kaspersky

Kaspersky Endpoint Security для Linux 12.5.0

© 2026 АО "Лаборатория Касперского"

Содержание

Kaspersky Endpoint Security для Linux

О приложении

- Ключевые возможности
- Что нового в версии 12.5
- Исправленные ошибки
- Аппаратные и программные требования
- Комплект поставки
- Совместимость с другими приложениями
- Сравнение функциональности в зависимости от решений "Лаборатории Касперского"

Развертывание и первоначальная настройка

- Режимы использования и схемы развертывания
- Подготовка среды к установке приложения
- Выбор механизма перехвата системных событий
- Подготовка дистрибутивов
- Подготовительные действия в Kaspersky Security Center
- Установка с помощью Kaspersky Security Center
- Установка с помощью командной строки
- Дополнительная настройка после установки в отдельных ОС
- Сценарий миграции на Kaspersky Security Center Linux с использованием скрипта быстрой установки
- Обновление предыдущей версии приложения
  - Об обновлении плагинов управления Kaspersky Endpoint Security
  - Параметры приложения после обновления версии
- Удаление приложения

Работа с приложением

- Лицензирование
  - Как перейти на другое решение "Лаборатории Касперского"
  - Управление лицензионными ключами
  - Просмотр информации о лицензионных ключах
- Интерфейсы управления приложением
  - Управление через Kaspersky Security Center
    - О политиках Kaspersky Security Center
    - Управление политиками
    - Экспорт и импорт параметров политики
    - О задачах для Kaspersky Endpoint Security, созданных в Kaspersky Security Center
    - Вход и выход из Web Console и Cloud Console
  - Управление через командную строку
    - Локальные задачи Kaspersky Endpoint Security
    - Изменение параметров задач
    - Настройка расписания запуска задач
    - Управление общими параметрами приложения
    - Использование фильтра для ограничения результатов запросов
    - Экспорт и импорт параметров приложения
  - Управление через графический интерфейс

Мониторинг состояния защиты
Статусы постоянной защиты
События и отчеты
Настройка записи событий в журнал операционной системы
Настройка параметров журнала событий приложения
Просмотр событий приложения
Просмотр отчетов
Сбор метрик о состоянии системы
Мониторинг стабильности работы приложения
Проверка целостности компонентов приложения
Управление доступом к приложению
Предустановленные роли
Как назначить или отозвать роль пользователя
Функциональные области RBAC в Kaspersky Security Center
Рекомендации для типовых ролей защищаемых устройств
Обновление баз и модулей приложения
Как выбрать источник и схему распространения обновлений
Как настроить задачу обновления баз
Как выполнить обновление с помощью Kaspersky Update Utility
Как откатить обновление баз и модулей приложения
Защита устройств от угроз
Защита от файловых угроз
Как сформировать область защиты
Как выбрать действие при обнаружении файловой угрозы
Что такое Интеллектуальный режим проверки файлов
Как оптимизировать проверку файлов
Особенности проверки символических и жестких ссылок
Поиск вредоносного ПО
Как сформировать область проверки
Как настроить расписание проверки
Как проверить отдельный файл или директорию
Как оптимизировать запуск задач выборочной проверки
Проверка важных областей
Проверка контейнеров
Как настроить интеграцию с инструментами для управления контейнерами
Как сформировать область проверки контейнеров и образов по требованию
Как оптимизировать проверку контейнеров
Как выбрать действие над контейнером при обнаружении зараженного объекта
Как запустить выборочную проверку контейнеров и образов
Проверка съемных дисков
Анализ поведения
Защита от эксплойтов
Защита от шифрования
Как выбрать действие при обнаружении вредоносного шифрования
Как сформировать область защиты

Защита от атак BadUSB
Как настроить авторизацию USB-устройств
Как разрешить подключение USB-устройств с помощью экранной клавиатуры
Как разрешить подключение USB-устройств с помощью сканера штрихкодов
Защита сетевых соединений и средств коммуникации
Защита от почтовых угроз
Что делать при обнаружении почтовой угрозы
Как оптимизировать проверку вложений в сообщениях электронной почты
Зачем нужен фильтр вложений электронной почты
Защита от веб-угроз
Как выбрать действие при обнаружении веб-угрозы
Что такое Анти-Фишинг
Защита от сетевых угроз
Как выбрать действие при обнаружении сетевой угрозы
Как управлять заблокированными устройствами
Управление сетевым экраном
Как создать сетевое пакетное правило
Примеры использования сетевых пакетных правил
Как добавить IP-адрес в сетевую зону: Публичная, Локальная, Доверенная
Что такое динамические правила
Как создать правила для соединения с Kaspersky Security Center
Контроль безопасности
Контроль устройств
Как управлять списком доверенных устройств в командной строке
Как настроить режим доступа к устройствам
Как настроить правила доступа к устройствам
Как настроить шаблон сообщений Контроля устройств
Предоставление временного доступа к устройству
Веб-Контроль
Как создать правило доступа к веб-ресурсам
Как изменить шаблоны сообщений Веб-Контроля
Правила формирования масок адресов веб-ресурсов
Контроль приложений
Инвентаризация приложений
Как настроить режим работы Контроля приложений
Создание категории приложений
"Золотой образ"
О правилах контроля приложений
Режим тестирования правил контроля приложений
Контроль целостности системы
Контроль целостности системы в реальном времени
Проверка целостности системы
Доверенная зона
Как добавить исключения из защиты
Как добавить доверенные веб-адреса
Как добавить доверенный IP-адрес компьютера
Как выбрать контролируемые сетевые порты

Как добавить сертификат в список доверенных корневых сертификатов
Как добавить доверенный домен
Как исключить точки монтирования
Как добавить доверенные приложения
Как добавить доверенные устройства
Общие настройки
Настройки обнаружения
Kaspersky Security Network
Как включить или выключить использование Kaspersky Security Network
Что такое облачный режим работы приложения
Зачем нужен KSN Proxy
Настройка отправки информации в хранилище Kaspersky Security Center
Как настроить запуск приложения
Настройка разрешений на управление задачами
Защита паролем
О пользовательских разрешениях
Пользовательские разрешения по умолчанию
Настройки производительности
Настройки сети
Как настроить использование прокси-сервера
Как приложение перехватывает трафик
Как настроить политику проверки сертификатов
Как настроить контролируемые порты
Исключения из перехвата трафика средствами операционной системы
Перехват файловых операций
Настройка перехвата системных событий
Настройка дополнительных параметров телеметрии
Резервное хранилище
Защита от сложных угроз и целевых атак
Действия по реагированию
Поиск индикаторов компрометации
Сетевая изоляция
Включение и выключение сетевой изоляции устройства вручную в Web Console
Настройка длительности сетевой изоляции в автоматическом режиме
Настройка параметров сетевой изоляции в ручном режиме
Настройка исключений из сетевой изоляции в Web Console
Помещение файла на карантин
Получение файла с устройства
Удаление файла с устройства
Запуск процесса
Завершение процесса
Запрет запуска объектов
Работа с карантином
Endpoint Detection and Response Optimum
Как включить интеграцию с EDR Optimum
Как проверить, что интеграция с EDR Optimum включена и работает
Cloud Sandbox

- Endpoint Detection and Response Expert (on-premises)
  - Как подготовить эталонный образ для корректной интеграции с EDR Expert (on-premises)
  - Как настроить интеграцию с EDR Expert (on-premises)
  - Как проверить, что интеграция с EDR Expert (on-premises) включена и работает
- Endpoint Detection and Response Expert (cloud)
  - Как настроить интеграцию встроенного агента с EDR Expert (cloud)
  - Как оптимизировать отправку телеметрии EDR Expert (cloud)
  - Как настроить исключения из телеметрии EDR Expert (cloud)
  - Как экспортировать / импортировать фильтры событий EDR Expert (cloud)
- Kaspersky Anti Targeted Attack Platform
  - Как настроить интеграцию с EDR (KATA)
  - Как настроить интеграцию с NDR (KATA)
  - Как проверить, что интеграция с KATA включена и работает
- Sandbox
  - Как настроить интеграцию с Sandbox
  - Как проверить, что интеграция с Sandbox включена и работает
  - Как отправить файл на проверку в Sandbox вручную
- Kaspersky Managed Detection and Response
  - Рекомендации по созданию эталонного образа для корректной интеграции с MDR
  - Загрузка конфигурационного файла KPSN
  - Как настроить интеграцию с MDR
  - Как проверить, что интеграция с MDR включена
- Kaspersky Unified Monitoring and Analysis Platform
  - Как настроить интеграцию с KUMA
  - Как проверить, что интеграция с KUMA включена и работает

Защита виртуальных сред
- Как настроить обнаружение SVM
- Как Легкий агент выбирает SVM
- Как распределить подключение Легких агентов между SVM
- Как защитить соединение между Легким агентом и SVM
- Как узнать статус работы Легкого агента

Лучшие практики
- Оптимизация потребления ресурсов приложением
  - Анализ работы приложения на устройстве
  - Рекомендации для Защиты от файловых угроз и задач проверки
  - Рекомендации для Защиты от веб-угроз и Защиты от сетевых угроз
  - Рекомендации для Анализа поведения
- Совместная работа с решениями "Лаборатории Касперского"
  - Kaspersky Security Center Linux
  - Network Detection and Response (KATA)
  - Kaspersky Unified Monitoring and Analysis Platform

Справочник по компонентам приложения
- Команды управления Kaspersky Endpoint Security
  - Команды управления лицензионными ключами
  - Команды управления пользователями и ролями

