступна (ошибка HTTP 503).
89479040	Время ожидания ответа от шлюза истекло. Проверьте параметры 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 годности лицензионного ключа истек.
89479054	На компьютере установлена некорректная системная дата.
89479055	Срок действия пробной лицензии истек.
89479056	Истек срок действия лицензии.
89479057	Превышено допустимое количество активаций программы с помощью указанного кода.
89479058	Процедура активации завершилась с системной ошибкой.
89479059	Невозможно использовать ключ для некоммерческой лицензии в качестве ключа для коммерческой лицензии.
8947905C	Требуется код активации.
89479062	Невозможно подключиться к серверу активации.
89479064	Сервер активации недоступен. Проверьте параметры подключения к интернету и попробуйте активировать программу снова.
89479065	Дата выпуска баз программы превышает дату окончания срока действия лицензии.
89479066	Невозможно заменить активный ключ на ключ с истекшим сроком годности.
89479067	Невозможно добавить резервный ключ, если его срок годности истекает раньше по сравнению с действующей лицензией.
89479068	Отсутствует обновленный ключ по подписке.
8947906A	Неверный код активации (не совпадает контрольная сумма).
8947906B	Ключ уже активен.
8947906C	Типы лицензий, которые соответствуют активному и резервному ключам, не совпадают.
8947906D	Лицензия не допускает работу компонента.
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. Проверьте параметры подключения к интернету.
89479218	Не удалось связаться с сервером активации или с прокси-сервером.
89479219	Отказ в удалённом доступе.
8947921A	Время ожидания ответа истекло.
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 активации.
89479221	Ошибка отправки данных.
89479222	Ошибка приема данных.
89479223	Ошибка локального SSL-сертификата.
89479224	Ошибка SSL-шифрования.
89479225	Ошибка SSL-сертификата сервера.
89479226	Некорректное содержимое сетевого пакета.
89479227	Пользователю отказано в доступе.
89479228	Некорректный файл SSL-сертификата.
89479229	Не удалось установить SSL-соединение.
8947922A	Не удалось отправить или принять сетевой пакет. Повторите попытку позднее.
8947922B	Некорректный файл с отозванными сертификатами.
8947922C	Ошибка запроса SSL-сертификата.
89479401	Неизвестная ошибка сервера.
89479402	Внутренняя ошибка сервера.
89479403	Лицензионный ключ для введенного кода активации отсутствует.
89479404	Активный ключ заблокирован.
89479405	Отсутствуют обязательные параметры запроса для активации программы.
89479406	Неверные имя пользователя или пароль.
89479407	На сервер передан неверный код активации.
89479408	Код активации не подходит для Kaspersky Endpoint Security. Неизвестно, для какой программы предназначен код активации.
89479409	В запросе отсутствует код активации.
8947940B	Истек срок действия лицензии (по данным от сервера активации).
8947940C	Превышено число активаций программы с помощью этого кода активации.
8947940D	Неверный формат идентификатора запроса.
8947940E	Код активации не подходит для Kaspersky Endpoint Security. Код активации предназначен для другой программы "Лаборатории Касперского".
8947940F	Невозможно обновить лицензионный ключ.
89479410	Код активации не подходит для этого региона.
89479411	Код активации не подходит для языковой версии Kaspersky Endpoint Security.
89479412	Требуется дополнительное обращение к серверу 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	Формат кода активации не поддерживается сервером активации.
89479418	Неверный формат кода активации.
89479419	На компьютере установлено некорректное системное время.
8947941A	Код активации не подходит для версии Kaspersky Endpoint Security.
8947941B	Подписка истекла.
8947941C	Превышен предел количества активаций для данного лицензионного ключа.
8947941D	Неверная цифровая подпись лицензионного ключа.
8947941E	Требуются дополнительные данные пользователя.
8947941F	Проверка данных пользователя завершена с ошибкой.
89479420	Подписка неактивна.
89479421	Технические работы на сервере активации.
89479501	Неизвестная ошибка на стороне Kaspersky Endpoint Security.
89479502	Передан недопустимый параметр (например, пустой список адресов серверов активации).
89479503	Неверный код активации.
89479504	Неверное имя пользователя.
89479505	Неверный пароль пользователя.
89479506	Сервер активации вернул неверный ответ.
89479507	Запрос на активацию прерван.
89479509	Сервер активации вернул пустой список переадресации.

Приложение. Профили программы

Профиль – компонент, задача или функция Kaspersky Endpoint Security. Профили предназначены для управления программой из командной строки. Вы можете использовать профили для выполнения команд `START`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT` и `IMPORT`. С помощью профилей вы можете настроить параметры программы (например, `STOP DeviceControl`) или запустить задачу (например, `START Scan_My_Computer`).

Доступны следующие профили:

- `AdaptiveAnomaliesControl` – Адаптивный контроль аномалий.
- `AMSI` – AMSI-защита.
- `BehaviorDetection` – Анализ поведения.
- `DeviceControl` – Контроль устройств.
- `EntAppControl` – Контроль программ.
- `File_Monitoring` или `FM` – Защита от файловых угроз.
- `Firewall` или `FW` – Сетевой экран.

- `HIPS` – Предотвращение вторжений.
- `IDS` – Защита от сетевых угроз.
- `IntegrityCheck` – Проверка целостности.
- `Mail_Monitoring` или `EM` – Защита от почтовых угроз.
- `Rollback` – Откат обновления.
- `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.
- `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 программой через REST API

Kaspersky Endpoint Security позволяет настраивать параметры программы, 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 программы 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 программой 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 программы с REST API

Для управления программой через REST API нужно установить Kaspersky Endpoint Security с поддержкой REST API. Если вы управляете Kaspersky Endpoint Security через REST API, управлять программой с помощью Kaspersky Security Center невозможно.

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=<Имя пользователя>`

     Имя пользователя для управления программой через REST API. Введите имя пользователя в формате `<DOMAIN>\<UserName>` (например, `RESTAPI_User=COMPANY\Administrator`). Вы можете управлять программой через REST API только под этой учетной записью. Для работы с REST API вы можете выбрать только одного пользователя.
   - `RESTAPI_Port=<Порт>`

     Порт для обмена данными. Необязательный параметр. По умолчанию выбран порт 6782.
   - `AdminKitConnector=1`

Управление программой с помощью систем администрирования. По умолчанию управление разрешено.

Также вы можете задать параметры работы с REST API с помощью файла setup.ini.

Вы можете задать параметры работы с REST API только во время установки программы. Изменить параметры после установки программы невозможно. Если вы хотите изменить параметры, удалите Kaspersky Endpoint Security и установите заново с новыми параметрами работы с REST API.

Пример:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator /s
```

В результате вы сможете управлять программой через REST API. Для проверки работы откройте документацию REST API с помощью GET-запроса.

Пример:

```
GET http://localhost:6782/kes/v1/api-docs
```

Работа с API

Ограничить доступ к программе 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 программе через локальный интерфейс.

Для управления программой через REST API нужно запустить REST-клиент под учетной записью, которую вы задали при установке программы с поддержкой REST API. Для работы с REST API вы можете выбрать только одного пользователя.

ОТКРЫТЬ ДОКУМЕНТАЦИЮ REST API

Управление программой через REST API состоит из следующих этапов:

1. Получите текущие значения параметров программы. Для этого отправьте GET-запрос.

   Пример:

   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. Программа 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 программы. Для этого отправьте POST-запрос. Используйте структуру параметров, полученную в ответ от GET-запроса.

Пример:

```
POST http://localhost:6782/kes/v1/settings/ExploitPrevention
{
"action": 0,
"enableSystemProcessesMemoryProtection": false,
"enabled": true
}
```

4. Программа применит изменения в параметрах и отправит ответ с результатами настройки программы.

Источники информации о программе

Страница Kaspersky Endpoint Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Security вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Endpoint Security содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

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 программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Endpoint Security, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе.

В сообществе 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 программ). 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 программы и обнаружить, на каком этапе работы программы возникает ошибка.

Кроме того, специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на компьютере, подробные отчеты работы компонентов программы.

Во время работ по диагностике специалисты Службы технической поддержки могут попросить вас изменить параметры программы:

- Активировать функциональность получения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, 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 программы способами, не описанными в Руководстве администратора 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 программы и безвозвратно удаляются при удалении программы.

Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке %ProgramData%\Kaspersky Lab\KES\Traces.

Файлы трассировки называются следующим образом: `KES<служебный номер версии_dateXX.XX_timeXX.XX_pidXXX.><тип файла трассировки>.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 программы, в результате работы которого произошло событие.
- Степень важности события (информационное, предупреждение, критическое, ошибка).
- Описание события выполнения команды компонента программы и результата выполнения этой команды.

Kaspersky Endpoint Security сохраняет пароли пользователя в файл трассировки только в зашифрованном виде.

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 программа 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 программа 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 программе.
- 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 программных модулей.

Файл трассировки `BL.log`, помимо общих данных, содержит информацию о событиях, возникающих во время работы программы, а также данные, необходимые для устранения неполадок в работе программы. Этот файл создается, если программа 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 программы.

Файл трассировки `WD.log`, помимо общих данных, содержит информацию о событиях, возникающих в процессе работы службы avpsus, в том числе события обновления программных модулей.

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<номер версии_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 программ, 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 программы.

Содержание файлов трассировки веб-плагина программы

Файлы трассировки веб-плагина программы хранятся на компьютере, на котором развернута Kaspersky Security Center 12 Web Console, в папке Program Files\Kaspersky Lab\Kaspersky Security Center Web Console 12\logs.

Файлы трассировки веб-плагина программы называются следующим образом: `logs-kes_windows-<тип файла трассировки>.DESKTOP-<дата обновления файла>.log`. Web Console начинает записывать данные после установки и удаляет файлы трассировки после удаления Web Console.

Файлы трассировки веб-плагина программы, 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 программы*.
- 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 программы

Трассировка программы – это подробная запись действий, выполняемых программой, и сообщений о событиях, происходящих во время работы программы.

Выполняйте трассировку программы под руководством Службы технической поддержки "Лаборатории Касперского".

Чтобы создать файл трассировки программы, выполните следующие действия:

1. В главном окне программы нажмите на кнопку .

   Откроется окно **Поддержка**.

2. В окне **Поддержка** нажмите на кнопку **Мониторинг проблем**.

3. Используйте переключатель **Включить трассировку программы**, чтобы включить или выключить трассировку работы программы.

4. В раскрывающемся списке **Трассировка** выберите режим трассировки работы программы:

   - **С ротацией**. Сохранить результаты трассировки в ограниченное число файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера. Если выбран этот режим, вы можете указать максимальное количество файлов для ротации и максимальный размер каждого файла.

   - **Записывать в один файл**. Сохранить один файл трассировки (без ограничений по размеру).

5. В раскрывающемся списке **Уровень** выберите уровень трассировки.

   Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки. Если указания Службы технической поддержки отсутствуют, рекомендуется устанавливать уровень трассировки **Обычный (500)**.

6. Перезапустите Kaspersky Endpoint Security.

7. Чтобы остановить процесс трассировки, вернитесь в окно **Поддержка** и выключите трассировку.

Вы также можете создать файлы трассировки во время установки программы из командной строки, в том числе с помощью файла setup.ini.

Файлы трассировки хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы. Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке %ProgramData%\Kaspersky Lab\KES\Traces. По умолчанию трассировка выключена.

Трассировка производительности программы

Kaspersky Endpoint Security позволяет получить информацию о проблемах в работе компьютера при использовании программы. Например, вы можете получить информацию о задержках при загрузке операционной системы после установки программы. Для этого Kaspersky Endpoint Security создает файлы трассировки производительности. *Трассировка производительности* – это запись действий, выполняемых программой, для диагностики проблем производительности Kaspersky Endpoint Security. Для получения информации Kaspersky Endpoint Security использует сервис трассировки событий Windows (англ. ETW – Event Tracing for Windows). Диагностику работы Kaspersky Endpoint Security и установление причин возникновения проблем выполняет Служба технической поддержки "Лаборатории Касперского".

Выполняйте трассировку программы под руководством Службы технической поддержки "Лаборатории Касперского".

Чтобы создать файл трассировки производительности, выполните следующие действия:

1. В главном окне программы нажмите на кнопку .

   Откроется окно **Поддержка**.

2. В окне **Поддержка** нажмите на кнопку **Мониторинг проблем**.

3. Используйте переключатель **Включить трассировку производительности**, чтобы включить или выключить трассировку производительности программы.

4. В раскрывающемся списке **Трассировка** выберите режим трассировки работы программы:

   - **С ротацией**. 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.

   - **Записывать в один файл**. Сохранить один файл трассировки (без ограничений по размеру).

5. В раскрывающемся списке **Уровень** выберите уровень трассировки:

   - **Легкий**. 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 **Поддержка** и выключите трассировку.

В результате в папке %ProgramData%\Kaspersky Lab\KES\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 программы и безвозвратно удаляются при удалении программы. Файлы дампов хранятся в папке %ProgramData%\Kaspersky Lab\KES\Traces.

Чтобы включить или выключить запись дампов, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Общие**.
3. В блоке **Отладочная информация** используйте флажок **Включить запись дампов**, чтобы включить или выключить запись дампов программы.
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.

Чтобы включить или выключить защиту файлов дампов и файлов трассировки, выполните следующие действия:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Общие**.
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.

Ограничения и предупреждения

Kaspersky Endpoint Security имеет ряд некритичных для работы программы ограничений.

Установка программы

- 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.

- После установки на зараженный компьютер программа не предупреждает пользователя о необходимости запустить проверку компьютера. Могут возникнуть проблемы с активацией программы. 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 программы в параметрах инсталляционного пакета не поддерживается.

- При импорте настроек программы 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 программы или в текстовом файле ksn_*.txt, который расположен в папке с дистрибутивом программы.

- При обновлении с Kaspersky Endpoint Security 10 Service Pack 2 для Windows (сборка 10.3.0.6294) компонент Предотвращение вторжений переводится во включенное состояние.

- При обновлении Kaspersky Endpoint Security 10 для Windows Service Pack 2 (сборка 10.3.0.6294) в резервное хранилище новой версии программы переносятся файлы, которые помещены в резервное хранилище и на карантин в предыдущей версии программы. Для версий ниже Kaspersky Endpoint Security 10 для Windows Service Pack 2 (сборка 10.3.0.6294) эти файлы не переносятся. Для их сохранения необходимо восстановить файлы из карантина и резервного хранилища до начала обновления программы. После завершения обновления выполните повторное сканирование восстановленных файлов.

- 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 попытке установить Модуль шифрования AES любой версии на компьютер с Kaspersky Endpoint Security для Windows 11.6.0 установка Модуля шифрования завершится ошибкой с текстом, что установлена программа более новой версии, если ни один из компонентов шифрования не установлен. Начиная с версии Kaspersky Endpoint Security 10 для Windows Service Pack 2 (версия 10.3.0.6294) отдельного установочного файла для Модуля шифрования нет. Библиотеки шифрования включены в дистрибутив программы. Kaspersky Endpoint Security 11.6.0 несовместим с модулями шифрования AES. Необходимые для шифрования библиотеки устанавливаются автоматически при выборе компонента для шифрования дисков (FDE) или компонента для шифрования файлов и папок (FLE).

- Установка программы может завершиться с ошибкой *На вашем компьютере установлена программа, в которой имя программы отсутствует или нечитаемое*. Это означает, что на вашем компьютере остались несовместимые программы или их фрагменты. Для удаления артефактов несовместимых программ отправьте запрос с подробным описанием ситуации в техническую поддержку "Лаборатории Касперского" через Kaspersky CompanyAccount.

- Начиная с версии программы 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*, *Проверка важных областей*, *Выборочная проверка* и *Проверка целостности*.

- Если вы отменили удаление программы, запустите ее восстановление после перезагрузки компьютера.

- 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.

- Если вы выполняете обновление предыдущей версии программы до версии 11.6.0, для установки Kaspersky Endpoint Agent перезагрузите компьютер и войдите в систему под учетной записью с правами локального администратора, иначе Kaspersky Endpoint Agent в процессе обновления установлен не будет.

- Если установка программы 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 программа была установлена локально в тихом режиме, для смены установленных компонентов используйте подложенный файл setup.ini.

- Если вы обновляете Kaspersky Endpoint Security 10 для Windows Service Pack 2 Maintenance Release 4 с установленным компонентом файлового шифрования (FLE) на компьютерах с операционной системой Windows 10 версии 1809, 1903 и 1909, FDE-драйверы не будут устанавливаться в образ WinRE.

- После установки программы 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.

- После обновления программы с версий ниже Kaspersky Endpoint Security 11 для Windows обязательно перезагружайте компьютер.

Поддержка серверных платформ

- Файловая система ReFS поддерживается с ограничениями:
  - После запуска антивирусной проверки сервера исключения из проверки, добавленные с помощью технологии iChecker, сбрасываются после перезагрузки сервера.
  - Kaspersky Endpoint Security не обнаруживает файлы eicar.com и susp-eicar.com, если файл meicar.exe находился на компьютере до установки Kaspersky Endpoint Security.
- Конфигурации Server Core и Cluster Mode не поддерживаются.
- Шифрование файлов (FLE) и технология Шифрование диска Kaspersky (FDE) на серверных платформах не поддерживаются.
- Контроль устройств на серверных платформах не поддерживается.
- Операционная система Microsoft Windows Server 2008 исключена из поддержки. Установка программы на компьютер под управлением операционной системы Microsoft Windows Server 2008 не поддерживается.
- Если вы запустили несколько рабочих сеансов на терминальном сервере, уведомления Kaspersky Endpoint Security могут работать некорректно. Пример: пользователь сеанса#1 запустил проверку репутации файла в KSN. Kaspersky Endpoint Security покажет уведомление с результатами проверки пользователю сеанса#2.

Поддержка виртуальных платформ

- Не поддерживается полнодисковое шифрование (FDE) на виртуальных машинах Hyper-V.
- Не поддерживается полнодисковое шифрование (FDE) на виртуальных платформах Citrix.
- Операционная система Windows 10 Enterprise multi-session поддерживается с ограничениями:
  - Kaspersky Endpoint Security определяет Windows 10 Enterprise multi-session как операционную систему для сервера. Соответственно, Windows 10 Enterprise multi-session поддерживается с ограничениями серверных платформ. Например, для серверов доступны не все компоненты Kaspersky Endpoint Security. Также для активации программа будет использовать лицензионный ключ для сервера, а не рабочей станции.
  - 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 с Kaspersky Security Center

- Вы можете управлять компонентом Адаптивный контроль аномалий только в Kaspersky Security Center версии 11 и выше.
- В отчете Kaspersky Security Center 11 для угроз, обнаруженных с помощью компонента AMSI-защита, может не отображается информация о действии, предпринятом в отношении угрозы.
- Статус работы компонентов AMSI-защита и Адаптивный контроль аномалий доступен только в Kaspersky Security Center версии 11 и выше. Вы можете просмотреть статус работы в консоли Kaspersky Security Center в свойствах компьютера в разделе **Задачи**. Отчеты для этих компонентов также доступны только в Kaspersky Security Center версии 11 и выше.

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.
- Активация программы по подписке через Kaspersky Security Center не выполняется, если на компьютере истекла лицензия или активна пробная лицензия. Чтобы заменить пробную лицензию или лицензию, которая скоро истечет, на лицензию по подписке, используйте задачу распространения лицензии.
- В интерфейсе программы дата истечения лицензии отображается в локальном времени компьютера.
- Установка программы с подложенным файлом ключа на компьютере с нестабильным доступом в интернет может вызвать временное появление событий о том, что программа не активирована или лицензия не допускает работу компонента. Это вызвано тем, что в процессе установки программа сначала устанавливает и пытается активировать встроенную пробную лицензию, для активации которой требуется доступ в интернет.
- Во время пробного периода установка любого обновления программы или патча на компьютере с нестабильным доступом в интернет может вызвать временное появление событий о том, что программа не активирована. Это вызвано тем, что в процессе установки обновления программа повторно устанавливает и активирует встроенную пробную лицензию, для активации которой требуется доступ в интернет.
- Если при установке программа была автоматически активирована пробной лицензией, а затем удалена без сохранения информации о лицензии, при повторной установке она не активируется пробной лицензией автоматически. В этом случае активируйте программу вручную.
- Если вы используете Kaspersky Security Center версии 11 и Kaspersky Endpoint Security для Windows 11.6.0, 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.

Откат вредоносных действий

- Программа восстанавливает файлы только на устройствах с файловой системой NTFS и FAT32.
- Программа 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*.
- Программа не контролирует изменения файлов, выполненные процессами на уровне ядра операционной системы.
- Программа не контролирует изменения файлов, выполненные через сетевой интерфейс (например, файл размещен в папке общего доступа и процесс запущен удаленно с другого компьютера).

Сетевой экран

- 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 программ для TCP и UDP и пакетных правилах.
  - По локальному адресу для входящих пакетов или соединений (кроме UDP) в запрещающих правилах программ 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.
- В программах версий 11.0.0 и 11.0.1 применение заданных MAC-адресов работает некорректно. Настройки MAC-адресов для версий 11.0.0 / 11.0.1 и 11.1.0 и выше несовместимы. После обновления программы или плагина с этих версий до версий 11.1.0 и выше необходимо проверить и перенастроить заданные MAC-адреса в правилах Сетевого экрана.
- При обновлении программы с версии 11.1.1 и 11.2.0 на 11.6.0 не мигрируют состояния разрешений (Permission) для следующих правил Сетевого экрана:
  - Запросы к серверу DNS по протоколу TCP.
  - Запросы к серверу DNS по протоколу UDP.
  - Любая сетевая активность.
  - Входящие ответы ICMP Destination Unreachable.
  - Входящая активность по протоколу ICMP.
- Если для разрешающего пакетного правила вы настроили сетевой адаптер или время жизни пакета (TTL), приоритет такого правила ниже запрещающего правила программ. То есть, если программе запрещена сетевая активность (например, программа 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 программ.
- В Kaspersky Endpoint Security для Windows 11.5.0 - 11.6.0 может произойти сбой при импорте списка пакетных правил Сетевого экрана. В результате из правила могут быть удалены удаленные и локальные адреса, заданные пользователем. Чтобы исправить ошибку, обратитесь в Службу технической поддержки. Служба технической поддержки предоставит вам обновление плагина с исправлением. Или вы можете обновить программу до следующей версии после релиза.
- При импорте списка пакетных правил Сетевого экрана Kaspersky Endpoint Security может изменять названия правил. Программа 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, программа 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.
- В Kaspersky Endpoint Security версии 11.6.0 и ниже при срабатывании сетевого пакетного правила в отчете Сетевого экрана в графе **Имя программы** всегда отображается значение *Kaspersky Endpoint Security*. При этом Сетевой экран блокирует соединение на пакетном уровне для всех программ. 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 программы** остается пустым.

Контроль программ

- При работе на операционный системе Microsoft Windows 10 в режиме списка запрещенных программ возможно некорректное применение правил блокировки, в результате которого будет заблокирован запуск программ, которые не указаны в правилах.
- При блокировании компонентом Контроль программ PWA-приложений (Progressive Web App) в отчете в качестве заблокированного приложения указывается appManifest.xml.