Управление параметрами и задачами приложения
Команды управления общими параметрами приложения
Команды управления параметрами задач
Команды управления задачами
Команды управления общими параметрами проверки контейнеров
Команды управления параметрами проверки сетевого трафика
Мониторинг состояния и защиты
Команды статистики
Команда вывода событий
Команды управления событиями приложения
Команда управления сбором метрик о состоянии системы
Контроль безопасности
Команды управления Контролем устройств
Команды управления Контролем приложений
Команды управления Веб-Контролем
Защита сетевых соединений
Команды управления заблокированными устройствами
Команды управления сетевым экраном
Защита от сложных угроз и целевых атак
Команды управления карантином
Команды управления компонентом EDR Expert (on-premises)
Команды управления компонентом EDR Expert (cloud)
Команды управления компонентом NDR (KATA)
Команды управления сетевой изоляцией устройства
Команды управления параметрами интеграции с KUMA
Команды управления параметрами интеграции с Sandbox
Команды управления поиском IOC
Команды приложения в режиме Легкого агента
Параметры приложения в командной строке
Задача Обновление
Защита устройств от угроз
Задача Защита от файловых угроз
Оптимизация проверки сетевых директорий
Поиск вредоносного ПО
Задача Поиск вредоносного ПО
Задача Выборочная проверка
Задача Проверка важных областей
Задача Проверка съемных дисков
Проверка контейнеров
Параметры проверки контейнеров
Задача Проверка контейнеров
Интеграция с Jenkins
Задача Защита от шифрования
Задача Анализ поведения
Защита от эксплойтов

Использование Kaspersky Security Network
Подключение к Kaspersky Security Network
Включение и выключение облачного режима
Задача Защита от атак BadUSB
Защита сетевых соединений и средств коммуникации
Задача Защита от веб-угроз
Проверка сетевого трафика
Просмотр и изменение параметров проверки сетевого трафика
Просмотр исключений из проверки зашифрованных соединений
Управление списком доверенных корневых сертификатов
Настройка и просмотр исключений из перехвата трафика
Задача Защита от сетевых угроз
Управление сетевым экраном
Настройка списка сетевых пакетных правил
Настройка сетевых зон
Контроль безопасности
Задача Контроль устройств
Веб-Контроль
Задача Веб-Контроль
Просмотр и изменение параметров Веб-Контроля
Контроль приложений
Задача Контроль приложений
Создание и изменение списка категорий
Просмотр списка категорий
Настройка списка правил контроля приложений
Настройка инвентаризации
Задача Инвентаризация
Просмотр списка обнаруженных приложений
Задача Контроль целостности системы
Задача Проверка целостности системы
Защита от сложных угроз и целевых атак
Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)
Параметры интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises)
Управление сертификатами для подключения к серверам OSMP EDR Expert (on-premises)
Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud)
Параметры интеграции с Kaspersky Endpoint Detection and Response Expert (cloud)
Управление сертификатами для подключения к серверам OSMP EDR Expert (cloud)
Интеграция с Kaspersky Endpoint Detection and Response (KATA)
Параметры интеграции с Kaspersky Endpoint Detection and Response (KATA)
Управление сертификатами для подключения к серверу KATA
Интеграция с Kaspersky Network Detection and Response (KATA)
Параметры интеграции с Kaspersky Network Detection and Response (KATA)
Управление сертификатами для подключения к серверу NDR
Интеграция с Sandbox
Параметры интеграции с Sandbox
Управление сертификатами для подключения к серверу Sandbox
Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum

Настройка интеграции с Kaspersky Managed Detection and Response
Управление сетевой изоляцией устройства
Настройка параметров карантина
Работа с файлами карантина в командной строке
Поиск индикаторов компрометации
Управление запретом запуска объектов
Настройка интеграции с KUMA
Задача Интеграция с Kaspersky Unified Monitoring and Analysis Platform
Управление сертификатами для подключения к серверу KUMA
Общие параметры
Общие параметры приложения
Расписание задач
Настройка параметров прокси-сервера
Настройка параметров резервного хранилища
Параметры проверки сетевого трафика
Настройка глобальных исключений
Параметры защиты паролем
Параметры приложения в Консоли администрирования
Обновление баз
Защита устройств от угроз
Защита от файловых угроз
Окно Области проверки
Окно Новая область проверки
Окно Параметры проверки
Окно Действия при обнаружении угрозы
Исключения Защиты от файловых угроз
Окно Области исключения
Окно Новая область исключения
Окно Исключения по маске
Окно Исключения по названию угрозы
Окно Исключения по процессам
Окно Доверенный процесс
Поиск вредоносного ПО
Окно Области проверки
Окно <Новая область проверки>
Окно Параметры области проверки
Окно Области проверки
Окно Параметры проверки
Окно Действия при обнаружении угрозы
Раздел Исключения
Окно Области исключения
Окно Новая область исключения
Окно Исключения по маске
Окно Исключения по названию угрозы
Проверка важных областей
Окно Области проверки
Окно Новая область проверки

Окно Параметры области проверки
Окно Области проверки
Окно Параметры проверки
Окно Действия при обнаружении угрозы
Раздел Исключения
Окно Области исключения
Окно Новая область исключения
Окно Исключения по маске
Окно Исключения по названию угрозы
Мониторинг контейнеров
Окно Параметры проверки контейнеров
Проверка контейнеров
Окно Параметры проверки контейнеров
Окно Параметры проверки
Окно Действия при обнаружении угрозы
Раздел Исключения
Окно Исключения по маске
Окно Исключения по названию угрозы
Проверка съемных дисков
Анализ поведения
Окно Исключения по процессам
Окно Доверенный процесс
Защита от эксплойтов
Окно Исключения Защиты от эксплойтов
Окно Исключение Защиты от эксплойтов
Защита от шифрования
Окно Области проверки
Окно Новая область проверки
Окно Параметры защиты
Окно Области исключения
Окно Новая область исключения
Окно Исключения по маске
Kaspersky Security Network
Параметры Kaspersky Security Network
Положение о Kaspersky Security Network
Положение о Kaspersky Private Security Network
Защита от атак BadUSB
Защита сетевых соединений и средств коммуникации
Защита от почтовых угроз
Окно Параметры защиты от почтовых угроз
Окно Фильтр вложений
Защита от веб-угроз
Окно Доверенные веб-адреса
Окно Параметры проверки
Защита от сетевых угроз
Окно Исключения

Управление сетевым экраном
Окно Сетевые пакетные правила
Окно Добавление сетевого пакетного правила
Окно Добавление IP-адресов
Окно Доступные сети
Окно Сетевое соединение
Контроль безопасности
Контроль устройств
Окно Доверенные устройства
Окно Доверенное устройство (Идентификатор устройства)
Окно Устройства на клиентских устройствах
Окно Список устройств на основе событий Контроля устройств
Окно Доступ к доверенному устройству
Окно Пользователь или группа
Окно Тип устройства
Окно Настройка правила доступа к устройствам
Окно Пользователь или группа
Окно Расписание доступа
Окно Шины подключения
Веб-Контроль
Окно Правило Веб-Контроля
Окно Выбор категорий содержания
Окно Выбор категорий типов данных
Окно Выбор адресов
Окно Выбор групп адресов
Окно Добавление группы адресов
Окно Выбор пользователей
Окно Пользователь или группа
Окно Расписание доступа
Контроль приложений
Окно Правила Контроля приложений
Окно Добавление правила
Окно Категории приложений
Окно Пользователь или группа
Инвентаризация
Окно Области проверки
Окно Новая область проверки
Раздел Исключения
Окно Области исключения
Окно Новая область исключения
Контроль целостности системы
Окно Области проверки
Окно Новая область проверки
Окно Области исключения
Окно Новая область исключения
Окно Исключения по маске

Проверка целостности системы
Окно Области проверки
Окно Новая область проверки
Раздел Исключения
Окно Области исключения
Окно Новая область исключения
Окно Исключения по маске
Локальные задачи
Управление задачами
Защита от сложных угроз и целевых атак
Интеграция с Kaspersky Managed Detection and Response
Интеграции с Kaspersky Endpoint Detection and Response (on-premises)
Настройка подключения к серверам KATA
Настройка общих параметров подключения к серверам KATA
Настройка параметров передачи данных на серверы KATA
Интеграция с Kaspersky Network Detection and Response (KATA)
Настройка подключения к серверам NDR
Настройка общих параметров подключения к серверам NDR
Настройка параметров передачи данных на серверы NDR
Интеграция с KUMA
Окно Серверы KUMA
Окно Сервер KUMA
Окно Параметры подключения к серверам KUMA
Окно добавления сертификата сервера
Окно добавления сертификата клиента
Карантин
Запрет запуска объектов
Общие параметры
Прокси-сервер
Окно Исключения для прокси-сервера
Потребление ресурсов процессора для задач проверки
Запуск задач при работе от аккумулятора
Запуск приложения
Автоматический перезапуск при получении критических обновлений
Защита паролем
Параметры трассировки и записи дампов
Использование резидентной памяти приложением
Проверка зашифрованных соединений
Окно Доверенные домены
Окно Доверенные корневые сертификаты
Окно Исключения из перехвата трафика
Окно Исключение из перехвата трафика
Окно Контролируемые порты
Глобальные исключения
Окно Путь к точке монтирования
Исключение памяти процессов из проверки
Резервное хранилище

Обнаружение приложений, которые злоумышленники могут использовать для нанесения вреда
Перехват файловых операций
Отправка информации в хранилище Kaspersky Security Center
Перехват системных событий
Дополнительные параметры телеметрии
Режим Легкого агента
Подключение к Серверу интеграции
Окно Подключение к Серверу интеграции
Окно Проверка сертификата Сервера интеграции
Окно Аутентификация на Сервере интеграции
Параметры обнаружения SVM
Тег для подключения к SVM
Алгоритм выбора SVM
Защита соединения
Известные проблемы и ограничения
Обращение в Службу технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Получение информации для Службы технической поддержки
Как включить и настроить создание файла трассировки
Как включить и настроить запись дампов
Удаленная диагностика устройства с помощью Kaspersky Security Center
Приложения
Приложение 1. Конфигурационные файлы и параметры приложения по умолчанию
Правила редактирования конфигурационных файлов задач приложения
Конфигурационные файлы первоначальной настройки
Параметры первоначальной настройки в инсталляционном пакете
Предустановленные конфигурационные файлы
Параметры задач командной строки по умолчанию
Параметры по умолчанию задачи File_Threat_Protection (ID:1)
Параметры по умолчанию задачи Scan_My_Computer (ID:2)
Параметры по умолчанию задачи Scan_File (ID:3)
Параметры по умолчанию задачи Critical_Areas_Scan (ID:4)
Параметры по умолчанию задачи Update (ID:6)
Параметры по умолчанию задачи System_Integrity_Monitoring (ID:11)
Параметры по умолчанию задачи Firewall_Management (ID:12)
Параметры по умолчанию задачи Anti_Cryptor (ID:13)
Параметры по умолчанию задачи Web_Threat_Protection (ID:14)
Параметры по умолчанию задачи Device_Control (ID:15)
Параметры по умолчанию задачи Removable_Drives_Scan (ID:16)
Параметры по умолчанию задачи Network_Threat_Protection (ID:17)
Параметры по умолчанию задач Container_Scan (ID:18) и Custom_Container_Scan (ID:19)
Параметры по умолчанию задачи Behavior_Detection (ID:20)
Параметры по умолчанию задачи Application_Control (ID:21)
Параметры по умолчанию задачи Inventory_Scan (ID:22)
Параметры по умолчанию задачи KATAEDR (ID:24)
Параметры по умолчанию задачи Web_Control (ID:26)
Параметры по умолчанию задачи Standalone_Sandbox (ID:29)