Контроль устройств

- 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.
- 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.

Веб-Контроль

- Не поддерживаются форматы OGV и WEBM.
- Не поддерживается протокол RTMP.

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 Adaptive Anomalies Control Rules report, 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.

Шифрование диска (FDE)

- Для работы шифрования жестких дисков перезагрузите операционную систему после установки программы.
- 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 программа предоставила к этим устройствам доступ, она 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 опции **Быстрый запуск** 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 установленной программой 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.
- Особенности восстановления операционной системы из резервной копии на зашифрованное GPT-устройство см. в базе знаний Службы технической поддержки.
- Не поддерживается совместное существование нескольких загрузочных агентов на одном зашифрованном компьютере.

- 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 `<домен>/<имя учетной записи Windows>`, 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.

Шифрования файлов (FLE)

- Не поддерживается шифрование файлов и папок в операционных системах семейства Microsoft Windows Embedded.
- Для шифрования файлов и папок требуется перезагрузка операционной системы после установки программы.
- 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 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.
- 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 установлена программа 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 программа несовместима 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.
- 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). 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. Подробнее о поддержке Client-Side Caching (CSC) при использовании шифрования см. в базе знаний Службы технической поддержки.
- 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 шифровании съемных дисков с поддержкой портативного режима не поддерживается отмена срока действия пароля.
- При совместной работе по сети под правилами шифрования FLE через программы, использующие метод отображения файла в память, например WordPad или FAR, и программы, 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.
- Файловое шифрование в папках синхронизации OneDrive не поддерживается. Добавление папок с уже зашифрованными файлами в список синхронизации OneDrive может привести к потере данных в зашифрованных файлах.
- 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.

- После обновления приложения Kaspersky Endpoint Security для Windows версии 11.0.1 и ниже для доступа к зашифрованным файлам после перезагрузки компьютера нужно убедиться, что Агент администрирования запущен. Агент администрирования имеет отложенный запуск, поэтому получить доступ к зашифрованным файлам сразу после загрузки операционной системы невозможно. После следующей перезагрузки компьютера ждать запуска Агента администрирования не нужно.

Другие ограничения

- В серверных операционных системах не выводится предупреждение о необходимости лечения активного заражения.
- Возможна некорректная обработка веб-адресов, которые добавлены в доверенный список.
- 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, программа блокирует это соединение для предотвращения загрузки вредоносных файлов из интернета.
- Kaspersky Endpoint Security не поддерживает стандарт RFC9218 для протокола HTTP/2. Если Kaspersky Endpoint Security обнаруживает такой формат обмена данными в трафике, приложение блокирует это соединение, а браузер показывает ошибку ERR_HTTP2_PROTOCOL_ERROR. Если вам нужно получить доступ к этому веб-ресурсу, вы можете исключить веб-ресурс из проверки защищенных соединений, или вы можете обратиться в Службу технической поддержки для получения патча.
- Мониторинг системы. Не отображается полная информация о процессах.
- При первом запуске Kaspersky Endpoint Security для Windows возможно временное попадание в некорректную группу программы, которая подписана цифровой подписью. В дальнейшем группа для программы, которая подписана цифровой подписью, будет автоматически изменена на корректную.
- При проверке почты с помощью расширения Защиты от почтовых угроз для Microsoft Outlook мы рекомендуем использовать режим кеширования сервера Exchange (опция Use Cached Exchange Mode).
- Задача *Антивирусная проверка* не поддерживает работу с 64-битной версией Microsoft Outlook. То есть, Kaspersky Endpoint Security не проверяет файлы, связанные с работой почтового клиента Outlook x64 (PST- и OST-файлы), даже если почта включена в область проверки.
- При переключении в Kaspersky Security Center 10 программы с использования глобального Kaspersky Security Network на использование локального Kaspersky Security Network 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 подтвердить согласие на участие. Ознакомиться с текстом Положения вы можете в интерфейсе программы или при редактировании продуктовой политики.
- При повторном сканировании вредоносного объекта, который заблокирован сторонним программным обеспечением, пользователь не информируется о повторном обнаружении угрозы. Событие о повторном обнаружении угрозы отображается в продуктовом отчете и отчете в Kaspersky Security Center 10.
- Установка компонента Endpoint Sensor не поддерживается на операционной системе Microsoft Windows Server 2008.
- В отчет Kaspersky Security Center 10 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.
- 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.
- Программа 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 программы в режиме Safe Mode.
- Для корректной работы Kaspersky Endpoint Security для Windows версии 11.5.0 и 11.6.0 с программным обеспечением Cisco AnyConnect необходимо установить модуль соответствия (англ. Compliance Module) версии 4.3.183.2048 или выше. Подробнее о совместимости Cisco Identity Services Engine см. в документации Cisco.
- Мы не гарантируем работу контроля аудио до первой перезагрузки после установки программы.
- 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.
- Задача проверки доступности KSN больше не поддерживается.
- Отключение опции Disable external management of the system services не будет позволять остановить службу программы, 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\.
- При обновлении программы с версии 11.1.0 на 11.6.0 настройки AMSI-защиты будут сброшены на значения по умолчанию.
- Если вы используете политики ограниченного использования программ (англ. SRP – Software Restriction Policies), возможен сбой при загрузке компьютера (черный экран). Мы рекомендуем

изменить параметры SRP: для параметра **Применять политики ограниченного использования программ к следующим объектам** установите значение **Ко всем файлам программ, кроме библиотек (таких как DLL)** и добавьте правила с уровнем безопасности **Неограниченный** для путей с файлами программы (`C:\Program Files\Common Files\Kaspersky Lab` и `C:\Program Files\Kaspersky Lab`). Подробнее об использовании SRP см. в *документации Microsoft*.

- 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 программы 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 программы.
- В локальном интерфейсе программы 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.
- 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, программа блокирует это соединение для предотвращения загрузки вредоносных файлов из интернета.
- При проверке зашифрованного соединения Kaspersky Endpoint Security принудительно использует протокол HTTP/1.
- 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).

Глоссарий

OLE-объект

Файл, присоединенный или встроенный в другой файл. Программы "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.

Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и программами "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех программ "Лаборатории Касперского", работающих в операционной системе Windows. Для программ, 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 программы.

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 программы "Лаборатории Касперского".

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами "Лаборатории Касперского" как фишинговые. База регулярно обновляется и входит в поставку программы "Лаборатории Касперского".

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ 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.

Дополнительный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

Задача

Функции, выполняемые программой "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.

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 программой "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 папке `Folder` и вложенных папках. 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

Программа, 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.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Приложение 1. Параметры программы

Вы можете настроить параметры Kaspersky Endpoint Security с помощью политики, задач или интерфейса программы. Подробная информация о компонентах программы 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. 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 программа. При обнаружении вредоносного файла Kaspersky Endpoint Security блокирует операцию с файлом. Далее программа 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 Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в программе, 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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
Область защиты	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 программ "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 Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет. **Лечить; блокировать, 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. **Блокировать**. Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически блокирует зараженные файлы без попытки их вылечить.

	Перед лечением или удалением зараженного файла Kaspersky Endpoint Security 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 форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов сторонних программ.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
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 состояния флажка.
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.
Режим проверки *(доступен только в Консоли администрирования (MMC) и интерфейсе Kaspersky Endpoint Security)*	Kaspersky Endpoint Security проверяет файлы, к которыми работает пользователь, операционная система или программа 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 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.
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 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 программе 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 программами.

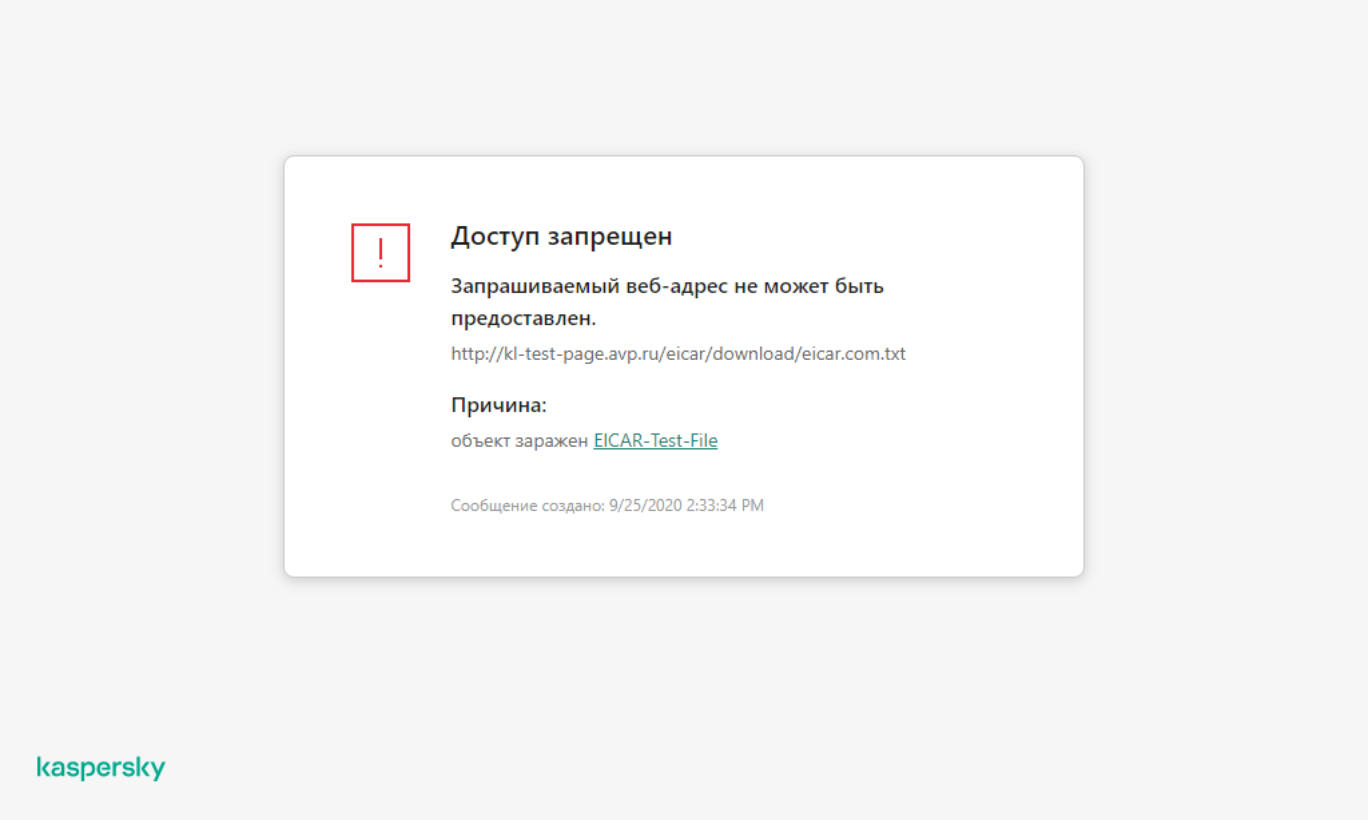
Защита от веб-угроз

Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует вредоносные и фишинговые веб-сайты. 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. Вы можете задать порты, которые Kaspersky Endpoint Security будет контролировать, или выбрать все порты.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений.

При попытке пользователя открыть вредоносный или фишинговый веб-сайт, Kaspersky Endpoint Security заблокирует доступ и покажет предупреждение (см. рис. ниже).



Сообщение о запрете доступа к веб-сайту

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 Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в программе, 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 программы, а также выполняет максимально глубокий эвристический анализ. • **Рекомендуемый**. Уровень безопасности веб-трафика, обеспечивающий оптимальный баланс между производительностью Kaspersky Endpoint Security и безопасностью веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на уровне **Средний**. 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 уровне **Поверхностный**.
Действие при обнаружении угрозы	**Запрещать загрузку**. 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 программы и пополняется при обновлении баз 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 программ "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 программ, 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.
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 программы и пополняется при обновлении баз 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.

Защита от почтовых угроз

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других программ, представляющих угрозу. Также компонент проверяет сообщения на наличие вредоносных и фишинговых ссылок. По умолчанию компонент Защита от почтовых угроз постоянно находится в оперативной памяти компьютера и проверяет все сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, NNTP или в почтовом клиенте Microsoft Office Outlook (MAPI). Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Компонент Защита от почтовых угроз не проверяет сообщения, если почтовый клиент открыт в браузере.

При обнаружении вредоносного файла во вложении Kaspersky Endpoint Security меняет тему сообщения: `[Сообщение заражено] <тема сообщения>` или `[Зараженный объект удален] <тема сообщения>`.

Компонент взаимодействует с почтовыми клиентами, установленными на компьютере. Для почтового клиента Microsoft Office Outlook предусмотрено расширение с дополнительными параметрами. Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft Office Outlook во время установки Kaspersky Endpoint Security.

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 Kaspersky Endpoint Security применяет разные наборы параметров. Наборы параметров, сохраненные в программе, 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. Уровень безопасности почты **Высокий** 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 Kaspersky Endpoint Security 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. Уровень безопасности почты **Низкий** 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 Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Endpoint Security удаляет зараженный объект. Kaspersky Endpoint Security добавит информацию о выполненном действии в тему сообщения: `[Зараженный объект удален] <тема сообщения>`.

	Лечить; блокировать, если лечение невозможно. При обнаружении зараженного объекта во входящем сообщении Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Endpoint Security добавит предупреждение к теме сообщения: `[Сообщение заражено] <тема сообщения>`. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Если вылечить объект не удалось, Kaspersky Endpoint Security блокирует отправку сообщения, почтовый клиент показывает ошибку. **Блокировать**. При обнаружении зараженного объекта во входящем сообщении Kaspersky Endpoint Security добавит предупреждение к теме сообщения: `[Сообщение заражено] <тема сообщения>`. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении Kaspersky Endpoint Security 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	Флажок включает / выключает проверку 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 программ "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 вложенные архивы	Проверка архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.

	Если во время проверки приложение Kaspersky Endpoint Security 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 офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
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.
Не проверять архивы более N сек	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 (англ. IDS – Intrusion Detection System) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Endpoint Security блокирует сетевое соединение с атакующим компьютером.

Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах Kaspersky Endpoint Security. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей программы.

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 флажок установлен, Kaspersky Endpoint Security контролирует сетевой трафик на наличие этих атак. При обнаружении атаки программа фильтрует и блокирует трафик, который связан с атакой. Таким образом, если на компьютер совершена атака типа Интенсивные сетевые запросы, программа снижает нагрузку на атакуемый ресурс. Если на компьютер совершена атака типа Сканирование портов, Kaspersky Endpoint Security предотвращает утечку данных о компьютере. Вы можете выключить обнаружение этих типов атак, так как некоторые разрешенные программы выполняют действия, характерные для таких атак. Таким образом, вы можете избежать ложных срабатываний.
Добавить атакующий компьютер в список блокирования на N минут	Если флажок установлен, то 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. Вы можете посмотреть список блокирования в окне инструмента Мониторинг сети. Kaspersky Endpoint Security очищает список блокирования при перезапуске программы и при изменении параметров Защиты от сетевых угроз.
Исключения	Список содержит IP-адреса, сетевые атаки с которых компонент Защита от сетевых угроз не блокирует. Kaspersky Endpoint Security 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 программ 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 программа использует Агент администрирования. При этом Сетевой экран автоматически создает сетевые правила, необходимые для работы Агента администрирования и программы. 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 программы. 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 программ*. Используются для ограничения сетевой активности конкретной программы. Учитываются не только характеристики сетевого пакета, но и конкретная программа, которой адресован этот сетевой пакет, либо которая инициировала отправку этого сетевого пакета.

Контроль доступа программ к ресурсам операционной системы, процессам и персональным данным обеспечивает компонент Предотвращение вторжений с помощью *прав программ*.

Во время первого запуска программы Сетевой экран выполняет следующие действия:

1. Проверяет безопасность программы с помощью загруженных антивирусных баз.

2. Проверяет безопасность программы в Kaspersky Security Network.

   Для более эффективной работы Сетевого экрана вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает программу в одну из *групп доверия*: Доверенные, Слабые ограничения, Сильные ограничения, Недоверенные.

   Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля активности программ. Kaspersky Endpoint Security помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

   Kaspersky Endpoint Security помещает программу 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 программу в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации программы от KSN группа доверия может быть изменена автоматически.

4. Блокирует сетевую активность программы в зависимости от группы доверия. Например, программам из группы доверия "Сильные ограничения" запрещены любые сетевые соединения.

При следующем запуске программы Kaspersky Endpoint Security проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие сетевые правила. Если программа была изменена, Kaspersky Endpoint Security исследует программу 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 программ. Если для одного и того же вида сетевой активности заданы и сетевые пакетные правила, и сетевые правила программ, то эта сетевая активность обрабатывается по сетевым пакетным правилам.