Параметры по умолчанию задачи KATANDR (ID:31)
Параметры по умолчанию задачи KUMA (ID:33)
Параметры по умолчанию задачи Защита от почтовых угроз (ID: 35)
Параметры по умолчанию задачи Защита от атак BadUSB (ID:37)
Параметры по умолчанию задачи KATANDR (ID:31)
Приложение 2. Настройка совместной работы с Антивирусом Касперского для Linux Mail Server
Приложение 3. Параметры для взаимодействия с внешними службами
Приложение 4. Расширения файлов для быстрой проверки съемных дисков
Приложение 5. Переменные в шаблонах сообщений
Приложение 6. События в работе приложения
Критическое
Предупреждение
Информационное сообщение
Приложение 7. Коды возврата
Приложение 8. Подготовка архива с базами приложения
Приложение 9. Требования к IOC-файлам
Юридическая информация
Предоставление данных
Данные, предоставляемые при использовании кода активации
Данные, предоставляемые при загрузке обновлений с серверов обновлений "Лаборатории Касперского"
Данные, передаваемые при использовании приложения в режиме Легкого агента
Данные, передаваемые приложению Kaspersky Security Center
Данные, предоставляемые при переходе по ссылкам из интерфейса приложения
Данные, предоставляемые при использовании Kaspersky Security Network
Данные, предоставляемые при интеграции с решением Kaspersky Endpoint Detection and Response Optimum
Данные, предоставляемые при интеграции с компонентом Kaspersky Endpoint Detection and Response (KATA)
Данные, предоставляемые при интеграции с компонентом Kaspersky Endpoint Detection and Response Expert (on-premises)
Данные, предоставляемые при интеграции с компонентом Kaspersky Endpoint Detection and Response Expert (cloud)
Данные, предоставляемые при интеграции с компонентом Kaspersky Network Detection and Response (KATA)
Данные, предоставляемые при интеграции с решением Kaspersky Unified Monitoring and Analysis Platform
Информация о стороннем коде
Уведомления о товарных знаках

Kaspersky Endpoint Security для Linux

Обзор

Kaspersky Endpoint Security для Linux

Что нового в версии 12.5

Типовые схемы развертывания

Сравнение функциональности

Известные проблемы и ограничения

Быстрый старт

Аппаратные и программные требования

Совместимость

Подготовка дистрибутивов

Подготовка среды к установке

Развертывание приложения

Сценарий миграции на Kaspersky Security Center Linux

Работа с приложением

Активация

Обновление баз

Обновление с помощью Kaspersky Update Utility

Защита от файловых угроз

Доверенная зона

Оптимизация ресурсов

Работа в командной строке

Управление приложением через командную строку

Команды управления

Параметры приложения в командной строке

Поддержка

Мониторинг состояния защиты

Обновление предыдущей версии приложения

Обращение в Службу технической поддержки

О приложении

Kaspersky Endpoint Security для Linux обеспечивает современную комплексную защиту устройств с операционными системами Linux и позволяет предотвращать, обнаруживать и реагировать на различного вида угрозы, сетевые и мошеннические атаки. Приложение входит в состав многих мультиплатформенных решений "Лаборатории Касперского" и гибко настраивается в зависимости от задач в IT-инфраструктуре вашей организации.

Управлять приложением Kaspersky Endpoint Security, установленном на защищаемых устройствах, вы можете как локально, так и централизованно с помощью Kaspersky Security Center.

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

Ключевые возможности

Защита от массовых киберугроз

Защита на основе передовых технологий – фундамент вашей IT-безопасности. Kaspersky Endpoint Security позволяет избежать заражения файловой системы устройств пользователей, контролирует подключение съемных дисков к устройству и проверяет их на наличие вирусов. Контролирует вредоносную активность приложений и защищает файлы от удаленного вредоносного шифрования. Базы с информацией о новых глобальных угрозах – вирусах, троянах, шифровальщиках, хакерских атаках – обновляются регулярно и автоматически.

Защита сетевых соединений и средств коммуникации

Kaspersky Endpoint Security надежно защищает сетевое окружение вашей организации: проверяет почту, сайты и скачиваемые файлы на наличие вирусов, сетевых червей и других угроз, прежде чем вы их открываете. Приложение позволяет проверять входящий сетевой трафик на действия, характерные для сетевых атак, контролирует параметры сетевого экрана операционной системы и фильтрует сетевую активность.

Контроль безопасности на рабочем месте

Контролируя с помощью Kaspersky Endpoint Security доступ пользователей к приложениям, веб-ресурсам и подключаемым устройствам на рабочих местах, вы обеспечиваете еще один уровень безопасности в вашей организации. Это позволяет защитить устройства от заражения и предотвратить потерю или утечку данных.

Защита от сложных угроз и целевых атак

Приложение может взаимодействовать с решениями Detection and Response от "Лаборатории Касперского": Kaspersky Managed Detection and Response (MDR) и Kaspersky Anti Targeted Attack Platform (KATA). Также поддерживается работа с SIEM-решением Kaspersky Unified Monitoring and Analysis Platform (KUMA). Kaspersky Endpoint Security наблюдает за процессами, запущенными на устройствах пользователей, открытыми сетевыми соединениями и изменяемыми файлами. Взаимодействие с Detection and Response решениями обеспечивает защиту от таких угроз, как эксплойты, программы-вымогатели, бесфайловые атаки и использование злоумышленниками законных системных инструментов для нанесения вреда устройствам или данным.

Защита виртуальных и облачных сред

Kaspersky Endpoint Security в составе решения Kaspersky Security для виртуальных сред Легкий агент обеспечивает защиту виртуальных машин с гостевыми операционными системами Linux на различных платформах виртуализации серверов и платформах VDI. Проверку объектов на вирусы выполняет специальный компонент, установленный на отдельную виртуальную машину – SVM (Secure Virtual Machine). Таким образом, для обеспечения безопасности приложение использует ресурсы SVM, а не ресурсы виртуальной машины, что вместе с интеллектуальной оптимизацией (например, использование общего кеша) минимизирует общую нагрузку на IT-инфраструктуру.

Что нового в версии 12.5

В Kaspersky Endpoint Security 12.5 для Linux появились следующие возможности и доработки:

- Поддержана возможность установки приложения Kaspersky Endpoint Security 12.5 для Linux на устройства с процессорами Эльбрус. Работа приложения на процессорах Эльбрус поддерживается с ограничениями.

- Реализована возможность интеграции с Kaspersky Endpoint Detection and Response Expert (cloud) – облачным решением, предназначенным для защиты IT-инфраструктуры организации от сложных киберугроз, в том числе тех, которые не могут быть обнаружены EPP-приложениями, установленными на корпоративных активах. Решение обеспечивает полную видимость, корреляцию и автоматизацию, используя широкий спектр инструментов реагирования и источников данных, включая активы конечных точек, данные сети и облачного окружения, что обеспечивает единый процесс обнаружения и реагирования с помощью интегрированных компонентов и целостных сценариев в едином интерфейсе для повышения эффективности специалистов по безопасности.

  Интеграция Kaspersky Endpoint Security для Linux с решением Kaspersky Endpoint Detection and Response Expert (cloud) временно недоступна до запуска этого решения, который запланирован на конец 2026 года. После чего ожидается, что интеграция будет доступна для данной версии Kaspersky Endpoint Security без необходимости дополнительного обновления.

- Реализована возможность защитить паролем выполнение действий с приложением Kaspersky Endpoint Security. Защита паролем позволяет ограничить действия, которые пользователи могут выполнять с приложением Kaspersky Endpoint Security в соответствии с предоставленными разрешениями. Ограничение доступа к настройкам приложения снижает риск несанкционированных или непреднамеренных изменений в приложении.

- Доработан компонент Контроль устройств. Добавлена возможность экспортировать список доверенных устройств в файл и импортировать из файла.

- Доработан компонент Защита от атак BadUSB. Теперь при подключении сканера штрихкода вы можете отсканировать штрихкод с экрана для авторизации сканера, а не вводить код авторизации для разблокировки устройства.

- Доработан обновляемый модуль ядра (ULKM):
  - Добавлена поддержка режима перехвата системных событий на основе обновляемого модуля ядр (ULKM), для систем с включенным Secure Boot.
  - Расширен список операционных систем, на которых приложение может использовать механизм перехвата обновляемого модуля ядра.
  - Добавлена поддержка обновляемого модуля ядра для компонентов Защиты от шифрования и Контроля устройств.
- Доработан процесс установки приложения в операционной системе Astra Linux Special Edition в режиме замкнутой программной среды. Теперь при наличии установленного пакета совместимости пользователю не нужно вручную выполнять дополнительные действия, чтобы запустить приложение Kaspersky Endpoint Security после установки на устройство с операционной системой Astra Linux Special Edition.
- Добавлена возможность при установке приложения изменять параметры конфигурационного файла kesl.ini с помощью конфигурационного файла autoinstall.ini.
- Улучшена диагностика ошибок при установке и удалении приложения:
  - детализированы коды возврата для более четкого понимания возникшей проблемы;
  - добавлены сообщения об отсутствующих зависимостях (внешних библиотеках, компонентах, утилитах или других программах), необходимых для установки и корректной работы приложения;
  - добавлены сообщения о неправильно настроенных правах доступа к системным директориям;
  - добавлены и уточнены тексты ошибок, отображающихся в Kaspersky Security Center;
  - добавлена возможность включить режим игнорирования ошибок пакетного менеджера при установке приложения.
- Реализован автоматический перезапуск приложения при установке после первого обновления баз и модулей приложения. Добавлена возможность настроить автоматический перезапуск приложения при получении критически важных обновлений по истечении первых суток после установки приложения. Вы можете настроить автоматический перезапуск приложения с помощью командной строки в общих параметрах приложения или в свойствах политики с помощью Web Console или Консоли администрирования.
- Добавлена возможность управлять кешем событий при интеграции с решениями Detection and Response с помощью параметра `UseIncreasedXdrEventsCache` из конфигурационного файла kesl.ini. Вы можете выбрать между высокой производительностью и объемом используемой оперативной памяти.
- Добавлена возможность ускоренного завершения процесса kesl при остановке или перезапуске приложения с помощью параметра `FastShutdown` из конфигурационного файла kesl.ini, что позволяет оперативно восстанавливать работу приложения на системах с высокой нагрузкой и предотвращать избыточное потребление ресурсов.
- Добавлена возможность настроить ограничение памяти, потребляемой компонентом Анализ поведения на обработку очереди событий, с помощью параметра `ReduceSWMemoryConsumption` из конфигурационного файла kesl.ini. Использование данного параметра может влиять на качество защиты. Обязательно ознакомьтесь с документацией.

- Улучшена стабильность сетевого доступа. Теперь в случае аварийного завершения процесса kesl, Watchdog-сервер удаляет правила сетевого экрана, добавляемые приложением при запуске компонентов Защита от веб-угроз и Защита от сетевых угроз, что позволяет избежать потери интернет-соединения и быстрее восстановить сетевой доступ на устройстве.

- Добавлена возможность запрещать одновременный запуск задач проверки для оптимизации работы приложения. Теперь при включенном запрете в случае одновременного запуска задач проверки задачи ставятся в очередь.

- В исключения Защиты от файловых угроз добавлена обработка символических ссылок. Теперь пути преобразуются в конечные адреса файлов.

- Реализовано включение и настройка директории файлов дампов через команду изменения общих параметров приложения без перезагрузки приложения. Эти параметры для настройки файлов дампов удалены из конфигурационного файла kesl.ini.

- Реализована обязательность пароля при интеграции с решениями Kaspersky Endpoint Detection and Response Expert (on-premises), Kaspersky Anti Targeted Attack Platform и Kaspersky Unified Monitoring and Analysis Platform. Теперь при настройке интеграции для клиентского сертификата требуется указывать пароль.

- Добавлена возможность сжимать трафик при интеграции с решением Kaspersky Unified Monitoring and Analysis Platform во время передачи событий телеметрии, что снижает нагрузку на каналы связи.

- Обновлен список поддерживаемых операционных систем, в том числе добавлена поддержка 64-битных операционных систем CentOS версий 5.2, 5.4, 6.4 и 6.6.

- Добавлены языки локализации интерфейса приложения: испанский (Мексика) и португальский (Бразилия).

Что было нового в предыдущих версиях

Версия 12.4

В приложении Kaspersky Endpoint Security 12.4 для Linux появились следующие возможности и доработки:

- Добавлен новый функциональный компонент Защита от почтовых угроз. Компонент проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других приложений, представляющих угрозу.

- Добавлен новый функциональный компонент Защита от атак BadUSB. Компонент позволяет предотвратить подключение к клиентскому устройству зараженных USB-устройств, имитирующих клавиатуру.

- Доработан компонент Контроль устройств. Добавлена возможность предоставить по запросу пользователя временный доступ к заблокированным устройствам.

- Доработан компонент Защита от эксплойтов. Добавлена возможность настраивать исключения объектов из проверки компонентом.

- Доработан обновляемый модуль ядра:
  - Теперь обновляемый модуль ядра позволяет оптимизировать перехват файловых операций. Производительность приложения увеличивается за счет использования кеша файлов и процессов, не нуждающихся в проверке.
  - Теперь при использовании обновляемого модуля ядра вы можете более точно настраивать глобальные исключения. Если используется механизм перехвата на основе технологии fanotify, из перехвата файловых операций исключаются указанные точки монтирования целиком. Использование обновляемого модуля ядра позволяет исключать конкретные локальные или удаленные директории, смонтированные на устройстве.
- Компонент EDR (KATA), обеспечивающий интеграцию с Kaspersky Endpoint Detection and Response (KATA), переименован в EDR Expert (on-premises). Компонент также обеспечивает интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premises). Задача интеграции переименована в *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* (KATAEDR, ID:24).
- Реализована возможность интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) – решением для кибербезопасности бизнеса, позволяющим защититься от большинства киберрисков и покрыть основные сценарии распространения угроз. Компоненты Kaspersky Endpoint Detection and Response Expert (on-premises) развертываются на единой платформе управления Open Single Management Platform (OSMP). Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises) поддерживает все возможности интеграции с компонентом Kaspersky Endpoint Detection and Response (KATA), а также содержит новые возможности:
  - Запуск YARA-проверки. *YARA-проверка* – процесс, в ходе выполнения которого Kaspersky Endpoint Security использует YARA-файлы для поиска сигнатур вредоносной активности на устройстве.
  - Сбор форензики – цифровых данных, которые могут быть полезны при расследовании инцидентов, связанных с киберпреступлениями и утечками данных.
  - Отправка расширенных данных о событиях на устройствах (телеметрии) на сервер сбора телеметрии на платформе OSMP.
  - Отправка только телеметрии с индикатором атаки (Indicator of Attack, IOA) и поддержка пользовательских фильтров, заданных в политике в Web Console.
  - Активация компонента EDR Expert (on-premises), обеспечивающего интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises) и с Kaspersky Endpoint Detection and Response (KATA), путем добавления лицензионного ключа.
  - Выбор режима интеграции в параметрах задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* в командной строке или в свойствах политики в Web Console.
- Реализована возможность использования приложения в режиме Агента Endpoint Detection and Response для совместной работы на защищаемых устройствах решений Detection and Response от "Лаборатории Касперского" и антивирусных приложений от сторонних поставщиков. В этом режиме для защиты устройства не используются стандартные компоненты защиты и контроля Kaspersky Endpoint Security. Стандартную защиту устройства обеспечивает приложение от стороннего поставщика.
- Добавлена возможность создавать файлы трассировки приложения при первом запуске после его установки. Теперь вы можете включить создание файлов трассировки при первом запуске приложения в Web Console, в Консоли администрирования или в параметрах конфигурационного файла первоначальной настройки.
- Обновлен интерфейс политики в Web Console. Изменилась структура разделов в политике, чтобы быстрее находить нужные функции.

- Добавлена возможность выбрать режим перехвата трафика, который приложение использует в своей работе: использование технологии eBPF или использование утилиты iptables.

- Добавлена возможность выбрать источник телеметрии (только eBPF или eBPF и auditd). Для auditd вы также можете выбрать режим работы (монопольный режим или режим многоадресной рассылки).

- Реализована возможность выбрать режим отправки файлов и директорий на проверку в Sandbox: вручную, только автоматический, автоматический и ручной.

- Расширены возможности приложения при использовании в режиме Легкого агента:

  - Доступен механизм перехвата системных событий на основе обновляемого модуля ядра.

  - Доступен функциональный компонент Защита от эксплойтов.

  - Повышен уровень обнаружения угроз.

- Добавлена возможность использовать Kaspersky Private Security Network (KPSN) напрямую без помощи службы прокси-сервера KSN на Сервере администрирования.

- Добавлена возможность создавать политики для автономных пользователей в Web Console и Консоли администрирования. Политики для автономных пользователей действуют при выходе устройства из сети организации.

- При просмотре и экспорте списка точек монтирования в Web Console и в Консоли администрирования, а также при просмотре в командной строке, добавилось отображение информации о том, что точка монтирования обнаружена в пространстве имен.

- Доработан альтернативный механизм получения системной телеметрии в компоненте Анализ поведения на 64-битных операционных системах с версией ядра 4.18 и выше с поддержкой eBPF, который позволяет освободить ресурсы подсистемы аудита ядра auditd.

- Добавлена возможность включать в данные телеметрии при интеграции с Kaspersky Managed Detection and Response следующую информацию:

  - признак того, что событие произошло в контейнере;

  - идентификатор пространства имен контейнера;

  - имя контейнера.

- Обновлен список поддерживаемых операционных систем.

Версия 12.3

В приложении Kaspersky Endpoint Security 12.3 для Linux появились следующие возможности и доработки:

- Реализован механизм перехвата системных событий на основе обновляемого модуля ядра (недоступно в режиме Легкого агента). Если операционная система на устройстве поддерживает технологию fanotify и соответствует другим требованиям для установки обновляемого модуля ядра, вы можете настроить использование обновляемого модуля ядра в работе приложения. Использование обновляемого модуля ядра позволяет оптимизировать перехват запуска процессов приложением Kaspersky Endpoint Security. Обновляемый модуль ядра входит в комплект поставки приложения.

- За счет использования обновляемого модуля ядра улучшена работа компонента Защита от шифрования (недоступно в режиме Легкого агента). Теперь приложение может обнаруживать больше видов программ-шифровальщиков.

- Добавлен новый функциональный компонент Защита от эксплойтов (недоступно в режиме Легкого агента). Компонент отслеживает программный код, использующий уязвимости на устройстве для получения эксплойтом прав администратора или выполнения вредоносных действий.

- Доработан компонент Контроль устройств:

  - Добавлена возможность настроить список пользователей или групп пользователей, для которых добавленные устройства будут доверенными.

  - Добавлена возможность разрешать доступ к устройствам хранения данных только на чтение.

  - Улучшено информирование пользователя с помощью событий за счет добавления новых событий, уточнения и унификации текстов событий в плагинах и в командной строке.

- Расширены возможности интеграции с решением Kaspersky Managed Detection and Response:

  - Реализована возможность сетевой изоляции устройства.

  - Реализована возможность помещения файлов на карантин и восстановления файлов из карантина.

  - Реализована возможность запуска процесса и завершения процесса.

- Добавлена возможность активировать компонент MDR, обеспечивающий интеграцию с Kaspersky Managed Detection and Response, путем добавления лицензионного ключа.

- Доработан компонент Анализ поведения. Добавлена возможность настроить исключение процесса из проверки при работе компонентов MDR и EDR (KATA).