Сетевые правила программ имеют особенность. Сетевые правило программ включает в себя правила доступа по статусу сети: *публичная*, *локальная*, *доверенная*. Например, для группы доверия "Сильные ограничения" по умолчанию запрещена любая сетевая активность программы в сетях всех статусов. Если для отдельной программы (родительская программа) задано сетевое правило, то дочерние процессы других программ будут выполнены в соответствии с сетевым правилом родительской программы. Если сетевое правило для программы отсутствует, дочерние процессы будут выполнены в соответствии с правилом доступа к сетям группы доверия.

Например, вы запретили любую сетевую активность всех программ для сетей всех статусов, кроме браузера X. Если в браузере X (родительская программа) 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.

Статусы сетевых соединений

Сетевой экран позволяет контролировать сетевую активность в зависимости от статуса сетевого соединения. Kaspersky Endpoint Security получает статус сетевого соединения от операционной системы компьютера. Статус сетевого соединения в операционной системе задает пользователь при настройке подключения. Вы можете изменить статус сетевого соединения в параметрах Kaspersky Endpoint Security. Сетевой экран будет контролировать сетевую активность в зависимости от статуса сети в параметрах Kaspersky Endpoint Security, а не операционной системы.

Выделены следующие статусы сетевого соединения:

- **Публичная сеть**. Сеть не защищена антивирусными программами, 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 каждой программы в соответствии с сетевыми правилами этой программы.

  Сетевой экран по умолчанию присваивает статус *Публичная сеть* сети Интернет. Вы не можете изменить статус 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.

Параметр	Описание
Сетевые пакетные правила	Таблица сетевых пакетных правил. Сетевые пакетные правила используются для ввода ограничений на сетевые пакеты независимо от программы. 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 программ.
Сетевые соединения	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.
Сетевые правила	**Приложения** Таблица программ, работу которых контролирует компонент Сетевой экран. Программы распределены по группам доверия. Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля сетевой активности программ. Вы можете выбрать программу из единого списка всех программ, установленных на компьютерах под действием политики, и добавить программу в группу доверия. **Сетевые правила** Таблица сетевых правил программ, входящих в группу доверия. В соответствии с этими правилами Сетевой экран регулирует сетевую активность для программ. 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 вредоносную программу.

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, программа предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) цифровой код, сформированный программой (см. рис. ниже). Эта процедура называется авторизацией клавиатуры.

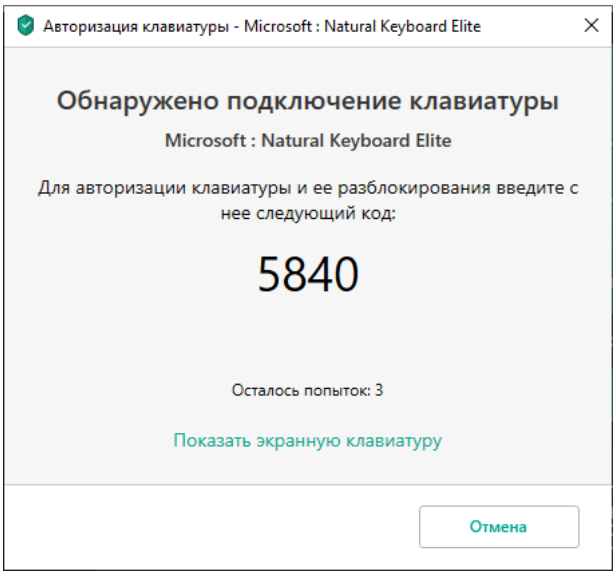
Если код введен правильно, программа сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется.

При подключении авторизованной клавиатуры через другой USB-порт компьютера программа снова запрашивает ее авторизацию.

Если цифровой код введен неправильно, программа формирует новый. Число попыток для ввода цифрового кода равно трем. Если цифровой код введен неправильно трижды или закрыто окно **Авторизация клавиатуры <Название клавиатуры>**, программа блокирует ввод с этой клавиатуры. При повторном подключении клавиатуры или перезагрузке операционной системы программа снова предлагает пройти авторизацию клавиатуры.

Программа разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.

Компонент Защита от атак BadUSB не устанавливается по умолчанию. Если вам нужен компонент Защита от атак BadUSB, вы можете добавить компонент в свойствах инсталляционного пакета перед установкой программы или измените состав компонентов программы после установки программы.



Авторизация клавиатуры

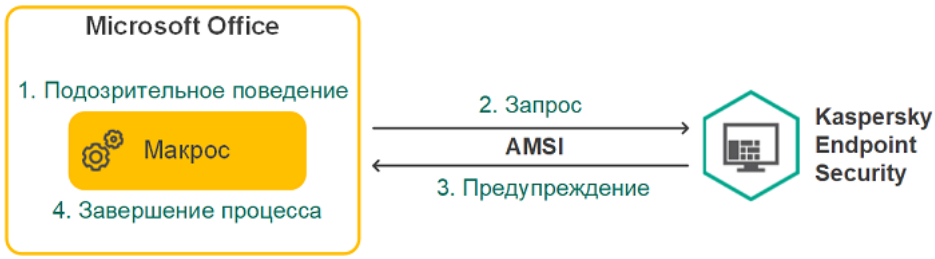
Параметры компонента Защита от атак BadUSB

Параметр	Описание
Запретить использование экранной клавиатуры для авторизации USB-устройств	Если флажок установлен, программа запрещает использование экранной клавиатуры для авторизации USB-устройства, с которого невозможно ввести код авторизации.

AMSI-защиты

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, программы 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 установлен флажок **Не блокировать взаимодействие с AMSI-защитой**.

AMSI-защита доступна для следующих операционных систем рабочих станций и серверов:

- Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

Параметры компонента Поставщик AMSI-защиты

Параметр	Описание
Проверять архивы	Проверка архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов сторонних программ.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
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 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 уязвимую программу. При обработке этих данных уязвимая программа выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО.

Если попытка запустить исполняемый файл из уязвимой программы не была произведена пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла или информирует пользователя.

Параметры компонента Защита от эксплойтов

Параметр	Описание
При обнаружении эксплойта	• **Блокировать операцию**. Если выбран этот вариант, то, обнаружив эксплойт, Kaspersky Endpoint Security блокирует действия этого эксплойта. • **Информировать**. Если выбран этот вариант, то в случае обнаружения эксплойта Kaspersky Endpoint Security не блокирует действия эксплойта 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 программ на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы.

Компонент Анализ поведения использует шаблоны опасного поведения программ. Если активность программы 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.

Параметры компонента Анализ поведения

Параметр	Описание
При обнаружении вредоносной активности программы	• **Удалять файл**. Если выбран этот вариант, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security удаляет исполняемый файл вредоносной программы и создает резервную копию файла в резервном хранилище. • **Завершать работу программы**. Если выбран этот вариант, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security завершает работу этой программы. • **Информировать**. Если выбран этот вариант, то в случае обнаружения вредоносной активности программы, Kaspersky Endpoint Security не завершает работу этой программы и добавляет информацию о вредоносной активности этой программы в список активных угроз.
Включить	Если переключатель включен, то Kaspersky Endpoint Security анализирует

защиту папок общего доступа от внешнего шифрования	активность в папках общего доступа. Если активность совпадает с одним из шаблонов опасного 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. • **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. • **Блокировать соединение**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security блокирует сетевую активность компьютера, осуществляющего изменение, и создает резервные копии измененных файлов. Если включен компонент Откат вредоносных действий и выбран вариант **Блокировать соединение**, то выполняется восстановление измененных файлов из резервных копий.
Блокировать соединение на N минут	Время, на которое Kaspersky Endpoint Security блокирует сетевую активность удаленного компьютера, осуществляющего шифрование папок общего доступа.
Исключения	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*).

Предотвращение вторжений

Компонент Предотвращение вторжений (англ. HIPS – Host Intrusion Prevention System) предотвращает выполнение программами 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 программ с помощью *прав программ*. Права программ включают в себя следующие параметры доступа:

- доступ к ресурсам операционной системы (например, параметры автозапуска, ключи реестра);
- доступ к персональным данным (например, к файлам, программам).

Сетевую активность программ контролирует Сетевой экран с помощью *сетевых правил*.

Во время первого запуска программы компонент Предотвращение вторжений выполняет следующие действия:

1. Проверяет безопасность программы с помощью загруженных антивирусных баз.
2. Проверяет безопасность программы в Kaspersky Security Network.

   Для более эффективной работы компонента Предотвращение вторжений вам рекомендуется принять участие в Kaspersky Security Network.

3. Помещает программу в одну из *групп доверия*: Доверенные, Слабые ограничения, Сильные ограничения, Недоверенные.

   Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля активности программ. Kaspersky Endpoint Security помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

   Kaspersky Endpoint Security помещает программу 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 программу в группу доверия в зависимости от параметров компонента Предотвращение вторжений. После получения данных о репутации программы от KSN группа доверия может быть изменена автоматически.

4. Блокирует действия программы в зависимости от группы доверия. Например, программам из группы доверия "Сильные ограничения" запрещен доступ к модулям операционной системы.

При следующем запуске программы Kaspersky Endpoint Security проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие права программ. Если программа была изменена, Kaspersky Endpoint Security исследует программу как при первом запуске.

Параметры компонента Предотвращение вторжений

Параметр	Описание
Права программ	**Программы** Таблица программ, работу которых контролирует компонент Предотвращение вторжений. Программы распределены по группам доверия. Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля активности программ. Вы можете выбрать программу из единого списка всех программ, установленных на компьютерах под действием политики, и добавить программу в группу доверия. Права доступа программы приведены в следующих таблицах: • **Файлы и системный реестр**. Таблица, которая содержит права доступа программ, входящих в группу доверия, к ресурсам операционной системы и персональным данным.

	• **Права**. Таблица, которая содержит права доступа программ, входящих в группу доверия, к процессам и ресурсам операционной системы. • **Сетевые правила**. Таблица сетевых правил программ, входящих в группу доверия. В соответствии с этими правилами Сетевой экран регулирует сетевую активность для программ. 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	**Имя** Таблица содержит ресурсы компьютера, распределенные по категориям. Компонент Предотвращение вторжений контролирует доступ других программ к ресурсам из этой таблицы. Ресурсом может быть категория реестра, файл или папка, ключ реестра. **Программы** Таблица программ, работу которых контролирует компонент Предотвращение вторжений, для выбранного ресурса. Программы распределены по группам доверия. Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля активности программ.
Группа доверия для программ, запущенных до начала работы Kaspersky Endpoint Security	Группа доверия, в которую Kaspersky Endpoint Security будет помещать программы, запускаемые до Kaspersky Endpoint Security.
Обновлять права для ранее неизвестных программ из базы KSN	Если флажок установлен, то компонент Предотвращение вторжений обновляет права ранее неизвестных программ, используя базы Kaspersky Security Network.
Доверять программам, имеющим цифровую подпись	Если флажок установлен, то компонент Предотвращение вторжений помещает программы 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 программы доверенными и распределяет их по группам доверия на основании других параметров.
Удалять права для программ, не запускавшихся более N дней	Если флажок установлен, то Kaspersky Endpoint Security автоматически удаляет информацию о программе (группа доверия, права доступа) при выполнении следующих условий: • Вы вручную поместили программу в группу доверия или настроили права доступа. • Программа не запускалась в течении заданного периода времени.

	Если группа доверия и права программы определены автоматически, Kaspersky Endpoint Security удаляет информацию об этой программе через 30 дней. Изменить время хранения информации о программе или выключить автоматическое удаление невозможно. При следующем запуске этой программы Kaspersky Endpoint Security исследует программу как при первом запуске.
Группа доверия для программ, которые не удалось распределить по другим группам	Раскрывающийся список, элементы которого определяют, в какую группу доверия Kaspersky Endpoint Security будет помещать неизвестную программу. Вы можете выбрать один из следующих элементов: • **Слабые ограничения**. • **Сильные ограничения**. • **Недоверенные**.

Откат вредоносных действий

Компонент Откат вредоносных действий позволяет Kaspersky Endpoint Security выполнить откат действий, произведенных вредоносными программами в операционной системе.

Во время отката действий вредоносной программы в операционной системе Kaspersky Endpoint Security обрабатывает следующие типы активности вредоносной программы:

- **Файловая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет исполняемые файлы, созданные вредоносной программой (на всех носителях, кроме сетевых дисков);
  - удаляет исполняемые файлы, созданные программами, в которые внедрилась вредоносная программа;
  - восстанавливает измененные или удаленные вредоносной программой файлы.

  Функциональность восстановления файлов имеет ряд ограничений.

- **Реестровая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет разделы и ключи реестра, созданные вредоносной программой;
  - не восстанавливает измененные или удаленные вредоносной программой разделы и ключи реестра.

- **Системная активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - завершает процессы, которые запускала вредоносная программа;
  - завершает процессы, в которые внедрялась вредоносная программа;

- не возобновляет процессы, которые остановила вредоносная программа.

- **Сетевая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - запрещает сетевую активность вредоносной программы;
  - запрещает сетевую активность тех процессов, в которые внедрялась вредоносная программа.

Откат действий вредоносной программы может быть запущен компонентом Защита от файловых угроз, Анализ поведения или при антивирусной проверке.

Откат действий вредоносной программы 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.

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, программа Kaspersky Endpoint Security получает от служб KSN сведения о категории и репутации проверяемых файлов, а также сведения о репутации проверяемых веб-адресов.

Использование Kaspersky Security Network является добровольным. Программа предлагает использовать KSN во время первоначальной настройки программы. 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 программы.

Для снижения нагрузки на серверы KSN специалисты "Лаборатории Касперского" могут выпускать обновления для программы, которые временно выключают или частично ограничивают обращения в Kaspersky Security Network. В этом случае статус подключения к KSN в локальном интерфейсе программы – *Включено с ограничениями*.

Инфраструктура KSN

Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения KSN:

- *Глобальный KSN* – это решение, которое используют большинство программ "Лаборатории Касперского". Участники KSN получают информацию от Kaspersky Security Network, 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 Security Network.

- *Локальный KSN* – это решение, позволяющее пользователям компьютеров, на которые установлена программа Kaspersky Endpoint Security или другие программы "Лаборатории Касперского", получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в KSN со своих компьютеров. Локальный KSN 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.

По умолчанию Kaspersky Security Center использует Глобальный KSN. Вы можете настроить использование Локального KSN в Консоли администрирования (MMC), Kaspersky Security Center 12 Web Console, а также с помощью командной строки. Настроить использование Локального KSN в Kaspersky Security Center Cloud Console невозможно.

Подробнее о работе Локального KSN см. в *документации для Kaspersky Private Security Network*.

KSN Proxy

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy.

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.

Подробную информацию о службе KSN Proxy см. в *справке Kaspersky Security Center*.

Параметры Kaspersky Security Network

Параметр	Описание
Включить расширенный режим KSN	*Расширенный режим KSN* – режим работы программы, 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 программы, при котором Kaspersky Endpoint Security использует облегченную версию антивирусных баз. Работу программы 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 KSN Proxy *(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 KSN при недоступности KSN Proxy *(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 на стороне "Лаборатории Касперского", в случае использования Глобального KSN, так и на сторонних серверах, в случае использования Локального KSN.

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).

Kaspersky Endpoint Security контролирует только HTTP- и HTTPS-трафик.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений.

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 программы). 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 программ" 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.

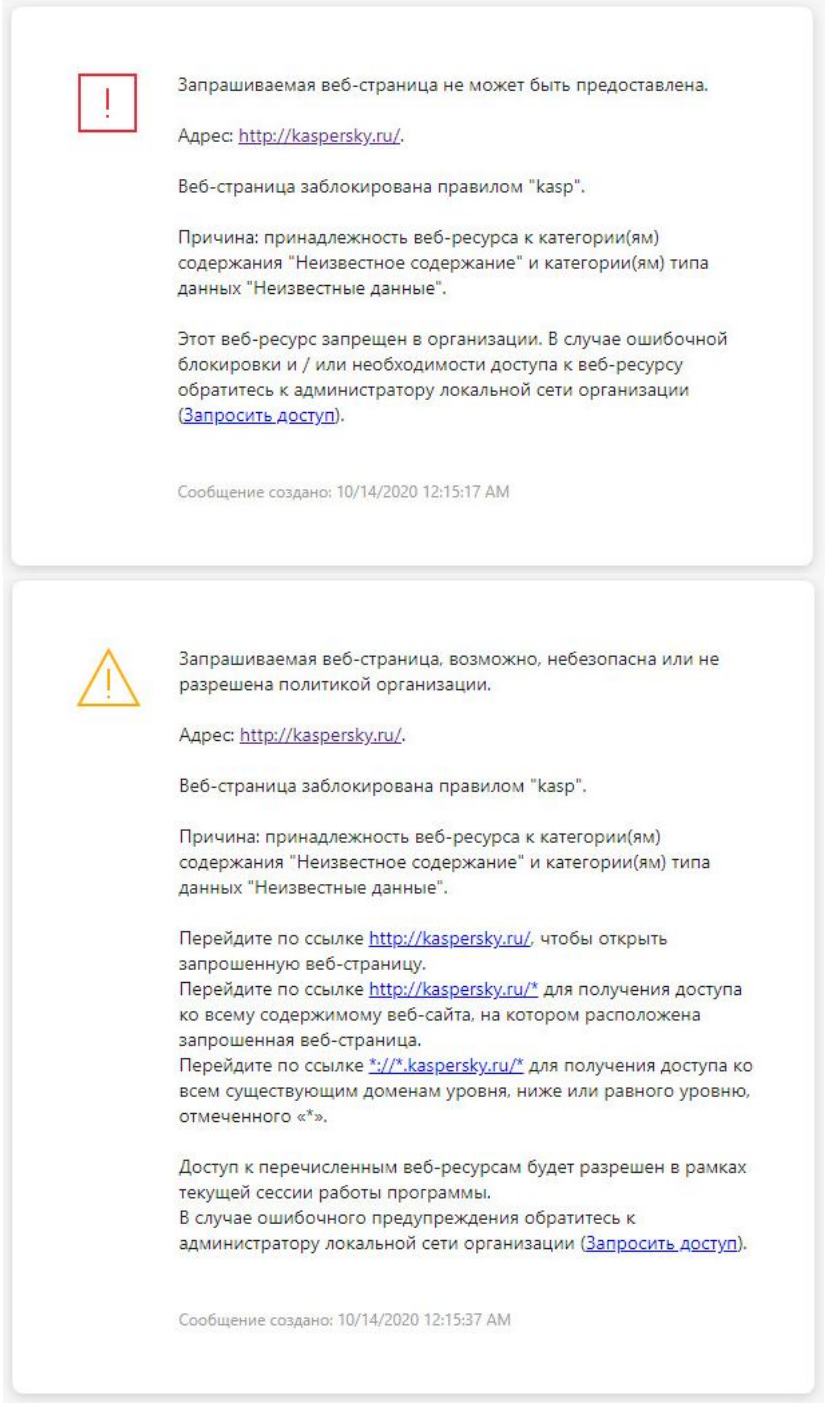
  Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

- 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

Параметры компонента Веб-Контроль

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.

Шаблоны сообщений	• **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**. Поле ввода содержит шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно.
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. Мониторинг активности пользователя в интернете может потребовать больше ресурсов компьютера при расшифровке HTTPS-трафика.

Контроль устройств

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

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.

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 –  .
  - 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). Таким образом, вы можете ограничить подключение всех устройств, 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.

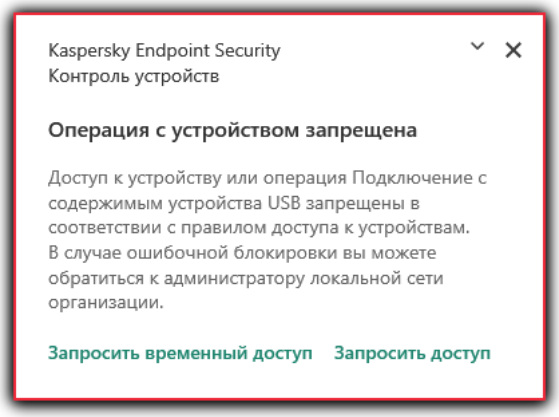
  Вы можете добавить доверенные устройства по следующим данным:

  - **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 программа Kaspersky Endpoint Security сохраняла события подключения / отключения устройства, разрешите доступ к соответствующему типу устройств (статус ✓) или добавьте устройство в список доверенных.

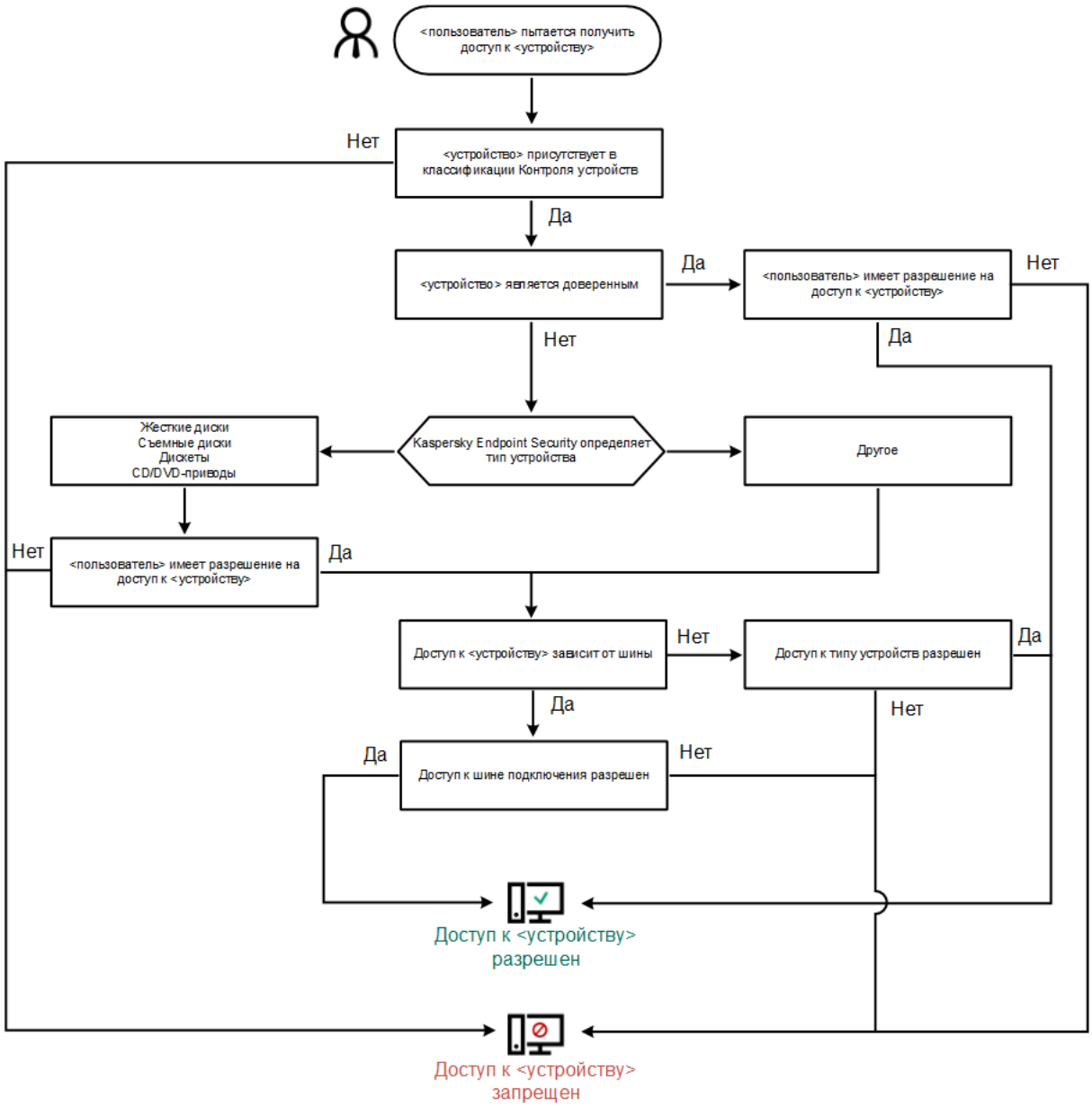
При подключении к компьютеру устройства, доступ к которому запрещен Контролем устройств, Kaspersky Endpoint Security заблокирует доступ и покажет уведомление (см. рис. ниже).



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 установленной программой Kaspersky Endpoint Security требуется запросить доступ к устройству, которое, по его мнению, было заблокировано ошибочно, передайте ему инструкцию по запросу доступа.

Параметры компонента Контроль устройств

Параметр	Описание
Разрешить запрашивать временный доступ *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, то кнопка **Запросить доступ** в локальном интерфейсе Kaspersky Endpoint Security доступна. При нажатии на эту кнопку открывается окно **Запрос доступа к устройству**. С помощью этого окна 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.
Доверенные устройства	Список доверенных устройств и пользователей, которым разрешен доступ к этим устройствам.
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.

Контроль программ

Контроль программ управляет запуском программ на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании программ. Также Контроль программ снижает риск заражения компьютера, ограничивая доступ к программам.

Настройка Контроля программ состоит из следующих этапов:

1. Создание категорий программ.

   Администратор создает категории программ, которыми администратор хочет управлять. Категории программ предназначены для всех компьютеров сети организации независимо от групп администрирования. Для создания категории вы можете использовать следующие критерии: KL-категория (например, *Браузеры*), хеш файла, производитель программы и другие.

2. Создание правил Контроля программ.

   Администратор создает правила Контроля программ в политике для группы администрирования. Правило включает в себя категории программ и статус запуска программ из этих категорий: запрещен или разрешен.

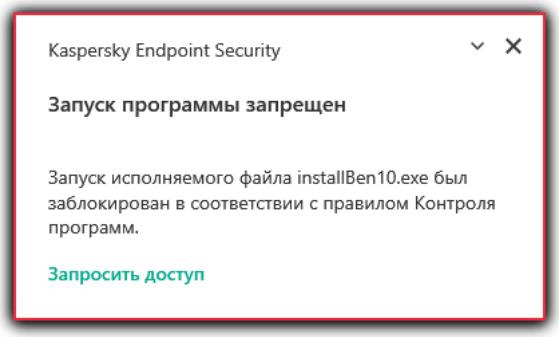
3. Выбор режима работы Контроля программ.

   Администратор выбирает режим работы с программами, которые не входят ни в одно из правил (списки запрещенных и разрешенных программ).

При попытке пользователя запустить запрещенную программу, Kaspersky Endpoint Security заблокирует запуск программы и покажет уведомление (см. рис. ниже).

Для проверки настройки Контроля программ предусмотрен *тестовый режим*. В этом режиме Kaspersky Endpoint Security выполняет следующие действия:

- разрешает запуск программ, в том числе запрещенных;
- показывает уведомление о запуске запрещенной программы и добавляет информацию в отчет на компьютере пользователя;
- отправляет данные о запуске запрещенных программ в Kaspersky Security Center.



Уведомление Контроля программ

Режимы работы Контроля программ

Компонент Контроль программ может работать в двух режимах:

- **Список запрещенных**. Режим, при котором Контроль программ разрешает пользователям запуск любых программ, кроме тех, которые запрещены в правилах Контроля программ.

  Этот режим работы Контроля программ установлен по умолчанию.

- **Список разрешенных**. Режим, при котором Контроль программ запрещает пользователям запуск любых программ, кроме тех, которые разрешены и не запрещены в правилах Контроля программ.

  Если разрешающие правила Контроля программ сформированы максимально полно, компонент запрещает запуск всех новых программ, не проверенных администратором локальной сети организации, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

  Вы можете ознакомиться с рекомендациями по настройке правил контроля программ в режиме списка разрешенных программ.

Настройка Контроля программ 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 программ.

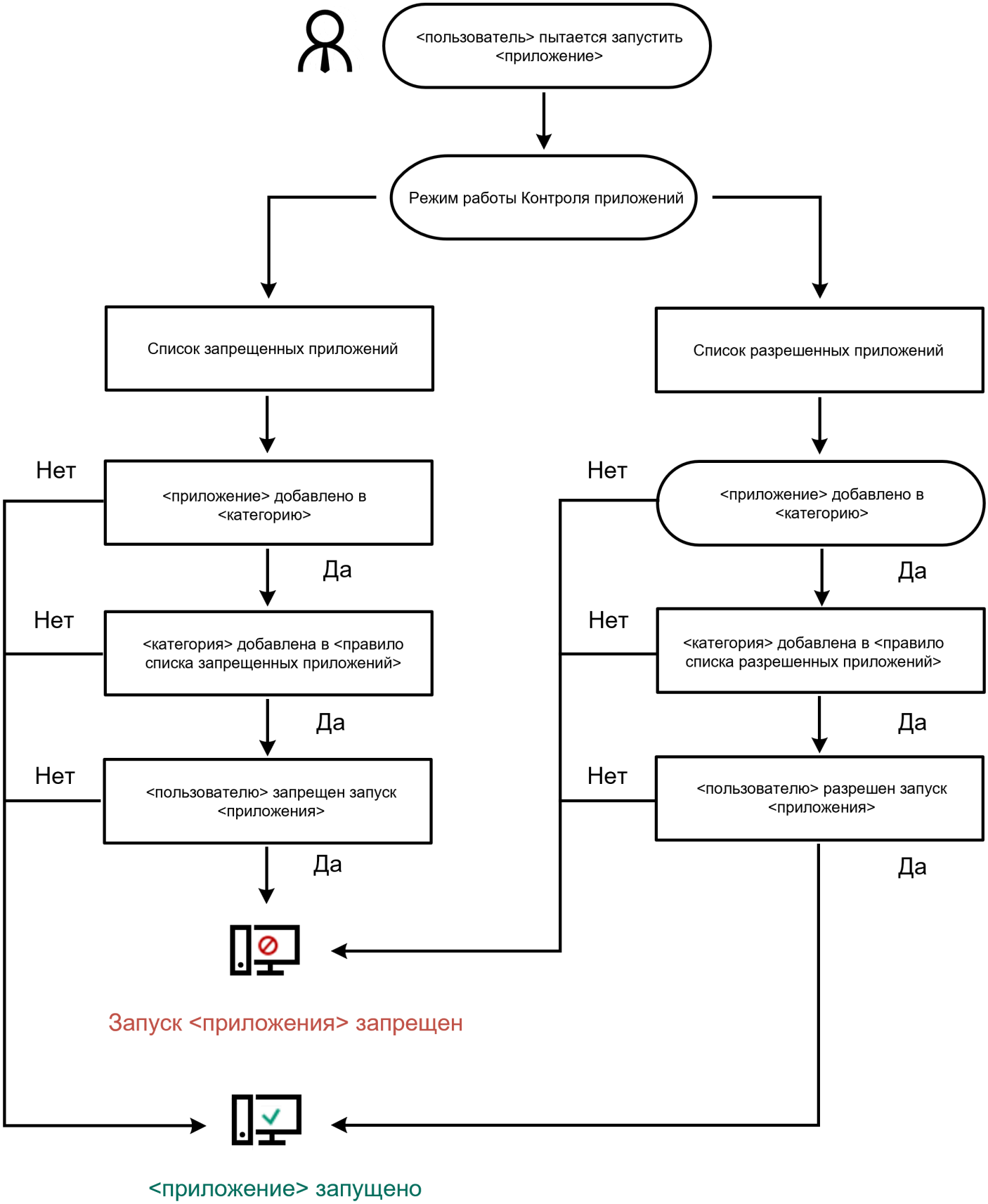
  Правила Контроля программ, сформированные в Консоли администрирования Kaspersky Security Center, основываются на созданных вами категориях программ, а не на включающих и исключающих условиях, как в локальном интерфейсе Kaspersky Endpoint Security.

- Получение информации о программах, которые установлены на компьютерах локальной сети организации.

Поэтому настройку работы компонента Контроль программ рекомендуется выполнять с помощью Kaspersky Security Center.

Алгоритм работы Контроля программ

Kaspersky Endpoint Security использует алгоритм для принятия решения о запуске программы (см. рис. ниже).



Алгоритм работы Контроля программ

Параметры компонента Контроль программ

Параметр	Описание
Тестовый режим	Если переключатель включен, Kaspersky Endpoint Security разрешает запуск программы, запрещенной в текущем режиме Контроля программ, но заносит информацию о ее запуске в отчет.

Режим контроля запуска программ	Вы можете выбрать один из следующих вариантов: • **Список запрещенных**. Если выбран этот вариант, Контроль программ разрешает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям запрещающих правил Контроля программ. • **Список разрешенных**. Если выбран этот вариант, Контроль программ запрещает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям разрешающих правил Контроля программ. При выборе режима **Список разрешенных** автоматически создается два правила Контроля программ: • **Программы ОС**. • **Доверенные программы обновления**. Изменение параметров и удаление автоматически созданных правил недоступно. Вы можете включить или выключить эти правила.
Контролировать загрузку DLL-модулей	Если флажок установлен, то Kaspersky Endpoint Security контролирует загрузку DLL-модулей при запуске пользователями программ. Информация о DLL-модуле и программе, загрузившей этот DLL-модуль, сохраняется в отчет. При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в параметрах Контроля программ включено правило по умолчанию **Программы ОС** или другое правило, которое содержит KL-категорию "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 **Программы 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 программа контролировала все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security.
Шаблоны сообщений	**Сообщение о блокировке**. Шаблон сообщения, которое появляется при срабатывании правила Контроля программ, блокирующего запуск программы. **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка программы, по мнению пользователя, произошла ошибочно.

Адаптивный контроль аномалий

Этот компонент доступен только для решений Kaspersky Endpoint Security для бизнеса Расширенный и Kaspersky Total Security для бизнеса. Подробнее о решениях Kaspersky Endpoint Security для бизнеса см. на *сайте "Лаборатории Касперского"*.

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена 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 офисной программы*). 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 программы. 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 **Срабатывание правил в обучающем режиме**.

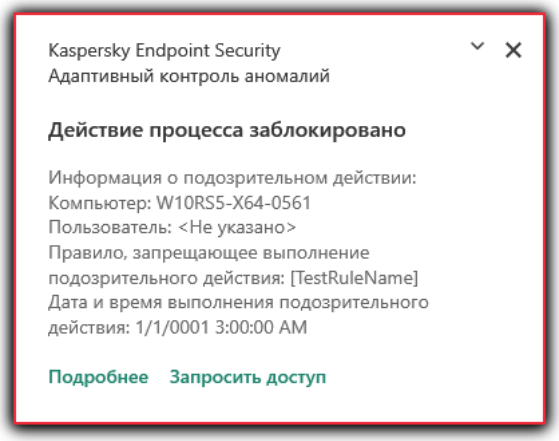
2. Анализ отчета о срабатывании правил.

   Администратор анализирует отчет о срабатываниях правил или содержание хранилища **Срабатывание правил в обучающем режиме**. Далее администратор может выбрать поведение Адаптивного контроля аномалий при срабатывании правила: блокировать или разрешить. Также администратор может продолжить отслеживать срабатывание правила и продлить работу программы в обучающем режиме. Если администратор не предпринимает никаких мер, программа также продолжит работать в обучающем режиме. Отсчет срока действия обучающего режима начинается заново.

Настройка Адаптивного контроля аномалий происходит в режиме реального времени. Настройка Адаптивного контроля аномалий 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 **Срабатывание правил в обучающем режиме**. Рекомендуется проверять отчет о срабатывании правил и содержимое хранилища **Срабатывание правил в обучающем режиме**.

При попытке вредоносной программы 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	В этом отчете содержится информация о статусе правил обнаружения

состоянии правил *(доступен только в консоли Kaspersky Security Center)*	Адаптивного контроля аномалий (например, статусы *Выключено* или *Блокировать*). Отчет формируется для всех групп администрирования.
Отчет о срабатываниях правил *(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.
Правила	Таблица правил Адаптивного контроля аномалий. Правила созданы специалистами "Лаборатории Касперского" на основе типичных сценариев потенциально 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.

Endpoint Sensor

В Kaspersky Endpoint Security 11.4.0 компонент Endpoint Sensor исключен из программы.

Вы можете управлять Endpoint Sensor в Kaspersky Security Center 12 Web Console и Консоли администрирования Kaspersky Security Center. Управлять Endpoint Sensor в программе 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. APT – Advanced Persistent Threat), атаки "нулевого дня" и другие. Kaspersky Anti Targeted Attack Platform включает в себя два функциональных блока: Kaspersky Anti Targeted Attack (далее также "*KATA*") и Kaspersky Endpoint Detection and Response (далее также "*KEDR*"). Вы можете приобрести KEDR отдельно. Подробнее о решении см. в *справке Kaspersky Anti Targeted Attack Platform*.

Управление Endpoint Sensor имеет следующие особенности:

- Если на компьютере установлена программа 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 установлена программа 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*.

Полнодисковое шифрование

Вы можете выбрать технологию шифрования: Шифрование диска Kaspersky или Шифрование диска BitLocker (далее также "BitLocker").

Шифрование диска Kaspersky

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 *Управления 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.

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 диска BitLocker создает мастер-ключ. Kaspersky Endpoint Security отправляет мастер-ключ 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 информацию о шифровании диска в Kaspersky Security Center. При этом Kaspersky Endpoint Security не отправит мастер-ключ в Kaspersky Security Center, и восстановить доступ к диску с помощью Kaspersky Security Center будет невозможно. Для корректной работы BitLocker с Kaspersky Security Center расшифруйте диск и зашифруйте диск повторно с помощью политики. Расшифровать диск вы можете локально или с помощью политики.

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).

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.

Параметры компонента Шифрование диска Kaspersky

Параметр	Описание
Режим шифрования	**Шифровать все жесткие диски**. Если выбран этот элемент, то при применении политики программа шифрует все жесткие диски.

	Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой установлена программа. **Расшифровывать все жесткие диски**. Если выбран этот элемент, то при применении политики программа расшифровывает все зашифрованные ранее жесткие диски. **Оставлять без изменений**. Если выбран этот элемент, то при применении политики программа 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, программа 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**. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security создает учетные записи Агента аутентификации для всех учетных записей компьютера, которые когда-либо были активными. **Все доменные учетные записи компьютера**. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security создает учетные записи Агента аутентификации для всех учетных записей компьютера, которые принадлежат какому-либо домену и которые когда-либо были активными. **Все локальные учетные записи компьютера**. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security создает учетные записи Агента аутентификации для всех локальных учетных записей компьютера, которые когда-либо были активными. **Локальный администратор**. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security создает учетную запись локального администратора. **Менеджер компьютера**. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security создает учетную запись Агента аутентификации для учетной записи, в свойствах которой в Active Directory указано, что она является управляющей. **Активная учетная запись**. Если флажок установлен, то при выполнении задачи полнодискового шифрования Kaspersky Endpoint Security автоматически создает учетную запись Агента аутентификации для активной в момент выполнения задачи учетной записи компьютера.
Автоматически создавать учетные записи Агента аутентификации для всех пользователей на компьютере при входе	Если флажок установлен, программа 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, программа 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 программа сохраняет имя учетной записи Агента аутентификации. При последующей аутентификации в Агенте аутентификации под той же учетной записью имя учетной записи вводить не требуется.
Шифровать только занятое пространство	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	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. Также вы можете включить использование технологии 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.
Справочные тексты	**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.

Параметры компонента Шифрование диска BitLocker

Параметр	Описание
Режим шифрования	**Шифровать все жесткие диски**. Если выбран этот элемент, то при применении политики программа шифрует все жесткие диски. Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой установлена программа. **Расшифровывать все жесткие диски**. Если выбран этот элемент, то при применении политики программа расшифровывает все зашифрованные ранее жесткие диски. **Оставлять без изменений**. Если выбран этот элемент, то при применении политики программа 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	Флажок включает / выключает 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	Если флажок установлен, то программа 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.
Настройки аутентификации	**Использовать 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). **Использовать 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.
  Вы можете разрешить пользователю использовать расширенный PIN-код. *Расширенный PIN-код* кроме цифр позволяет использовать другие символы: заглавные и строчные латинские буквы, специальные символы и пробел.

- **Использовать доверенный платформенный модуль (TPM), если он недоступен, то пароль**. Если флажок установлен, 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.

Шифрование файлов

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 программами. После применения политики программа 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 программами.

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена 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 программ. 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
Управление шифрованием	**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. **Шифровать 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 программ к зашифрованным файлам согласно правилам для программ. **Расшифровывать все**. Если выбран этот элемент, то Kaspersky Endpoint Security расшифровывает все зашифрованные файлы и папки.
Правила шифрования	На закладке отображаются правила шифрования файлов, хранящихся на локальных дисках. Вы можете добавить файлы следующим образом: • **Стандартные области**. 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 программ. Например, программы 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). • **Папки**. 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. Вы можете использовать набор `\..\` (например, `C:\Users\..\UserFolder\`). Набор `\..\` обозначает переход к родительской папке. 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.
Правила расшифровки	На закладке отображаются правила расшифровки файлов, хранящихся на локальных дисках.
Правила для программ	На закладке отображается таблица с правилами доступа программ к зашифрованным файлам и правилами шифрования файлов, создаваемых и

	изменяемых отдельными программами.
Настройки пароля для зашифрованных архивов	Параметры сложности пароля при создании зашифрованных архивов.

Шифрование съемных дисков

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена 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.

Параметры компонента Шифрование съемных дисков

Параметр	Описание
Управление шифрованием	**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.

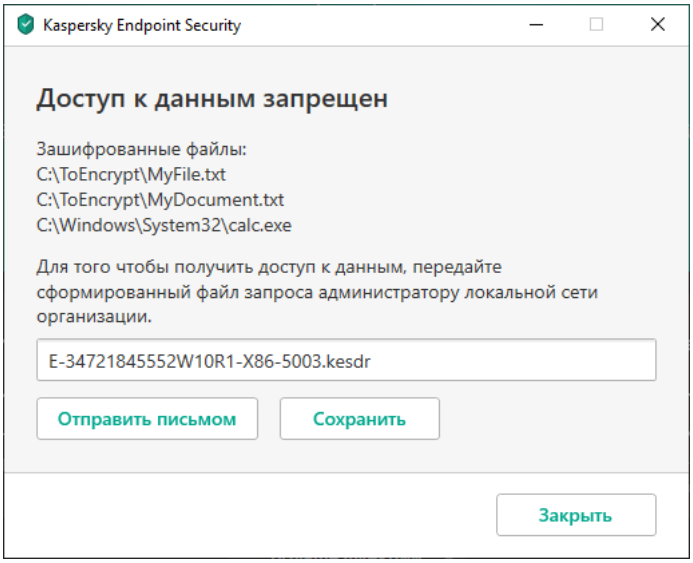
	Шифровать только новые файлы. Если выбран этот элемент, то при применении политики с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security шифрует на съемных дисках только те файлы, которые были добавлены или изменены после последнего применения политики Kaspersky Security Center. 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 установленной программой Kaspersky Endpoint Security и доступной функциональностью шифрования. Таким образом, доступ к личным файлам всегда открыт вне зависимости от того, установлена на компьютере программа 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 программа 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 шифрования выбранных устройств	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).

Разрешить 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 пароля для портативного режима	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**. 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 программ, 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 программ, установленных на компьютере. Включение объектов и программ в доверенную зону может потребоваться, например, если Kaspersky Endpoint Security блокирует доступ к какому-либо объекту или программе, в то время как вы уверены, что этот объект или программа 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 программ.

Исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Endpoint Security не проверяет объект на вирусы и другие программы, представляющие угрозу.

Исключения из проверки позволяют работать с легальными программами, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы злоумышленниками. Подробную информацию о легальных программах, 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 программы могут быть заблокированы. Чтобы избежать блокирования, для используемых программ 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 программу Radmin, предназначенную для удаленного управления компьютерами. Такая активность программы рассматривается Kaspersky Endpoint Security как подозрительная и может быть заблокирована. Чтобы исключить блокировку программы, нужно сформировать исключение из проверки, где указать название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского".

Если у вас на компьютере установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Endpoint Security может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из проверки, настроив Kaspersky Endpoint Security способом, описанным в этом документе.

Исключения из проверки могут использоваться в ходе работы следующих компонентов и задач программы, заданных администратором системы:

- Анализ поведения.

- Защита от эксплойтов.

- Предотвращение вторжений.

- Защита от файловых угроз.
- Защита от веб-угроз.
- Защита от почтовых угроз.
- Задачи проверки.

Список доверенных программ

Список доверенных программ – это список программ, у которых Kaspersky Endpoint Security не контролирует файловую и сетевую активность (в том числе и вредоносную), а также обращения этих программ к системному реестру. По умолчанию Kaspersky Endpoint Security проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и создаваемый ими сетевой трафик. Kaspersky Endpoint Security исключает из проверки программу, добавленную в список доверенных программ.