- Реализована возможность настраивать исключения при использовании прокси-сервера. Теперь вы можете указать компоненты приложения Kaspersky Endpoint Security, в работе которых не будет использоваться прокси-сервер, а также сформировать список адресов, для подключения к которым не будет использоваться прокси-сервер. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается использование прокси-сервера для подключения к Kaspersky Security Network, к SVM и к Серверу интеграции.

- Добавлена возможность настраивать исключения из перехвата трафика. Теперь вы можете указывать соединения, которые приложение будет исключать из перехвата трафика, с помощью плагинов управления приложением и с помощью командной строки.

- Добавлена возможность временно исключить из проверки файлы журналов баз данных для оптимизации их проверки Защитой от файловых угроз. Если файл журнала баз данных повторно используется тем же процессом в течение 10 минут после последней проверки, приложение не будет проверять этот файл журнала.

- Реализована возможность включить объединение элементов списков исключений в родительской и дочерней политиках при наследовании параметров родительской политики.

- В веб-плагине управления приложением добавлена возможность экспорта и импорта списков исключений в политике и задачах.

- Добавлена возможность настраивать параметры первоначальной настройки приложения Kaspersky Endpoint Security в Консоли администрирования Kaspersky Security Center при создании инсталляционного пакета или в свойствах инсталляционного пакета.

- Добавлена возможность настраивать отмену запуска запланированных задач на устройстве, работающем от аккумулятора.

- Реализована возможность включать и выключать использование прокси-сервера KSN при взаимодействии приложения Kaspersky Endpoint Security с серверами KSN (недоступно в режиме Легкого агента). Если использование прокси-сервера KSN включено, Kaspersky Endpoint Security взаимодействует с серверами KSN с помощью службы прокси-сервера KSN на Сервере администрирования. Если использование прокси-сервера KSN выключено, Kaspersky Endpoint Security взаимодействует с серверами KSN напрямую.

- В командной строке реализована команда, которая выводит список функций приложения, информацию об их статусах (используется или не используется) и технологиях Linux, с помощью которых реализованы эти функции приложения.

- Добавлена возможность отображать в командной строке и в графическом интерфейсе информацию о действующей на устройстве политике и профилях политики.

- Реализована возможность установить приложение с помощью командной строки на устройстве, где отсутствует интерпретатор языка Perl.

- Доработан перехват трафика. Теперь локальный трафик (трафик между процессами, находящими на одном устройстве) не перехватывается.

- Реализована возможность передавать необходимые параметры для отправки телеметрии при интеграции с Kaspersky Managed Detection and Response без использования конфигурационного файла KPSN. Если вы используете инфраструктурное решение Kaspersky Security Network или у вас есть только корневой тенант, то для интеграции приложения Kaspersky Endpoint Security с Kaspersky Managed Detection and Response конфигурационный файл KPSN не требуется.

- Оптимизировано хранение большого количества событий в журнале событий приложения. Увеличена скорость взаимодействия с базой данных событий при ее открытии и закрытии, а также при получении событий.

- Доработан графический интерфейс приложения (если приложение используется в режиме Легкого агента, графический интерфейс не поддерживается):

  - Добавлена возможность включать и выключать компонент Веб-Контроль.

  - Переработан стиль графического интерфейса (изменены цвета, добавлены скругления углов всех окон).

- Изменены названия действий над зараженными объектами в параметрах Защиты от файловых угроз и задачах проверки.

- Добавлен альтернативный механизм получения системной телеметрии в компоненте Анализ поведения на 64-битных операционных системах (с версией ядра 5.3 и выше с поддержкой eBPF), который позволяет освободить ресурсы подсистемы аудита ядра auditd. Приложение будет работать с eBPF автоматически, если операционная система удовлетворяет указанным требованиям, в том числе при использовании в режиме Легкого агента.

- Отображение даты и времени во всех интерфейсах управления приложением (за исключением командной строки) приведено к единому формату, определенному в RFC 3339, вида 2023-12-25 23:55:59.

- Обновлен список поддерживаемых операционных систем.

Версия 12.2

В приложении Kaspersky Endpoint Security 12.2 для Linux появились следующие возможности и доработки:

- Реализована возможность интеграции с Kaspersky Network Detection and Response (KATA) – компонентом решения Kaspersky Anti Targeted Attack Platform, – что обеспечивает защиту внутренней сети предприятия и позволяет отправлять данные о событиях на устройствах (телеметрию) на сервер Kaspersky Anti Targeted Attack Platform с компонентом Central Node (далее также сервер NDR).

- Реализована возможность интеграции с KATA Sandbox – компонентом решения Kaspersky Anti Targeted Attack Platform, – что позволяет выполнять анализ и проверку объектов для выявления вредоносной активности и признаков целевых атак на ИТ-инфраструктуру организации на специальных серверах с развернутыми виртуальными образами операционных систем.

- Реализована возможность интеграции с Kaspersky Unified Monitoring and Analysis Platform – комплексным программным решением, сочетающем в себе следующие функциональные возможности: получение, обработка и хранение событий информационной безопасности; анализ и корреляция поступающих данных; поиск по полученным событиям и создание уведомлений о выявлении признаков угроз информационной безопасности.

- Расширены возможности интеграции с Kaspersky Endpoint Detection and Response (KATA) – компонентом решения Kaspersky Anti Targeted Attack Platform:

  - Реализована функциональность запрета запуска объектов.

  - Реализована возможность помещения файлов на карантин.

  - Расширены данные о событиях на устройствах (телеметрии).

- Расширены возможности интеграции с решением Endpoint Detection and Response Optimum:

  - Реализована функциональность запрета запуска объектов.

  - Реализована возможность помещения файлов на карантин.

  - Реализована возможность исключения процесса из сетевой изоляции по его имени.

- Добавлена возможность применения технологии Cloud Sandbox, которая позволяет обнаруживать на устройстве сложные угрозы. Приложение Kaspersky Endpoint Security автоматически отправляет обнаруженные файлы в Cloud Sandbox для анализа. Cloud Sandbox запускает эти файлы в изолированной среде для выявления вредоносной активности и принимает решение о репутации этих файлов.

- Реализована возможность просматривать статистику о наиболее часто проверяемых файлах и приложениях, а также список точек монтирования, обнаруженных на защищаемом устройстве. Теперь для улучшения производительности вы можете добавить в исключения из проверки файлы, которые наиболее часто проверяет компонент Защита от файловых угроз, и пути к приложениям, которые наиболее часто проверяет компонент Анализ поведения, а также обнаруженные на устройстве точки монтирования.

- Добавлена возможность сбора метрик, связанных с производительностью приложения и позволяющих проанализировать влияние работы приложения Kaspersky Endpoint Security на операционную систему.

- Доработан компонент Управление сетевым экраном. Добавлена возможность указать несколько IP-адресов или диапазонов IP-адресов для сетевого пакетного правила.

- Добавлен механизм отслеживания зависаний операционной системы. Механизм проверяет зависание некоторых системных функций, одной из таких функций является функция execve. Процесс Watchdog-сервера wdserver один раз в три секунды запускает еще один процесс wdserver, в котором вызывает эти системные функции (вызов функции execve при этом запускает еще как минимум один процесс wdserver). Если wdserver диагностирует зависание системной функции, Watchdog-сервер перегружает процесс kesl.

- Добавлена возможность настроить отображение всплывающих уведомлений при использовании графического пользовательского интерфейса приложения. Теперь вы можете включать и выключать отображение всплывающих уведомлений в графическом пользовательском интерфейсе с помощью Web Console, Консоли администрирования или командной строки.

- Доработаны параметры расписания задач в командной строке. Теперь вы можете настроить остановку задачи при достижении максимального времени ее выполнения.

- Изменено состояние атрибутов "замок" при создании профиля политики Kaspersky Security Center. Теперь при создании профиля по умолчанию все "замки" открыты, чтобы по умолчанию параметры профиля не преобладали над параметрами "базовой" политики.

- Добавлен альтернативный механизм получения системной телеметрии на 64-битных операционных системах (с версией ядра 5.3 и выше с поддержкой eBPF с BTF), который позволяет освободить ресурсы подсистемы аудита ядра auditd. Приложение будет работать с eBPF автоматически, если операционная система удовлетворяет указанным требованиям.

- Отображение даты и времени во всех плагинах управления приложением приведено к единому формату, определенному в RFC 3339, вида 2023-12-25 23:55:59.

- Обновлен список поддерживаемых операционных систем.

Версия 12.1

В приложении Kaspersky Endpoint Security 12.1 для Linux появились следующие возможности и доработки:

- Реализована возможность интеграции с Kaspersky Endpoint Detection and Response Optimum, что обеспечивает защиту IT-инфраструктуры организации от таких угроз, как эксплойты (англ. exploits), программы-вымогатели (англ. ransomware), бесфайловые атаки (англ. fileless attacks) и использование злоумышленниками законных системных инструментов для нанесения вреда устройствам или данным.

- Реализована возможность добавлять в приложение два активных лицензионных ключа: основной ключ для активации приложения и дополнительный ключ для активации функциональности Kaspersky Endpoint Detection and Response Optimum. Дополнительный ключ требуется, если ваша основная лицензия не включает функциональность Kaspersky Endpoint Detection and Response Optimum.

- Добавлен новый функциональный компонент *Веб-Контроль*, который 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.

- Реализована функция мониторинга стабильности работы Kaspersky Endpoint Security, которая позволяет отслеживать количество нештатных остановок приложения и уведомлять администратора о нестабильной работе приложения.

- Доработана процедура установки Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console: в свойствах инсталляционного пакета приложения теперь можно задавать параметры первоначальной настройки приложения, ранее доступные только в конфигурационном файле autoinstall.ini.

- Расширены возможности управления дополнительными параметрами приложения через Kaspersky Security Center Web Console и Консоль администрирования Kaspersky Security Center: вы можете настраивать параметры, которые ранее можно было настраивать только путем редактирования конфигурационного файла kesl.ini.

- Добавлена возможность включать и выключать использование глобальных исключений и исключений Защиты от файловых угроз при выполнении задач проверки.