Например, если вы считаете объекты, используемые программой Microsoft Windows Блокнот, безопасными и не требующими проверки, то есть доверяете этой программе, вам следует добавить программу Microsoft Windows Блокнот в список доверенных программ, чтобы не проверять объекты, используемые этой программой.

Кроме того, некоторые действия, которые Kaspersky Endpoint Security классифицирует как подозрительные, могут быть безопасны в рамках функциональности ряда программ. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием программ автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких программ и отключить контроль их активности, рекомендуется добавить их в список доверенных программ.

Исключение доверенных программ из проверки позволяет избежать проблемы совместимости Kaspersky Endpoint Security с другими программами (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky Endpoint Security и другой антивирусной программой), а также увеличить производительность компьютера, что особенно важно при использовании серверных программ.

В то же время исполняемый файл и процесс доверенной программы по-прежнему проверяются на наличие в них вирусов и других программ, представляющих угрозу. Для полного исключения программы из проверки Kaspersky Endpoint Security следует пользоваться исключениями из проверки.

Параметры исключений

Параметр	Описание
Типы обнаруживаемых объектов	Вне зависимости от настроенных параметров программы Kaspersky Endpoint Security всегда обнаруживает и блокирует вирусы, черви и троянские программы. Эти программы могут нанести значительный вред компьютеру. • **Вирусы, черви**

Подкатегория: вирусы и черви (Viruses_and_Worms)

Степень угрозы: высокая

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	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 программы

Подкатегория: троянские программы (Trojan_programs)

Степень угрозы: высокая

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 программы

Подкатегория: рекламные программы (Adware)

Степень угрозы: средняя

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.

- Программы 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.
Dialer	Программы автодозвона	Могут устанавливать телефонные соединения через модем в скрытом режиме.
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.

- **Обнаруживать другие программы, 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.
Dialer	Программы автодозвона	Могут устанавливать телефонные соединения через модем в скрытом режиме.
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**

Kaspersky Endpoint Security проверяет упакованные объекты и модуль-распаковщик в составе самораспаковывающихся архивов SFX (self-extracting archive).

Чтобы скрыть опасные программы от обнаружения антивирусом, злоумышленники упаковывают их с помощью специальных упаковщиков или многократно упаковывают один объект.

Вирусные аналитики "Лаборатории Касперского" отобрали упаковщики, которые злоумышленники используют чаще всего.

Если Kaspersky Endpoint Security обнаружил в объекте такой упаковщик, то скорее всего он содержит вредоносную программу или программу, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.

Kaspersky Endpoint Security выделяет следующие программы:

- *Упакованные файлы, которые могут нанести вред* – используются для упаковки вредоносных программ: вирусов, червей, троянских программ.
- *Многократно упакованные файлы* (степень угрозы средняя) – объект упакован трижды одним или несколькими упаковщиками.

- **Множественно упакованные файлы**

Kaspersky Endpoint Security проверяет упакованные объекты и модуль-распаковщик в составе самораспаковывающихся архивов SFX (self-extracting archive).

Чтобы скрыть опасные программы от обнаружения антивирусом, злоумышленники упаковывают их с помощью специальных упаковщиков или многократно упаковывают один объект.

Вирусные аналитики "Лаборатории Касперского" отобрали упаковщики, которые злоумышленники используют чаще всего.

Если Kaspersky Endpoint Security обнаружил в объекте такой упаковщик, то скорее всего он содержит вредоносную программу или программу, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.

Kaspersky Endpoint Security выделяет следующие программы:

- *Упакованные файлы, которые могут нанести вред* – используются для упаковки вредоносных программ: вирусов, червей, троянских программ.
- *Многократно упакованные файлы* (степень угрозы средняя) – объект упакован трижды одним или несколькими упаковщиками.

Исключения

Таблица содержит информацию об исключениях из проверки.

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 папке `Folder` и вложенных папках. 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.
	• 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`.

Доверенные программы	Таблица доверенных программ, активность которых Kaspersky Endpoint Security не проверяет в процессе своей работы. Компонент Контроль программ регулирует запуск каждой из программ независимо от того, указана ли эта программа в таблице доверенных программ или нет.
Объединять значения при наследовании *(доступен только в консоли Kaspersky Security Center)*	Объединение списка исключений из проверки и списка доверенных программ 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 программ для всей организации. Удалить или изменить унаследованные элементы списка в дочерней политике невозможно. Элементы списка исключений из проверки и списка доверенных программ, 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.
Разрешить	*Локальные исключения и локальные доверенные программы (локальная*

использование локальных исключений / Разрешить использование локальных доверенных программ *(доступен только в консоли Kaspersky Security Center)*	*доверенная зона)* – список объектов и программ, сформированные пользователем в Kaspersky Endpoint Security для отдельного компьютера. Kaspersky Endpoint Security в процессе работы не контролирует объекты и программы из локальной доверенной зоны. Таким образом, кроме общей доверенной зоны, сформированной в политике, пользователь может создавать собственные локальные списки исключений и доверенных программ. Если флажок установлен, пользователь может сформировать локальный список исключений из проверки и локальный список доверенных программ. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списков в свойствах компьютера. Если флажок снят, пользователю доступны только общие списки исключений из проверки и доверенных программ, сформированные в политике. Если локальные списки сформированы, после выключения функции Kaspersky Endpoint Security продолжает исключать из проверки объекты из списков.
Доверенное системное хранилище сертификатов	Если выбрано одно из доверенных системных хранилище сертификатов, Kaspersky Endpoint Security исключает из проверки программы, подписанные доверенной цифровой подписью. Kaspersky Endpoint Security автоматически помещает такие программы в группу *Доверенные*. Если выбрано **Не использовать**, то Kaspersky Endpoint Security проверяет программы независимо от наличия цифровой подписи. Kaspersky Endpoint Security помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

Настройки программы

Вы можете настроить следующие общие параметры программы:

- режим работы;
- самозащита;
- производительность;
- отладочная информация;
- статус компьютера при применении параметров.

Параметры программы

Параметр	Описание
Запускать Kaspersky Endpoint Security при включении компьютера	Если флажок установлен, то Kaspersky Endpoint Security запускается после загрузки операционной системы и защищает компьютер пользователя в течение всего сеанса работы. Если флажок не установлен, то Kaspersky Endpoint Security не запускается после загрузки операционной системы до того момента, как пользователь запустит программу вручную. Защита компьютера выключена и данные пользователя могут находиться под угрозой.
Применять технологию лечения	Если флажок установлен, при обнаружении вредоносной активности в операционной системе на экране отображается всплывающее уведомление. В уведомлении Kaspersky Endpoint Security предлагает провести процедуру лечения активного заражения компьютера. После подтверждения пользователем этой

активного заражения	процедуры Kaspersky Endpoint Security устраняет угрозу. Завершив процедуру лечения активного заражения, Kaspersky Endpoint Security выполняет перезагрузку компьютера. Применение технологии лечения активного заражения требует значительных ресурсов компьютера, что может замедлить работу других программ. Если программа Kaspersky Endpoint Security установлена 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 программы и включить немедленное лечение активного заражения в свойствах задачи *Антивирусная проверка*. Далее вам нужно запустить задачу *Антивирусная проверка*.
Использовать Kaspersky Security Center в качестве прокси-сервера для активации *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, то при активации программы в качестве прокси-сервера используется Сервер администрирования Kaspersky Security Center.
Включить самозащиту	Если флажок установлен, то Kaspersky Endpoint Security предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти и записей в системном реестре.
Разрешить управление настройками Kaspersky Endpoint Security через программы удаленного управления	Если флажок установлен, доверенные программы удаленного администрирования (такие как TeamViewer, LogMeIn Pro и Remotely Anywhere) могут изменять настройки Kaspersky Endpoint Security. Недоверенным программам удаленного администрирования изменение настроек Kaspersky Endpoint Security будет запрещено, даже если флажок установлен.
Включить возможность внешнего управления системными службами	Если флажок установлен, то Kaspersky Endpoint Security разрешает управление службами программы с удаленного компьютера. При попытке управления службами программы с удаленного компьютера, над значком программы в области уведомлений панели задач Microsoft Windows отображается уведомление (если служба уведомлений не выключена пользователем).
Откладывать задачи по расписанию при работе от аккумулятора	Если флажок установлен, то режим экономии питания аккумулятора включен. Kaspersky Endpoint Security откладывает выполнение задач, для которых задан запуск по расписанию. По мере необходимости вы можете самостоятельно запускать задачи проверки и обновления.
Уступать	

ресурсы другим программам	Когда Kaspersky Endpoint Security выполняет задачи по расписанию, может увеличиваться нагрузка на центральный процессор и дисковые подсистемы, что замедляет работу других программ. Если флажок установлен, то при увеличении нагрузки Kaspersky Endpoint Security приостанавливает выполнение задач по расписанию и высвобождает ресурсы операционной системы для других программ.
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. Программа 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 установленной программой Kaspersky Endpoint Security в Web Console при появлении ошибок применения политики или выполнения задачи. Доступны статусы *OK*, *Предупреждение* и *Критический*.

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 программы в целом сохраняется в отчетах.

Отчеты хранятся в папке `C:\ProgramData\Kaspersky Lab\KES\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\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.

Параметры отчетов и хранения

Параметр	Описание
Хранить отчеты не более N дней	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 отчетов.
Ограничить размер файла отчетов до N 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 отчетов Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчетов таким образом, чтобы размер файла отчетов не превышал максимального значения.
Хранить объекты не более N дней	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 хранилища до N МБ	Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. По умолчанию максимальный размер составляет 100 МБ. После достижения максимального размера резервного хранилища Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения.
Передача данных на Сервер администрирования *(доступен только в Kaspersky Security Center)*	Категории событий на клиентских компьютерах, информация о которых должна передаваться на Сервер администрирования.

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, программа ограничивает собственный сетевой трафик в том случае, если подключение к интернету является лимитным. 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.
Прокси-сервер	Параметры прокси-сервера для доступа пользователей клиентских компьютеров в интернет. Kaspersky Endpoint Security использует эти параметры в работе некоторых компонентов защиты, в том числе для обновления баз и модулей программы. 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	Если флажок установлен, то при обновлении Kaspersky Endpoint Security из папки общего доступа прокси-сервер не используется.
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 программ. 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 программ из списка, рекомендованного "Лабораторией Касперского"**. Предустановленный список программ, сетевые порты которых контролирует Kaspersky Endpoint Security. В список включены, например, Google Chrome, Adobe Reader, Java и другие программы. **Контролировать все порты для указанных программ**. Список программ, 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 файловых 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 программами, 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 программы. Вы можете просмотреть предустановленный список доверенных сайтов только в интерфейсе Kaspersky Endpoint Security. В консоли Kaspersky Security Center просмотреть список невозможно.
При переходе на домен с недоверенным сертификатом	• **Разрешать**. Если выбран этот вариант, то 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. 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. • **Блокировать соединение**. Если выбран этот вариант, то 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.
В случае возникновении ошибки при проверке защищенного соединения	• **Блокировать соединение**. Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security блокирует это сетевое соединение. • **Добавлять домен в исключения**. Если выбран этот элемент, то 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 программы. Чтобы сбросить содержание списка, нужно выбрать элемент **Блокировать соединение**.

Блокировать соединения по протоколу SSL 2.0	Если флажок установлен, то Kaspersky Endpoint Security блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то Kaspersky Endpoint Security не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0, и не контролирует сетевой трафик, передаваемый по этим соединениям.
Расшифровать 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, Kaspersky Endpoint Security расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если флажок снят, Kaspersky Endpoint Security не имеет доступа к содержанию HTTPS-трафика. Поэтому программа контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://facebook.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.
Доверенные адреса	Список веб-адресов, для которых Kaspersky Endpoint Security не проверяет сетевые соединения. Вы можете ввести имя домена или IP-адрес. Kaspersky Endpoint Security поддерживает символ `*` для ввода маски в имени домена. Kaspersky Endpoint Security не поддерживает маски для IP-адресов. 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`.
Доверенные программы	Список программ, активность которых Kaspersky Endpoint Security не проверяет в процессе своей работы. Вы можете выбрать виды активности программы, которые Kaspersky Endpoint Security не будет контролировать (например, не проверять сетевой трафик). Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
Проверять защищенный трафик в продуктах Mozilla	Если флажок установлен, Kaspersky Endpoint Security проверяет зашифрованный трафик в браузере Mozilla Firefox и почтовом клиенте Thunderbird. Доступ к некоторым сайтам по протоколу HTTPS может быть заблокирован.

(доступен только в интерфейсе Kaspersky Endpoint Security)	Для проверки трафика в браузере Mozilla Firefox и почтовом клиенте Thunderbird должна быть включена проверка защищенных соединений. Если проверка защищенных соединений выключена, Kaspersky Endpoint Security не проверяет трафик в браузере Mozilla Firefox и почтовом клиенте Thunderbird. Kaspersky Endpoint Security расшифровывает и анализирует зашифрованный трафик с помощью корневого сертификата "Лаборатории Касперского". Вы можете выбрать хранилище сертификатов, в котором будет находиться корневой сертификат "Лаборатории Касперского": • **Использовать хранилище сертификатов Windows**. Это хранилище, в которое корневой сертификат "Лаборатории Касперского" добавляется при установке Kaspersky Endpoint Security. • **Использовать хранилище сертификатов Mozilla**. Программы 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 программы.

Параметры интерфейса

Параметр	Описание
Взаимодействие с пользователем *(доступен только в консоли Kaspersky Security Center)*	**С упрощенным интерфейсом**. На клиентском компьютере недоступно главное окно программы, 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 уведомления над значком программы. **С полным интерфейсом**. 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. **Без интерфейса**. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security. Также недоступны значок в области уведомлений Windows и уведомления.
Настройка уведомлений	Таблица с параметрами уведомлений о событиях различного уровня важности, которые могут происходить во время работы компонента или программы в целом, а также выполнения задачи. Уведомления об этих событиях Kaspersky Endpoint Security выводит на экран, доставляет по электронной почте или сохраняет в журналы.
Настройка почтовых уведомлений	Параметры SMTP-сервера для рассылки оповещений о событиях, регистрируемых при работе программы.
Отображать состояние программы в	Категории событий программы, при возникновении которых меняется значок Kaspersky Endpoint Security в области уведомлений панели задач Microsoft Windows ( или ).

области уведомлений	
Уведомления о состоянии локальных антивирусных баз	Параметры уведомлений о неактуальности антивирусных баз, которые использует программа.
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 выполнения операций.
Веб-ресурсы Службы технической поддержки *(доступен только в консоли Kaspersky Security Center)*	Список ссылок на веб-сайты с информацией о технической поддержке программы Kaspersky Endpoint Security. Добавленные ссылки отображаются в окне **Поддержка** локального интерфейса Kaspersky Endpoint Security вместо стандартных ссылок.
Сообщение пользователю *(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 программы на другом компьютере. Также вы можете использовать конфигурационный файл при развертывании программы через Kaspersky Security Center 12 при помощи инсталляционного пакета. Вы можете в любой момент вернуться к параметрам по умолчанию.

Параметры управления настройками программы доступны только в интерфейсе Kaspersky Endpoint Security.

Параметры управления настройками программы

Настройка	Описание
Импортировать	Извлечь настройки работы программы из файла формата CFG и применить их.
Экспортировать	Сохранить текущие настройки работы программы в файл формата CFG.
Восстановить	Вы в любое время можете восстановить настройки Kaspersky Endpoint Security, рекомендуемые "Лабораторией Касперского". В результате восстановления настроек для всех компонентов защиты будет установлен уровень безопасности **Рекомендуемый**.

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*.

Параметры управления задачами

Параметр	Описание
Разрешить использование локальных задач	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 использование локальных задач прекращается. 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 антивирусную 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.
Разрешить отображение групповых задач	Если флажок установлен, то групповые задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь может просмотреть полный список задач в интерфейсе программы. Если флажок снят, Kaspersky Endpoint Security показывает пустой список задач.
Разрешить управление групповыми задачами	Если флажок установлен, пользователь может запускать и останавливать заданные в Kaspersky Security Center групповые задачи. Пользователь может запускать и останавливать задачи в интерфейсе программы или в упрощенном интерфейсе программы. Если флажок снят, Kaspersky Endpoint Security запускает задачи автоматически по расписанию, или администратор запускает задачи вручную в Kaspersky Security Center.

Проверка компьютера

Антивирусная проверка является важным фактором для обеспечения безопасности компьютера. Требуется регулярно выполнять антивирусную проверку, чтобы исключить возможность распространения вредоносных программ, 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 запускать 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:

- память ядра;
- объекты, загрузка которых осуществляется при запуске операционной системы;
- резервное хранилище операционной системы;

- почтовый ящик Microsoft Outlook;
- 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

Kaspersky Endpoint Security проверяет модули программы на наличие повреждений или изменений.

Параметры проверки

Параметр	Описание
Уровень безопасности	Для проверки Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в программе, называются *уровнями безопасности*. • **Высокий**. Kaspersky Endpoint Security проверяет файлы всех типов. Во время проверки составных файлов Kaspersky Endpoint Security дополнительно проверяет файлы почтовых форматов. • **Рекомендуемый**. Kaspersky Endpoint Security проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты. Kaspersky Endpoint Security не проверяет архивы и установочные пакеты. • **Низкий**. Kaspersky Endpoint Security проверяет только новые и измененные файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера. Kaspersky Endpoint Security не проверяет составные файлы.
Действие при обнаружении угрозы	**Лечить; удалять, 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 их удаляет. **Лечить; блокировать, 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 Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.

Область защиты	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, почтовые базы, жесткий, съемный или сетевой диск, папка или файл.
Расписание проверки	**Вручную**. Режим запуска, при котором вы запускаете проверку вручную в удобное для вас время. **По расписанию**. Режим запуска задачи проверки, при котором Kaspersky Endpoint Security выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.
Запускать пропущенные задачи *(доступен только в консоли Kaspersky Security Center)*	Если флажок установлен, Kaspersky Endpoint Security запускает пропущенную задачу проверки, как только это станет возможным. Задача проверки может быть пропущена, например, если в установленное время запуска задачи проверки был выключен компьютер. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи проверки, а выполняет следующую задачу проверки по установленному расписанию.
Выполнять только во время простоя компьютера	Отложенный запуск задачи проверки, если ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка.
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 Kaspersky Endpoint Security, и запускать задачу проверки от имени этого пользователя.
Типы файлов	Файлы без расширения Kaspersky Endpoint Security считает исполняемыми. Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
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 файлы, если их проверка длится более N секунд	Ограничение длительности проверки одного объекта. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку файла. Это позволит сократить время выполнения проверки.

Проверять архивы	Проверка архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Проверять дистрибутивы	Флажок включает / выключает проверку дистрибутивов сторонних программ.
Проверять файлы офисных форматов	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты.
Проверять файлы почтовых форматов	Флажок включает / выключает функцию, с помощью которой Kaspersky Endpoint Security проверяет файлы почтовых форматов, а также почтовые базы данных. Программа полностью проверяет только файлы почтовых форматов MS Outlook, Windows Mail/Outlook Express и формата EML, и только при наличии на компьютере почтового клиента MS Outlook x86. 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.
Проверять архивы, защищенные паролем	Если флажок установлен, Kaspersky Endpoint Security проверяет архивы, защищенные паролем. Перед проверкой файлов, содержащихся в архиве, на экран выводится запрос пароля. Если флажок не установлен, Kaspersky Endpoint Security пропускает проверку защищенных паролем архивов.
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 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 программ "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	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 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 программе структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

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. 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.

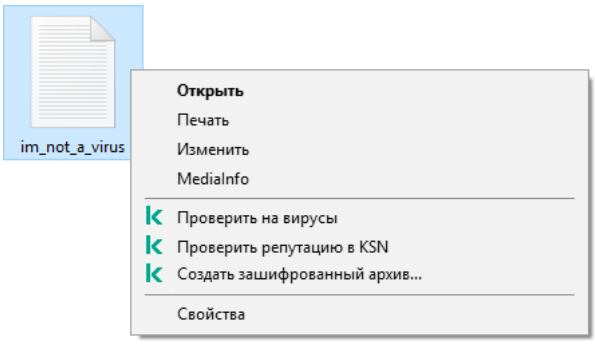
- Компьютер (ноутбук) перешел в режим питания от батареи.

При выполнении фоновой проверки Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.

Проверка из контекстного меню

Kaspersky Endpoint Security позволяет проверять отдельные файлы на вирусы и другие программы, 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

Параметры задачи Проверка из контекстного меню

Параметр	Описание
Действие при обнаружении угрозы	**Лечить; удалять, 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 их удаляет. **Лечить; блокировать, 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.
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 файлы, если их проверка длится более N сек	Ограничение длительности проверки одного объекта. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку файла. Это позволит сократить время выполнения проверки.
Проверять архивы	Проверка архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
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.
Не распаковывать составные файлы большого размера	Если флажок установлен, то Kaspersky Endpoint Security не проверяет составные файлы, размеры которых превышают заданное значение.
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 программ "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	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 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 программе структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Проверка съемных дисков

Kaspersky Endpoint Security позволяет проверять на вирусы и другие программы, представляющие угрозу, съемные диски при их подключении к компьютеру.

Параметры задачи Проверка съемных дисков

Параметр	Описание
Действие при подключении съемного диска	• **Не проверять**. • **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. • **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 съемного диска	Если флажок установлен, то Kaspersky Endpoint Security выполняет действие, выбранное в раскрывающемся списке **Действие при подключении съемного диска**, над съемными дисками, размер которых не превышает указанный максимальный размер.

	Если флажок снят, то Kaspersky Endpoint Security выполняет действие, выбранное в раскрывающемся списке **Действие при подключении съемного диска**, над съемными дисками любого размера.
Отображать ход проверки	Если флажок установлен, то Kaspersky Endpoint Security отображает ход проверки съемных дисков в отдельном окне, а также в окне **Задачи**. Если флажок снят, то Kaspersky Endpoint Security выполняет проверку съемных дисков в фоновом режиме.
Запретить остановку задачи проверки	Если флажок установлен, то в локальном интерфейсе Kaspersky Endpoint Security для задачи проверки съемных дисков недоступны кнопка **Остановить** в окне **Задачи** и кнопка **Остановить** в окне **Антивирусная проверка**.

Проверка целостности программы

Kaspersky Endpoint Security проверяет файлы программы, находящиеся в папке установки программы, на наличие повреждений или изменений. Например, если библиотека программы имеет некорректную цифровую подпись, то такая библиотека считается поврежденной. Для проверки файлов программы предназначена задача *Проверка целостности*. Запускайте задачу *Проверка целостности*, если программа Kaspersky Endpoint Security обнаружила вредоносный объект и не обезвредила его.

Вы можете создать задачу *Проверка целостности* в Kaspersky Security Center 12 Web Console и Консоли администрирования. Создать задачу в программе Kaspersky Security Center Cloud Console невозможно.

Нарушения целостности программы 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.

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 Kaspersky Endpoint Security 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 проверки, как только это станет возможным. Задача проверки может быть пропущена, например, если в установленное время запуска задачи проверки был выключен компьютер. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи проверки, а выполняет следующую задачу проверки по установленному расписанию.
Выполнять только во время	Отложенный запуск задачи проверки, если ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка.

простоя компьютера	
Запускать с правами пользователя *(доступен только в консоли Kaspersky Security Center)*	По умолчанию задача проверки запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Для доступа к папке установки программы могут потребоваться специальные права. Вы можете указать пользователя, обладающего этими правами, в параметрах Kaspersky Endpoint Security, и запускать задачу проверки от имени этого пользователя.

Обновление баз и модулей программы

Обновление баз и модулей программы Kaspersky Endpoint Security обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие программы, 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 программы.

Для регулярного обновления требуется действующая лицензия на использование программы. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

Основным источником обновлений Kaspersky Endpoint Security служат серверы обновлений "Лаборатории Касперского".

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 программ, 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 программы. Помимо баз Kaspersky Endpoint Security, можно обновлять и модули программы. Обновления модулей программы устраняют уязвимости Kaspersky Endpoint Security, добавляют новые функции или улучшают существующие.

В процессе обновления базы и модули программы на вашем компьютере сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы и модули программы отличаются от актуальной версии, на компьютер устанавливается недостающая часть обновлений.

Вместе с обновлением модулей программы может быть обновлена и контекстная справка программы.

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 блоке **Обновление** в окне **Задачи**.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении задачи обновления, записывается в отчет Kaspersky Endpoint Security.

Параметры обновления баз и модулей программы

Параметр	Описание
Режим запуска	**Автоматически**. Режим запуска задачи обновления, при котором 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, 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 Kaspersky Endpoint Security выполняет задачу обновления по сформированному вами расписанию. Если выбран этот режим запуска задачи обновления, вы также можете запускать задачу обновления Kaspersky Endpoint Security вручную.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Endpoint Security запускает пропущенную задачу обновления, как только это станет возможным. Задача обновления может быть пропущена, например, если в установленное время запуска задачи обновления был выключен компьютер. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи обновления, а выполняет следующую задачу обновления по установленному расписанию.
Источник обновлений	*Источник обновлений* – это ресурс, содержащий обновления баз и модулей программы Kaspersky Endpoint Security. Источником обновлений могут быть сервер Kaspersky Security Center, серверы обновлений "Лаборатории Касперского", сетевая или локальная папка. 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.
Запускать	По умолчанию задача обновления Kaspersky Endpoint Security запускается от имени

задачу с правами пользователя	пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление 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 Kaspersky Endpoint Security и запускать задачу обновления Kaspersky Endpoint Security от имени этого пользователя.
Загружать обновления модулей программы	Флажок включает / выключает закачку обновлений модулей программы наряду с обновлениями баз программы. Если флажок установлен, то Kaspersky Endpoint Security уведомляет пользователя о доступных обновлениях модулей программы и во время выполнения задачи обновления включает обновления модулей программы в пакет обновлений. При этом применение обновлений модулей программы определяется следующими параметрами: • **Устанавливать критические и одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает критические обновления автоматически, а остальные обновления модулей программы – после одобрения их установки, локально через интерфейс программы или на стороне Kaspersky Security Center. • **Устанавливать только одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс программы 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 программы и во время выполнения задачи обновления не включает обновления модулей программы в пакет обновлений. Если обновление модулей программы предполагает ознакомление и согласие с положениями Лицензионного соглашения, то программа 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\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 программы. 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-	Если флажок установлен, то при обновлении Kaspersky Endpoint Security из папки общего доступа прокси-сервер не используется.

сервер для локальных адресов *(доступен только в интерфейсе Kaspersky Endpoint Security)*	

Приложение 2. Группы доверия программ

Все программы, запускаемые на компьютере, Kaspersky Endpoint Security распределяет на группы доверия. Программы распределяются на группы доверия в зависимости от степени угрозы, которую эти программы могут представлять для операционной системы.

Существуют следующие группы доверия:

- **Доверенные**. В группу входят программы, для которых выполняется одно или более следующих условий:
  - Программы обладают цифровой подписью доверенных производителей.
  - О программах есть записи в базе доверенных программ Kaspersky Security Network.
  - Пользователь поместил программы в группу "Доверенные".

  Запрещенных операций для таких программ нет.
- **Слабые ограничения**. В группу входят программы, для которых выполняются следующие условия:
  - Программы не обладают цифровой подписью доверенных производителей.
  - О программах нет записей в базе доверенных программ Kaspersky Security Network.
  - Пользователь поместил программы в группу "Слабые ограничения".

  Такие программы имеют минимальные ограничения на работу с ресурсами операционной системы.
- **Сильные ограничения**. В группу входят программы, для которых выполняются следующие условия:
  - Программы не обладают цифровой подписью доверенных производителей.
  - О программах нет записей в базе доверенных программ Kaspersky Security Network.
  - Пользователь поместил программы в группу "Сильные ограничения".

  Такие программы имеют значительные ограничения на работу с ресурсами операционной системы.
- **Недоверенные**. В группу входят программы, для которых выполняются следующие условия:
  - Программы не обладают цифровой подписью доверенных производителей.
  - О программах нет записей в базе доверенных программ Kaspersky Security Network.

- Пользователь поместил программы в группу "Недоверенные".

Для таких программ запрещены все операции.

Приложение 3. Расширения файлов для быстрой проверки съемных дисков

com – исполняемый файл программы размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив;

sys – системный файл Microsoft Windows;

prg – текст программы dBase™, Clipper или Microsoft Visual FoxPro®, программа 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 – программа, работающая в режиме разделения времени;

drv – драйвер некоторого устройства;

vxd – драйвер виртуального устройства Microsoft Windows;

pif – файл с информацией о программе;

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 программ;

cla – класс Java;

vbs – скрипт Visual Basic®;

vbe – видеорасширение BIOS;

js, jse – исходный текст JavaScript;

htm – гипертекстовый документ;

htt – гипертекстовая заготовка Microsoft Windows;

hta – гипертекстовая программа 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;

eml – сообщение электронной почты Microsoft Outlook Express;

nws – новое сообщение электронной почты Microsoft Outlook Express;

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 – программа 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 программы размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив;

sys – системный файл Microsoft Windows;

prg – текст программы dBase™, Clipper или Microsoft Visual FoxPro®, программа 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 – программа, работающая в режиме разделения времени;

drv – драйвер некоторого устройства;

vxd – драйвер виртуального устройства Microsoft Windows;

pif – файл с информацией о программе;

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 программ;

cla – класс Java;

vbs – скрипт Visual Basic®;

vbe – видеорасширение BIOS;

js, jse – исходный текст JavaScript;

htm – гипертекстовый документ;

htt – гипертекстовая заготовка Microsoft Windows;

hta – гипертекстовая программа 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;

eml – сообщение электронной почты Microsoft Outlook Express;

nws – новое сообщение электронной почты Microsoft Outlook Express;

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 – программа 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 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.

`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`
	Обновление баз и модулей приложения.