- Реализована возможность интеграции с Kaspersky Symphony XDR: если приложение Kaspersky Endpoint Security используется в стандартном режиме, приложение может выполнять действия по реагированию "Запуск поиска вредоносного ПО" и "Обновление баз".

- Реализована передача на Сервер администрирования информации обо всех устройствах, установленных на клиентских устройствах или подключенных к ним (в том числе установленных и подключенных ранее и уже отключенных) при управлении приложением с помощью Kaspersky Security Center.

- Доработаны правила перехвата трафика для поддержки взаимодействия контейнеров в одной сети.

- Обновлен список поддерживаемых операционных систем.

Исправленные ошибки

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

Список ошибок, исправленных в версии 12.5

Идентификатор	Описание
10306343	При проверке статуса действующего лицензионного ключа ошибочно формировались уведомления об удалении и установке лицензионного ключа.
10295949	Не применялись параметры, заданные в действующем профиле политики для компонента Контроль устройств. В результате компонент продолжал работать с параметрами, заданными в политике.
10171454	Если первый источник обновления, указанный в настройках, был недоступен, ошибочно выводилось сообщение о проблеме с обновлением.
10109293	Если выбран режим перехвата сетевого трафика iptables (`NetInterceptorMode=UseIPTables`), некорректно обрабатывался трафик от приложений, открывающих сетевые сокеты с привязкой к конкретному сетевому интерфейсу.
10024219	В Консоли администрирования Kaspersky Security Center некорректно отображался статус обновляемого модуля ядра на управляемых устройствах.
9995631	Некорректная работа ограничения на использование резидентной оперативной памяти приложением (параметр `MaxMemory`) на системах с отключенным swap-разделом. Теперь при достижении установленного лимита выполняется перезапуск Kaspersky Endpoint Security.
9937329	Ошибочно формировались события *Устройство подключено* и *Устройство отключено* на системах с отключенной задачей Контроль устройств (Device_Control).
9934846	На системах с высокой нагрузкой не запускалось приложение. Увеличен тайм-аут ожидания соединения приложения с Watchdog-сервером.
9846405	Ошибочно формировались события *Объект не обработан* на системах с настроенным EFI-загрузчиком.
9815051	Ранее установленные сетевые соединения могли зависать при запуске на управляемых устройствах задач Защита от веб угроз (Web_Threat_Protection) и Защита от сетевых угроз (Network_Threat_Protection) в режиме перехвата сетевого трафика на основе технологии eBPF (`NetInterceptorMode=UseEBPF`). Теперь такие соединения будут разрываться при попытке передачи данных.

Идентификатор	Описание
9807202	На некоторых ОС РОСА при работе с утилитой mkfs.ext2 возникали проблемы с установкой.
9704644	Некорректно отображался статус устройства в случае использования приложения в режиме EDR-агента. Изменено значение статуса защиты устройства в случае использования приложения в режиме EDR-агента Endpoint Detection and Response.
9643969	В некоторых случаях при использовании перехвата сетевого трафика в режиме eBPF могла возникать проблема с сетевой связностью между хостами Scylla.
9633030	Запускалась задача Запрет запуска объектов (EDR Expert (on-premises)) при снятом в политике флажке **Включить запрет запуска объектов**.
9627894	Некорректно работал режим перехвата сетевого трафика на основе технологии eBPF на операционных системах с выключенным протоколом IPv6.
9606448	Возникали проблемы с активацией приложения с использованием Сервера администрирования Kaspersky Security Center в качестве прокси-сервера для доступа к серверам активации "Лаборатории Касперского" (при установленном флажке **Использовать Kaspersky Security Center в качестве прокси-сервера для активации** в политике).
9508605	При включенной интеграции с Kaspersky Endpoint Detection and Response Expert приложение потребляло большое количество памяти на системах с контейнерным окружением.
9456741	Приложение аварийно завершало работу из-за невозможности определить интерпретатор файла при перехвате запуска нового процесса.

Список ошибок, исправленных в веб-плагине версии 6.1

Идентификатор	Описание
9558745	В свойствах политики не отображался параметр **Показывать всплывающие уведомления в графическом пользовательском интерфейсе** для настройки отображения уведомлений в графическом интерфейсе Kaspersky Endpoint Security (**Параметры приложения** → **Общие настройки** → **Настройки уведомлений** → **Дополнительные настройки**).
9622658	При добавлении исключений из Поиска вредоносного ПО по хешу объекта эти исключения не сохранялись.
9798821	При добавлении отдельного веб-сайта в правило Веб-Контроля изменения в политике не сохранялись.
9990129	Отображалось нерелевантное поле **Комментарий** в форме добавления доверенного приложения.
9977884	Отображался нерелевантный переключатель **Уровень безопасности** в настройках компонента Защита от почтовых угроз.
9944635	Дублировалось название флажков **Проверять почтовые базы**. Теперь отображаются корректные названия – **Проверять почтовые базы** и **Проверять файлы почтовых форматов**.
10010439	При создании правил Веб-Контроля некорректно добавлялся назначаемый к правилу пользователь из списка Active Directory.
10218308	Сбрасывался режим использования Kaspersky Security Network при изменении настроек политики.

Аппаратные и программные требования

Минимальные аппаратные требования

Для установки приложения

- Процессор с архитектурой AMD64, частотой 2 ГГц или выше, имеющий два или более ядер, поддерживающий инструкции SSE2.
- Область подкачки не менее 1 ГБ.
- Оперативная память:
  - для 64-битных операционных систем: 2 ГБ оперативной памяти, доступной для приложения;
  - для 32-битных операционных систем: 1 ГБ оперативной памяти, доступной для приложения.
- 4 ГБ свободного места на жестком диске для установки приложения и хранения временных файлов и файлов журналов.

  Для хранения файлов трассировки приложения и файлов дампов приложения требуется дополнительное место на диске.

  Во время проверки архивов и составных объектов Защитой от файловых угроз и задачами проверки также требуется дополнительное место на диске, объем которого зависит от типа и распакованного размера таких объектов при установленных значениях параметров `ScanArchived=Yes` и/или `ScanSfxArchived=Yes` (по умолчанию эти параметры имеют значение `Yes` для задач проверки и `No` для Защиты от файловых угроз).

  Для проверки архивов и составных объектов рекомендуется обеспечить достаточно места в директории /tmp. Также вы можете ограничить размер проверяемых архивов (в нераспакованном виде) с помощью параметра `SizeLimit` для каждой задачи.

Для установки графического интерфейса

- Монитор, обеспечивающий отображение окон шириной 1000 пикселей и высотой 600 пикселей. Если применяется масштабирование экрана, то эти размеры также масштабируются.

Минимальные аппаратные требования для архитектуры Arm

Для установки приложения

- Процессор Armv8.2-A Kunpeng 920 или Armv8-A Baikal-M (BE-M1000) или платформа m-TrusT Терминал.
- Раздел подкачки не менее 1 ГБ.
- 2 ГБ оперативной памяти, доступной для приложения.

- 3 ГБ свободного места на жестком диске для установки приложения и хранения временных файлов и файлов журналов.

  Для хранения файлов трассировки приложения и файлов дампов приложения требуется дополнительное место на диске.

  Во время проверки архивов и составных объектов Защитой от файловых угроз и задачами проверки также требуется дополнительное место на диске, объем которого зависит от типа и распакованного размера таких объектов при установленных значениях параметров `ScanArchived=Yes` и/или `ScanSfxArchived=Yes` (по умолчанию эти параметры имеют значение `Yes` для задач проверки и `No` для Защиты от файловых угроз).

  Для проверки архивов и составных объектов рекомендуется обеспечить достаточно места в директории /tmp. Также вы можете ограничить размер проверяемых архивов (в нераспакованном виде) с помощью параметра `SizeLimit` для каждой задачи.

Для установки графического интерфейса

- Монитор, обеспечивающий отображение окон шириной 1000 пикселей и высотой 600 пикселей. Если применяется масштабирование экрана, то эти размеры также масштабируются.

Минимальные аппаратные требования для архитектуры Эльбрус (E2K)

Для установки приложения

- Процессор v3: Эльбрус-4C, v4: Эльбрус-8C или Эльбрус-1C+.
- Раздел подкачки не менее 2 ГБ.
- 2 ГБ оперативной памяти, доступной для приложения.
- 2 ГБ свободного места на жестком диске для установки приложения и хранения временных файлов и файлов журналов.

Для установки графического интерфейса

- Монитор, обеспечивающий отображение окон шириной 1000 пикселей и высотой 600 пикселей. Если применяется масштабирование экрана, то эти размеры также масштабируются.

Программные требования

Для установки Kaspersky Endpoint Security на устройстве должна быть установлена одна из операционных систем, указанных в таблице.

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

Из-за ограничений технологии fanotify приложение не поддерживает работу со следующими файловыми системами: autofs, binfmt_misc, cgroup, configfs, debugfs, devpts, devtmpfs, gfs2, gvfs, hugetlbfs, mqueue, nfsd, proc, parsecfs, pipefs, pstore, usbfs, rpc_pipefs, securityfs, selinuxfs, sysfs, tracefs.

Файловая защита точек монтирования через технологию FUSE ограничена в использовании без дополнительных действий со стороны администратора операционной системы. Вы можете добавить параметры user_allow_other в файл /etc/fuse.conf и опцию монтирования allow_root для каждой точки монтирования, что позволит приложению следить за файловыми событиями в этих точках монтирования.

64-битные ОС	64-битные ОС для архитектуры Arm	64-битные ОС для архитектуры Эльбрус (E2K)	32-битные ОС
• AlmaLinux OS 8.6, 8.7, 8.8, 8.9. • AlmaLinux OS 9.4, 9.5, 9.6. • AlterOS® 2025. • Amazon™ Linux 2023. • Astra Linux Common Edition 2.12. • Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5, 1.6, 1.7, 1.8). • Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6). • Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6). • Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3). • Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7). Работа операционных систем Astra Linux в режиме Мобильный поддерживается только в десктопном виде. • CentOS 5.2, 5.4, 6.4, 6.6, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9. Работа приложения на устройствах с ОС CentOS 5.2, 5.4, 6.4, 6.6 не поддерживается в решении Kaspersky Endpoint Security Cloud. Работа приложения на устройствах с ОС CentOS 5.2, 5.4, 6.4, 6.6 не поддерживается в Kaspersky Security Center Cloud Console. • CentOS Stream 8, 9, 10. • Debian GNU/Linux 12.8, 12.9, 12.10, 12.11, 12.12, 12.13. • Debian GNU/Linux 13.1, 13.2, 13.3. • EMIAS 1.0. • EulerOS 2.0 SP10. • Fedora Linux 41. • Kylin Desktop OS V10 SP1. • Linux Mint 21.3. • Linux Mint 22.2. • Mostech 12 release 2021.1. • openSUSE Leap 15.6. • Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9. • Oracle Linux 8.5, 8.6, 8.7, 8.8, 8.9. • Oracle Linux 9.4, 9.5, 9.6. • Red Hat Enterprise Linux 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9. • Red Hat Enterprise Linux 8.5, 8.6, 8.7, 8.8, 8.9, 8.10. • Red Hat Enterprise Linux 9.4, 9.5, 9.6. • Red Hat Enterprise Linux 10.0, 10.1. • Rocky Linux 8.6, 8.7, 8.8, 8.9. • Rocky Linux 9.4, 9.5, 9.6. • SberLinux 8.10, 9.1, 9.5, 9.6, 9.7. • SberOS 3.4.0, 3.5.0, 3.6.1. • SUSE Linux Enterprise Server 12.5, 12.6, 12.7. • SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7. • Ubuntu® 24.04 LTS. • Ubuntu 26.04 LTS. • Альт Образование 10, 11. • Альт Рабочая станция 11. • Альт Сервер 11. • Альт СП Рабочая станция релиз 10. • Альт СП Сервер релиз 10. • Атлант, сборка Alcyone, версия 2022.02. • Гослинукс 7.2.	• Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7). • CentOS Stream 9. • EulerOS 2.0 SP10. • SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7. • Ubuntu 26.04 LTS. • Альт Рабочая станция 11.2. • Альт Сервер 11.1. • Альт СП Рабочая Станция релиз 10. • Альт СП Сервер релиз 10. • РЕД ОС 8.0.	• ОС "Эльбрус" 9.3.6. • Astra Linux Special Edition РУСБ.10015-16 (исполнение 2) (очередное обновление 8.1). • Astra Linux Special Edition РУСБ.10265-01 (очередное обновление 8.1). • Альт СП Рабочая станция релиз 8, 10. • Альт СП Сервер релиз 8, 10.	• Debian GNU/Linux 12.8, 12.9, 12.10, 12.11, 12.12, 12.13.

64-битные ОС	64-битные ОС для архитектуры Arm	64-битные ОС для архитектуры Эльбрус (E2K)	32-битные ОС
• М ОС 12 Сервер release 2021.1. • Мос ОС 15.5 Arbat. • МСВСфера 9.5 АРМ. • МСВСфера 9.5 Сервер. • ОС МЭШ 12 Для московских школ для интерактивных панелей (с телеметрией и поддержкой ДИТ) release 2025. • ОС МЭШ 12 Для московских школ для компьютеров и ноутбуков (с телеметрией и поддержкой ДИТ) release 2025. • ОСнова 3.1. • РЕД ОС® 7.3. • РЕД ОС 8.0. • РОСА "Кобальт" 7.9 Рабочая станция. • РОСА "Кобальт" 7.9 Сервер. • РОСА "Хром" 12 Рабочая станция. • РОСА "Хром" 12 Сервер. • СинтезМ-Клиент 8.6. • СинтезМ-Сервер 8.6.			

Дополнительные программные и аппаратные требования для режима Легкого агента

Приложение Kaspersky Endpoint Security может использоваться в качестве Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент версии 6.5. Вы можете посмотреть требования к виртуальным инфраструктурам для работы приложения в режиме Легкого агента в справке Kaspersky Security для виртуальных сред Легкий агент.

Виртуальные машины

К виртуальным машинам, на которых устанавливается Kaspersky Endpoint Security в режиме Легкого агента, применяются программные и аппаратные требования приложения Kaspersky Endpoint Security со следующими ограничениями:

- Необходим виртуализированный сетевой интерфейс с полосой пропускания 100 Мбит/сек.
- На устройствах на базе архитектуры Arm не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента.
- В операционных системах Astra Linux Special Edition в режимах мандатного разграничения доступа и замкнутой программной среды не поддерживается использование приложения в режиме Легкого агента.

BIOS на виртуальной машине должен поддерживать спецификацию SMBIOS версии 2.1 или выше.

В зависимости от вашей виртуальной инфраструктуры на виртуальных машинах должны быть установлены:

- В инфраструктуре Microsoft Hyper-V – пакет служб интеграции (Integration Services).
- В инфраструктуре VMware vSphere – пакет VMware Tools.
- В инфраструктуре XenServer – программа XenTools.
- В инфраструктуре HUAWEI FusionSphere – пакет HUAWEI Tools.
- В инфраструктуре KVM (Kernel-based Virtual Machine) – QEMU Guest Agent.

Поддерживаемые типы терминальных серверов

- Сервер терминалов Astra Linux 3.0.5.

Комплект поставки

В комплект поставки приложения Kaspersky Endpoint Security входят следующие файлы:

Основные файлы приложения

- Для процессоров с 32-битной операционной системой:
  `kesl-12.5.0-<build number>.i386.rpm`
  `kesl_12.5.0-<build number>_i386.deb`
- Для процессоров с 64-битной операционной системой:
  `kesl-12.5.0-<build number>.x86_64.rpm`
  `kesl_12.5.0-<build number>_amd64.deb`
- Для процессоров с архитектурой Arm®, 64-битная операционная система:
  `kesl-12.5.0-<build number>.aarch64.rpm`
  `kesl_12.5.0-<build number>_arm64.deb`
- Для процессоров Эльбрус:
  `kesl-12.5.0-<build number>.e2k.rpm`
  `kesl_12.5.0-<build number>_e2k.deb`

Графический интерфейс приложения

- Для процессоров с 32-битной операционной системой:
  `kesl-gui-12.5.0-<build number>.i386.rpm`
  `kesl-gui_12.5.0-<build number>_i386.deb`
- Для процессоров с 64-битной операционной системой:
  `kesl-gui-12.5.0-<build number>.x86_64.rpm`
  `kesl-gui_12.5.0-<build number>_amd64.deb`
- Для процессоров с архитектурой Arm®, 64-битная операционная система:
  `kesl-gui-12.5.0-<build number>.aarch64.rpm`
  `kesl-gui_12.5.0-<build number>_arm64.deb`
- Для процессоров Эльбрус:
  `kesl-gui-12.5.0-<build number>.e2k.rpm`
  `kesl-gui_12.5.0-<build number>_e2k.deb`

Для установки приложения Kaspersky Endpoint Security на операционные системы с ограниченной поддержкой (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6) выбирайте дистрибутив с пометкой `OLD`.

Архив для удаленной установки приложения с помощью Kaspersky Security Center

`kesl-12.5.0.<build number>.zip`

Архив также содержит тексты пользовательских соглашений.

Тексты пользовательских соглашений

- `ksn_license.<language ID>` – текст Положения о Kaspersky Security Network.
- `license.<language ID>` – текст Лицензионного соглашения. В Лицензионном соглашении указано, на каких условиях вы можете пользоваться приложением.

Агент администрирования Kaspersky Security Center не входит в комплект поставки. Вы можете скачать его на странице загрузки приложений в разделе **Kaspersky Security Center**.

Совместимость с другими приложениями

Поддерживаемые версии Kaspersky Security Center

В зависимости от режима использования Kaspersky Endpoint Security вы можете управлять приложением с помощью Kaspersky Security Center версий, указанных в таблице.

Режим использования	Версия Kaspersky Security Center
Kaspersky Endpoint Security в стандартном режиме	Kaspersky Security Center Windows 14.2, 15.1. Управление через Консоль администрирования с помощью MMC-плагина управления и через Kaspersky Security Center Web Console с помощью веб-плагина управления. Kaspersky Security Center Linux 15.1, 15.2, 15.3, 15.4, 16.0, 16.1, 16.2, 16.3. Управление через Kaspersky Security Center Web Console с помощью веб-плагина управления.
Kaspersky Endpoint Security в стандартном режиме с компонентом Endpoint Detection and Response Optimum	Kaspersky Security Center Windows 15.1. Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.
Kaspersky Endpoint Security в режиме Легкого агента	Kaspersky Security Center Windows 15.1. Kaspersky Security Center Linux 16.1, 16.2, 16.3.
Kaspersky Endpoint Security в режиме EDR-агента	Kaspersky Security Center Windows 14.2, 15.1. Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2, 16.3.

Поддерживаемая версия Kaspersky Security для виртуальных сред Легкий агент

Приложение Kaspersky Endpoint Security может использоваться в качестве Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент версии 6.5.

Поддерживаемые версии решений на платформах KATA и OSMP

Приложение Kaspersky Endpoint Security совместимо с решениями на платформе Kaspersky Anti Targeted Attack Platform и решением Kaspersky Endpoint Detection and Response Expert (on-premises) следующих версий:

- Kaspersky Anti Targeted Attack Platform 6.0, 6.1, 7.0, 7.1 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), включая сценарии отправки файлов на проверку в Sandbox).
- Kaspersky Anti Targeted Attack Platform 8.0 (Kaspersky Network Detection and Response (KATA), включая сценарии отправки файлов на проверку в Sandbox).

  Подробнее о решении Kaspersky Anti Targeted Attack Platform см. в справке Kaspersky Anti Targeted Attack Platform.
- Kaspersky Endpoint Detection and Response Expert (on-premises) 8.0, 8.1, 8.2 на платформе Open Single Management Platform (далее также OSMP), включая сценарии отправки файлов на проверку в Sandbox.

  Подробнее о решении Kaspersky Endpoint Detection and Response Expert (on-premises) см. в справке Kaspersky Endpoint Detection and Response Expert (on-premises).

Поддерживаемые версии Агента администрирования для интеграции с Kaspersky Endpoint Detection and Response Expert (cloud)

Для интеграции приложения с решением Kaspersky Endpoint Detection and Response Expert (cloud) требуется Агент администрирования для Kaspersky Security Center Cloud Console определенных версий, описанных в справке Kaspersky Security Center Cloud Console.