`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`	

`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. 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 Kaspersky Endpoint Security использует публичный DNS-сервер, правила обработки данных регламентируются Политикой конфиденциальности этого сервиса. Если требуется запретить 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 (Защита от веб-угроз и Веб-Контроль).

`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`
	Обновление баз и модулей приложения.

`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`	

`ds.kaspersky.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: `Any`
Порт: `443`, `1443`
	Использование Kaspersky Security Network.

`click.kaspersky.com`
`redirect.kaspersky.com`
Протокол: `HTTPS`
	Переход по ссылкам из интерфейса.

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Протокол: `HTTP`
Порт: `80`
	Инфраструктура открытых ключей (англ. Public Key Infrastructure – PKI).

Приложение 6. События программы в журнале событий Windows

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 программы в целом сохраняется в журнале событий Windows.

Системный аудит

Коды событий

Идентификатор события	Описание	По умолчанию включено
201	Нарушено Лицензионное соглашение.	✓
203	Срок действия лицензии почти истек.	–
204	Срок действия лицензии скоро истекает.	–
206	Базы повреждены или отсутствуют.	–
207	Базы сильно устарели.	–
208	Базы устарели.	–
209	Автозапуск программы выключен.	–
210	Автоматическое обновление выключено.	–
211	Самозащита программы выключена.	–
212	Задача не может быть выполнена.	–
213	Действие с ресурсами программы заблокировано самозащитой.	–
214	Компоненты защиты выключены.	–
215	Компьютер работает в безопасном режиме.	–
216	Есть необработанные файлы.	–
217	Отчет очищен.	✓
218	Изменены настройки программы.	✓
219	Применена групповая политика.	✓
220	Групповая политика деактивирована.	–
221	Задача запущена.	–
222	Задача остановлена.	–
223	Задача завершена.	–
224	Для завершения обновления необходимо перезапустить программу.	–
225	Необходима перезагрузка компьютера.	✓
226	Установлены не все компоненты программы, которые позволяет использовать лицензия.	–
227	Установленные компоненты соответствуют лицензии.	–
229	Ошибка активации.	✓
230	Некорректный резервный код активации.	–
231	Обнаружена активная угроза. Требуется запуск процедуры лечения активного заражения.	–
232	Запущена процедура лечения активного заражения.	–
233	Процедура лечения активного заражения завершена.	–
235	Программа запущена.	✓

236	Программа остановлена.	✓
237	Обнаружено некорректное завершение предыдущей сессии работы программы.	✓
240	Срок действия лицензии скоро истекает.	✓
238	Параметры подписки были изменены.	✓
239	Подписка была продлена.	✓
335	Объект восстановлен из резервного хранилища.	✓
336	Невозможно восстановить объект из резервного хранилища.	✓
245	Обработка программой некоторых функций ОС отключена.	✓
250	Защищенное соединение разорвано.	✓
708	Настройки задачи успешно применены.	–
335	Объект восстановлен из резервного хранилища.	✓
2000	Ввод имени пользователя и пароля.	–
2001	Обнаружена подозрительная сетевая активность.	–
2020	Участие в KSN включено.	–
2021	Участие в KSN выключено.	–
2022	Серверы KSN доступны.	–
2023	Серверы KSN недоступны.	–
2024	Программа работает и обрабатывает данные в соответствии с местным законодательством и использует локальную инфраструктуру.	✓
227	Все компоненты программы, которые допускает лицензия, установлены и работают в нормальном режиме.	–

Анализ поведения

Коды событий

Идентификатор события	Описание	По умолчанию включено
303	Обнаружена легальная программа, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.	–
307	Объект удален.	–
308	Создана резервная копия объекта.	–
311	Невозможно создать резервную копию объекта.	–
313	Невозможно удалить.	–
323	Объект будет удален при перезагрузке.	–
329	Объект переименован.	–
331	Запрещено.	–
452	Процесс завершен.	–
453	Невозможно завершить процесс.	–
455	Откат выполнен.	–
458	Значение реестра восстановлено.	–
459	Значение реестра удалено.	–
453	Запуск кода/файла заблокирован.	–

Защита от эксплойтов

Коды событий

Идентификатор события	Описание	По умолчанию включено
302	Обнаружен вредоносный объект.	–
331	Запрещено.	–
455	Откат выполнен.	–
323	Объект будет удален при перезагрузке.	–
307	Объект удален.	–
329	Объект переименован.	–
457	Файл восстановлен.	–
458	Значение реестра восстановлено.	–
459	Значение реестра удалено.	–

Предотвращение вторжений

Коды событий

Идентификатор события	Описание	По умолчанию включено
301	Объект обработан.	–
302	Обнаружен вредоносный объект.	–
303	Обнаружена легальная программа, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.	–
306	Объект вылечен.	–
307	Объект удален.	–
308	Создана резервная копия объекта.	–
310	Невозможно создать резервную копию объекта.	–
312	Лечение невозможно.	–
313	Невозможно удалить.	–
314	Объект не обработан.	–
315	Объект пропущен.	–
317	Ошибка обработки.	✓
318	Обнаружен архив.	–
319	Обнаружен упакованный объект.	–
320	Объект зашифрован.	–
321	Объект поврежден.	–
322	Обнаружен защищенный паролем архив.	–
323	Объект будет удален при перезагрузке.	–
324	Объект будет вылечен при перезагрузке.	–
327	Объект перезаписан вылеченной ранее копией.	–
332	Информация об обнаруженном объекте.	–
335	Объект восстановлен из резервного хранилища.	–
336	Невозможно восстановить объект из резервного хранилища.	✓
340	Объект находится в списке разрешенных в Локальном KSN.	✓
401	Программа помещена в группу доверенных программ.	–
402	Программа помещена в группу с ограничениями.	–
403	Сработал компонент Предотвращение вторжений.	–
452	Процесс завершен.	–
453	Невозможно завершить процесс.	–

Защита от файловых угроз

Коды событий

Идентификатор события	Описание	По умолчанию включено
302	Обнаружен вредоносный объект.	✓
317	Ошибка обработки.	✓
336	Невозможно восстановить объект из резервного хранилища.	✓
340	Объект находится в списке разрешенных в Локальном KSN.	✓
301	Объект обработан.	–
306	Объект вылечен.	–
307	Объект удален.	–
308	Создана резервная копия объекта.	–
310	Невозможно создать резервную копию объекта.	–
312	Лечение невозможно.	–
313	Невозможно удалить.	–
314	Объект не обработан.	–
315	Объект пропущен.	–
318	Обнаружен архив.	–
319	Обнаружен упакованный объект.	–
320	Объект зашифрован.	–
321	Объект поврежден.	–
322	Обнаружен защищенный паролем архив.	–
323	Объект будет удален при перезагрузке.	–
324	Объект будет вылечен при перезагрузке.	–
325	Объект перезаписан вылеченной ранее копией.	–
303	Обнаружена легальная программа, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.	–
329	Объект переименован.	–
335	Объект восстановлен из резервного хранилища.	–
452	Процесс завершен.	–
453	Невозможно завершить процесс.	–
332	Информация об обнаруженном объекте.	–

Защита от веб-угроз

Коды событий

Идентификатор события	Описание	По умолчанию включено
301	Объект обработан.	–
302	Обнаружен вредоносный объект.	✓
303	Обнаружена легальная программа, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.	–
317	Ошибка обработки.	✓
318	Обнаружен архив.	–
319	Обнаружен упакованный объект.	–
321	Объект поврежден.	–
322	Обнаружен защищенный паролем архив.	–
329	Объект переименован.	–
362	Заблокирована опасная ссылка.	✓
1201	Обнаружена ранее открытая опасная ссылка.	✓
1211	Обнаружена ранее открытая вредоносная ссылка.	✓
363	Открыта опасная ссылка.	✓
341	Загрузка объекта запрещена.	–
370	Ссылка находится в списке разрешенных в Локальном KSN.	✓
370	Объект находится в списке разрешенных в Локальном KSN.	✓
332	Информация об обнаруженном объекте.	–

Защита от почтовых угроз

Коды событий

Идентификатор события	Описание	По умолчанию включено
301	Объект обработан.	–
306	Объект вылечен.	–
302	Обнаружен вредоносный объект.	✓
317	Ошибка обработки.	✓
340	Объект находится в списке разрешенных в Локальном KSN.	✓
307	Объект удален.	–
308	Создана резервная копия объекта.	–
312	Лечение невозможно.	–
314	Объект не обработан.	–
318	Обнаружен архив.	–
319	Обнаружен упакованный объект.	–
321	Объект поврежден.	–
322	Обнаружен защищенный паролем архив.	–
329	Объект переименован.	–
303	Обнаружена легальная программа, которая может быть использована злоумышленником для нанесения вреда компьютеру.	–
332	Информация об обнаруженном объекте.	–

Сетевой экран

Коды событий

Идентификатор события	Описание	По умолчанию включено
601	Сетевая активность разрешена.	–
602	Сетевая активность запрещена.	–

Защита от сетевых угроз

Коды событий

Идентификатор события	Описание	По умолчанию включено
651	Обнаружена сетевая атака.	–

Защита от атак BadUSB

Коды событий

Идентификатор события	Описание	По умолчанию включено
2050	Клавиатура авторизована.	–
2051	Клавиатура не авторизована.	✓
2052	Ошибка авторизации клавиатуры.	✓

AMSI-защита

Коды событий

Идентификатор события	Описание	По умолчанию включено
301	Объект обработан.	–
302	Обнаружен вредоносный объект.	✓
303	Обнаружена легальная программа, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.	–
314	Объект не обработан.	–
315	Объект пропущен.	–
317	Ошибка обработки.	✓
318	Обнаружен архив.	–
319	Обнаружен упакованный объект.	–
320	Объект зашифрован.	–
321	Объект поврежден.	–
322	Обнаружен защищенный паролем архив.	–
1512	Результат проверки объекта передан стороннему приложению.	–
329	Объект переименован.	–
332	Информация об обнаруженном объекте.	–
340	Объект находится в списке разрешенных в Локальном KSN.	✓
2200	AMSI-запрос заблокирован.	✓

Контроль программ

Коды событий

Идентификатор события	Описание	По умолчанию включено
701	Запуск программы разрешен.	–
702	Запуск программы запрещен.	–
703	Запуск программы запрещен в тестовом режиме.	–
704	Запуск программы разрешен в тестовом режиме.	–
707	Ошибка в настройках задачи. Настройки задачи не применены.	–
710	Запрещенный процесс был запущен до запуска Kaspersky Endpoint Security для Windows.	–
708	Настройки задачи успешно применены.	–

Контроль устройств

Коды событий

Идентификатор события	Описание	По умолчанию включено
801	Операция с устройством разрешена.	–
802	Операция с устройством запрещена.	–
803	Активирован временный доступ к устройству.	✓
808	Выполнена операция с файлом.	–
809	Сетевое соединение заблокировано.	–

Веб-Контроль

Коды событий

Идентификатор события	Описание	По умолчанию включено
751	Доступ разрешен.	–
752	Доступ запрещен.	–
753	Предупреждение о нежелательном содержимом.	–
754	Осуществлен доступ к нежелательному содержимому после предупреждения.	–
751	Открыта разрешенная страница.	–

Адаптивный контроль аномалий

Коды событий

Идентификатор события	Описание	По умолчанию включено
501	Жалоба на блокировку активности программы.	–
2201	Действие процесса пропущено.	–
2200	Действие процесса заблокировано.	✓

Шифрование данных

Коды событий

Идентификатор события	Описание	По умолчанию включено
904	Ошибка применения правил шифрования/расшифровки файлов.	✓
912	Ошибка шифрования/расшифровки файла.	✓
1305	Ошибка шифрования/расшифровки устройства.	✓
931	Ошибка создания зашифрованного архива.	✓
951	Ошибка активации портативного режима.	✓
953	Ошибка деактивации портативного режима.	✓
1311	Не удалось загрузить модуль шифрования.	✓
1340	Задача управления учетными записями Агента аутентификации завершилась с ошибкой.	✓
1312	Политика не может быть применена.	✓
1342	Обновление функциональности шифрования завершено с ошибкой.	✓
1343	Откат обновления функциональности шифрования завершен успешно.	✓
1345	Не удалось установить или обновить драйверы Kaspersky Disk Encryption в образе среды восстановления Windows.	✓
1346	Не удалось удалить драйверы Kaspersky Disk Encryption из образа среды восстановления Windows.	✓
1370	Ключ восстановления для BitLocker изменен.	✓
901	Началось применение правил шифрования/расшифровки файлов.	–
902	Завершено выполнение правил шифрования/расшифровки файлов.	–
903	Прервано применение правил шифрования/расшифровки файлов.	–
905	Продолжено применение правил шифрования/расшифровки файлов.	–
910	Запущена операция шифрования/расшифровки файла.	–
911	Завершена операция шифрования/расшифровки файла.	–
913	Шифрование файла не выполнено, так как файл является исключением.	–
914	Операция шифрования/расшифровки файла прервана.	–
1301	Запущена операция шифрования/расшифровки устройства.	–
1302	Завершена операция шифрования/расшифровки устройства.	–
1307	Устройство не зашифровано.	–
1303	Приостановка шифрования/расшифровки устройства.	–
1304	Возобновление шифрования/расшифровки устройства.	–
1309	Процесс шифрования/расшифровки устройства переведен в	–

	пассивный режим.	
1308	Процесс шифрования/расшифровки устройства переведен в активный режим.	–
1306	Пользователь отказался от политики шифрования.	–
940	Заблокирован доступ к файлу.	✓
950	Активирован портативный режим.	–
952	Деактивирован портативный режим.	–
1330	Создана новая учетная запись Агента аутентификации.	–
1337	Учетная запись не добавлена. Такая учетная запись уже существует.	–
1338	Учетная запись не изменена. Такая учетная запись не существует.	–
1339	Учетная запись не удалена. Такая учетная запись не существует.	–
1331	Удалена учетная запись Агента аутентификации.	–
1332	Изменен пароль для учетной записи Агента аутентификации.	–
1334	Аутентификация в Агенте аутентификации завершилась с ошибкой.	–
1333	Успешная аутентификации в Агенте аутентификации.	–
1335	Получен доступ к жесткому диску с помощью процедуры запроса доступа к зашифрованным устройствам.	–
1336	Попытка получения доступа к жесткому диску с помощью процедуры запроса доступа к зашифрованным устройствам завершилась с ошибкой.	–
1310	Загружен модуль шифрования.	–
1344	Откат обновления функциональности шифрования завершен с ошибкой.	✓
1341	Обновление функциональности шифрования завершено успешно.	✓
1332	Изменен пароль для учетной записи Агента Аутентификации.	–

Endpoint Sensor

Коды событий

Идентификатор события	Описание	По умолчанию включено
2100	Сервер Kaspersky Anti Targeted Attack Platform недоступен.	–
2105	Запуск программы был заблокирован.	✓
2106	Открытие документа было заблокировано.	✓
2104	Задачи с сервера Kaspersky Anti Targeted Attack Platform обрабатываются.	–
2103	Задачи с сервера Kaspersky Anti Targeted Attack Platform не обрабатываются.	–
2101	Компонент Endpoint Sensors подключен к серверу.	–
2102	Связь с сервером Kaspersky Anti Targeted Attack Platform восстановлена.	–
2112	Завершение всех процессов, запущенных с файл-образа или стрима.	✓
2113	Запуск программы.	✓
2111	Файл или стрим удален администратором сервера Kaspersky Anti Targeted Attack Platform.	✓
2110	Файл восстановлен из карантина сервера Kaspersky Anti Targeted Attack Platform администратором.	✓
2109	Файл помещен на карантин сервера Kaspersky Anti Targeted Attack Platform администратором.	✓
2107	Сетевая активность программ сторонних производителей заблокирована.	✓
2108	Сетевая активность программ сторонних производителей разблокирована.	✓

Проверка компьютера

Коды событий

Идентификатор события	Описание	По умолчанию включено
302	Обнаружен вредоносный объект.	✓
335	Объект восстановлен из резервного хранилища.	✓
336	Невозможно восстановить объект из резервного хранилища.	✓
340	Объект находится в списке разрешенных в Локальном KSN.	✓
301	Объект обработан.	–
329	Объект переименован.	–
306	Объект вылечен.	–
307	Объект удален.	–
308	Создана резервная копия объекта.	–
310	Невозможно создать резервную копию объекта.	–
312	Лечение невозможно.	–
313	Невозможно удалить.	–
314	Объект не обработан.	–
315	Объект пропущен.	–
317	Ошибка обработки.	–
318	Обнаружен архив.	–
319	Обнаружен упакованный объект.	–
320	Объект зашифрован.	–
321	Объект поврежден.	–
322	Обнаружен защищенный паролем архив.	–
323	Объект будет удален при перезагрузке.	–
324	Объект будет вылечен на перезагрузке.	–
327	Объект перезаписан вылеченной ранее копией.	–
303	Обнаружена легальная программа, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя.	–

Проверка целостности

Коды событий

Идентификатор события	Описание	По умолчанию включено
2002	Неуспешная проверка подписи модуля системы	–

Обновление баз

Коды событий

Идентификатор события	Описание	По умолчанию включено
101	Произошла внутренняя ошибка.	✓
1001	Выбран источник обновлений.	–
1002	Выбран прокси-сервер.	–
1003	Загрузка файла.	–
1004	Файл загружен.	–
1005	Файл установлен.	–
1006	Файл обновлен.	–
1007	Выполнен откат файла из-за ошибки обновления.	–
1008	Обновление файлов.	–
1009	Копирование обновлений.	–
1010	Откат файлов.	–
1011	Ошибка обновления компонента.	–
1012	Ошибка копирования обновлений компонента.	–
1013	Формирование списка файлов для загрузки.	–
1014	Локальная ошибка обновления.	–
1016	Операция отменена пользователем.	–
1017	Невозможен запуск двух задач одновременно.	–
1018	Ошибка проверки баз и модулей программы.	–
1019	Ошибка взаимодействия с Kaspersky Security Center.	–
1020	Нет доступных обновлений.	–
1021	Обновлены не все компоненты.	–
1022	Копирование обновлений успешно завершено.	–
1023	Обновление завершено успешно, а копирование обновлений завершено с ошибкой.	–
2153	Ошибка установки патча.	–
2156	Ошибка отката патча.	–
2150	Загрузка патчей.	–
2151	Установка патчей.	–
2152	Патч установлен.	–
2154	Откат патча.	–
2155	Откат патча выполнен.	–

Удаление данных

Коды событий

Идентификатор события	Описание	По умолчанию включено
223	Задача завершена.	–
221	Задача запущена.	–
222	Задача остановлена.	–
2252	Невозможно удалить объект.	–
2253	Статистика задачи удаления.	–
2251	Объект удален.	–

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Acrobat, Flash, Reader и Shockwave – товарные знаки или зарегистрированные в Соединенных Штатах Америки и / или в других странах товарные знаки Adobe Systems Incorporated.

Apple, FireWire, iTunes и Safari – товарные знаки Apple Inc., зарегистрированные в США и 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.

Android и Google Chrome – товарные знаки Google, Inc.

Citrix, Citrix Provisioning Services и XenDesktop – товарные знаки Citrix Systems, Inc. и/или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

Dell – товарный знак Dell, Inc. или дочерних компаний.

dBase – товарный знак dataBased Intelligence, Inc.

EMC – зарегистрированный товарный знак или товарный знак EMC Corporation в США и/или других странах.

Radmin – зарегистрированный товарный знак Famatech.

IBM – товарный знак International Business Machines Corporation, зарегистрированный во многих юрисдикциях по всему миру.

ICQ – товарный знак и/или знак обслуживания ICQ LLC.

Intel – товарный знак Intel Corporation, зарегистрированный в Соединенных Штатах Америки и в других странах.

IOS – зарегистрированный в Соединенных Штатах Америки и в других странах товарный знак Cisco Systems, Inc. и / или ее аффилированных компаний.

Lenovo и 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 – товарный знак или зарегистрированный в США и других странах товарный знак McAfee, Inc.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Surface и Hyper-V – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla, Firefox и Thunderbird – товарные знаки Mozilla Foundation.

Java и JavaScript – зарегистрированные товарные знаки компании Oracle и/или ее аффилированных компаний.

VERISIGN – зарегистрированный в США и других странах или незарегистрированный товарный знак VeriSign, Inc. и дочерних компаний.

VMware и VMware ESXi – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

Thawte – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

SAMSUNG – товарный знак компании SAMSUNG в США или других странах.