Совместимость со сторонними решениями

Приложение Kaspersky Endpoint Security в режиме EDR-агента может работать совместно с антивирусным приложением Dr. Web.

Сравнение функциональности в зависимости от решений "Лаборатории Касперского"

Kaspersky Endpoint Security входит в состав многих мультиплатформенных решений "Лаборатории Касперского". Доступная функциональность приложения определяется решением, которое вы приобрели у поставщика услуг в вашем регионе.

Функция	Kaspersky Endpoint Security для бизнеса – Стандартный	Kaspersky Endpoint Security для бизнеса – Расширенный	Kaspersky Total Security для бизнеса	Kaspersky Security для виртуальных и облачных сред, Desktop	Kaspersky Security для виртуальных и облачных сред – Enterprise Edition Desktop/CPU/Server	Kaspersky Security для виртуальных и облачных сред Core/Server	Kaspersky Symphony XDR	Kaspe EDR бизне Оптима
Защита от файловых угроз	✓	✓	✓	✓	✓	✓	✓	✓
Защита от почтовых угроз	✓	✓	✓	✓	✓	✓	✓	✓
Защита от веб-угроз	✓	✓	✓	✓	✓	✓	✓	✓
Защита от сетевых угроз	✓	✓	✓	✓	✓	✓	✓	✓
Управление сетевым экраном	✓	✓	✓	✓	✓	✓	✓	✓
Анализ поведения	✓	✓	✓	✓	✓	✓	✓	✓
Защита от атак BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Контроль устройств	✓	✓	✓	✓	✓	✓	✓	✓
Проверка съемных дисков	✓	✓	✓	✓	✓	✓	✓	✓
Защита от шифрования (для общих папок)	✓	✓	✓	–	✓	✓	✓	✓
Проверка контейнеров	–	–	–	–	✓	–	–	–
Контроль целостности системы	–	–	–	–	✓	–	–	–
Контроль приложений	–	✓	✓	✓	✓	–	✓	✓
Веб-Контроль	✓	✓	✓	✓	✓	✓	✓	✓
Интеграция с Kaspersky Unified Monitoring and Analysis Platform	–	–	–	–	–	–	✓	–
Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud)	–	–	–	–	–	–	–	–

Функция	Kaspersky Endpoint Security для бизнеса – Стандартный	Kaspersky Endpoint Security для бизнеса – Расширенный	Kaspersky Total Security для бизнеса	Kaspersky Security для виртуальных и облачных сред, Desktop	Kaspersky Security для виртуальных и облачных сред – Enterprise Edition Desktop/CPU/Server	Kaspersky Security для виртуальных и облачных сред Core/Server	Kaspersky Symphony XDR	Kaspe EDR бизне Оптима
Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)	–	–	–	–	–	–	✓	–
Kaspersky Endpoint Detection and Response Optimum	–	–	–	–	–	–	–	✓

Развертывание и первоначальная настройка

Следуя этому сценарию, вы можете развернуть приложение Kaspersky Endpoint Security и подготовить его к работе.

1 Выбор режима использования приложения

После того как вы купили решение "Лаборатории Касперского" на официальном сайте "Лаборатории Касперского" или у наших партнеров, вы получите письмо на адрес электронной почты, который указали при покупке. В письме будет код активации и информация о том, как получить файл ключа. Файл ключа вам может потребоваться, если на вашем предприятии не поддерживается онлайн-активация приложения с помощью кода.

Выбранное вами решение определяет режимы, в которых вы можете использовать приложение:

- Если у вас есть лицензия на Kaspersky Endpoint Security, вы можете использовать приложение в стандартном режиме.
- Если у вас есть лицензия на решение Kaspersky Security для виртуальных сред Легкий агент, вы можете использовать приложение в режиме Легкого агента.
- Если у вас есть лицензия на Kaspersky Endpoint Detection and Response Expert (on-premises), вы можете использовать приложение в режиме EDR-агента.

Развертывание приложения зависит от выбранного режима.

После установки Kaspersky Endpoint Security изменить режим использования приложения невозможно.

2 Подготовка среды

Выполните необходимые подготовительные действия в зависимости от вашей инфраструктуры.

3 Выбор механизма перехвата системных событий

Если операционная система на устройстве поддерживает технологию fanotify, в ходе установки приложения вы можете выбрать, какой механизм нужно использовать для перехвата системных событий.

4 Подготовка дистрибутивов

Скачайте файлы, необходимые для установки приложения. Состав необходимых файлов различается в зависимости от операционной системы защищаемого устройства и от способа развертывания приложения.

5 Подготовительные действия в Kaspersky Security Center

Выполните подготовительные действия в Kaspersky Security Center. Kaspersky Security Center рекомендуется использовать для централизованного управления защитой вашей организации. Также Kaspersky Security Center необходим, если вы будете использовать приложение Kaspersky Endpoint Security в режиме EDR-агента или в режиме Легкого агента.

6 Установка приложения

Установите приложение на устройствах тем способом, который соответствует требованиям вашей организации:

- Установка с помощью Kaspersky Security Center
- Установка с помощью командной строки

7 Дополнительная настройка после установки в отдельных ОС

В некоторых операционных системах Linux после установки Kaspersky Endpoint Security требуется дополнительная настройка.

Режимы использования и схемы развертывания

Kaspersky Endpoint Security входит в состав многих решений от "Лаборатории Касперского". Выбранное вами решение определяет режим приложения и схему развертывания.

Стандартный режим

Режим работы приложения по умолчанию. Kaspersky Endpoint Security обеспечивает комплексную защиту от различного вида угроз, сетевых и мошеннических атак для рабочих станций и серверов под управлением операционных систем Linux.

В этом режиме приложение использует компоненты защиты и контроля устройств, такие как Защита от файловых угроз или Анализ поведения, а также встроенные агенты для защиты от сложных угроз и целевых атак.

Вы можете установить приложение в этом режиме в составе EPP-решений (Endpoint Protection Platform) от "Лаборатории Касперского". Например, Kaspersky Endpoint Security в стандартном режиме входит в состав решения Kaspersky Endpoint Security для бизнеса.

Основной схемой развертывания приложения Kaspersky Endpoint Security является централизованное развертывание с помощью Kaspersky Security Center. На каждое защищаемое устройство требуется установить Kaspersky Endpoint Security и компонент Kaspersky Security Center Агент администрирования. Этот компонент обеспечивает связь устройств с Сервером администрирования Kaspersky Security Center и позволяет управлять устройствами через Kaspersky Security Center.

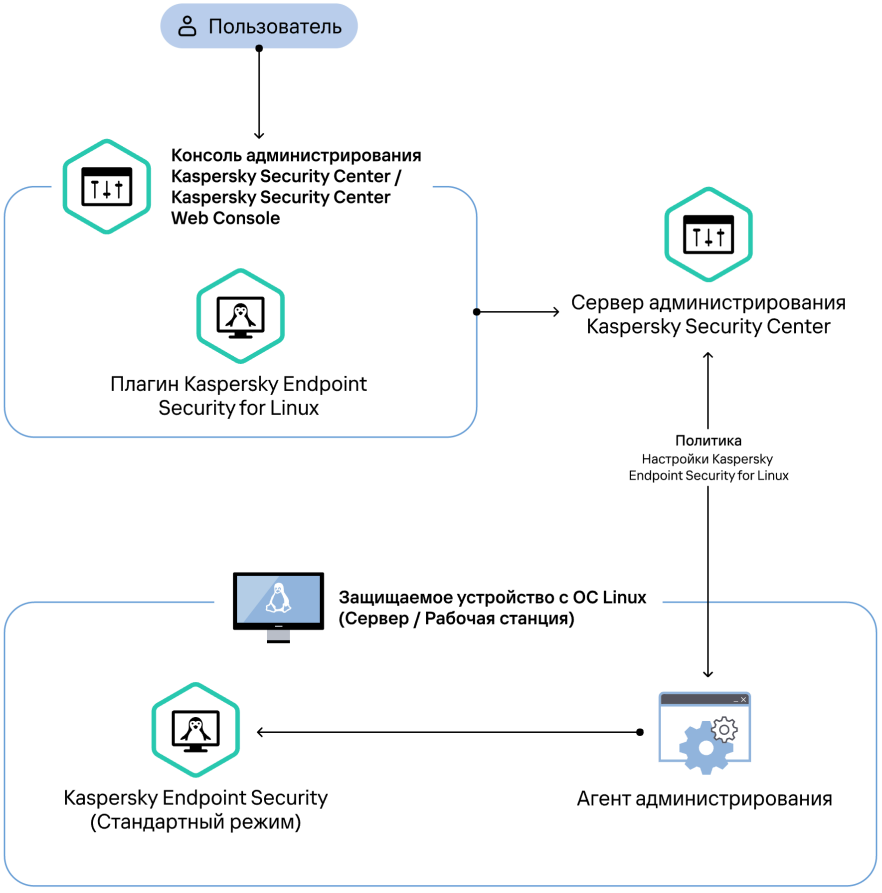


Схема развертывания Kaspersky Endpoint Security в стандартном режиме

Режим Агента Endpoint Detection and Response (EDR-агент)

Этот режим позволяет развернуть решения Detection and Response от "Лаборатории Касперского" совместно с антивирусными решениями от сторонних поставщиков. К Detection and Response решениям относятся:

- Kaspersky Endpoint Detection and Response Expert (on-premises) на платформе Open Single Management Platform (далее также "OSMP").
- Kaspersky Endpoint Detection and Response и Kaspersky Network Detection and Response на платформе Kaspersky Anti Targeted Attack Platform (далее также "KATA").

В режиме EDR-агента недоступны компоненты защиты и контроля, например, Защита от файловых угроз или Защита от веб-угроз. Защиту устройства обеспечивает стороннее антивирусное приложение. EDR-агент постоянно отслеживает процессы, запущенные на этих устройствах, открытые сетевые соединения и изменяемые файлы, а также взаимодействует с решениями Detection and Response для защиты от сложных угроз и целевых атак.

Для работы Kaspersky Endpoint Security в режиме EDR-агента требуется развернуть соответствующую инфраструктуру, информацию о ней смотрите в справке выбранного вами решения Detection and Response. Ознакомьтесь с особенностями работы в режиме EDR-агента в статье Известные проблемы и ограничения.

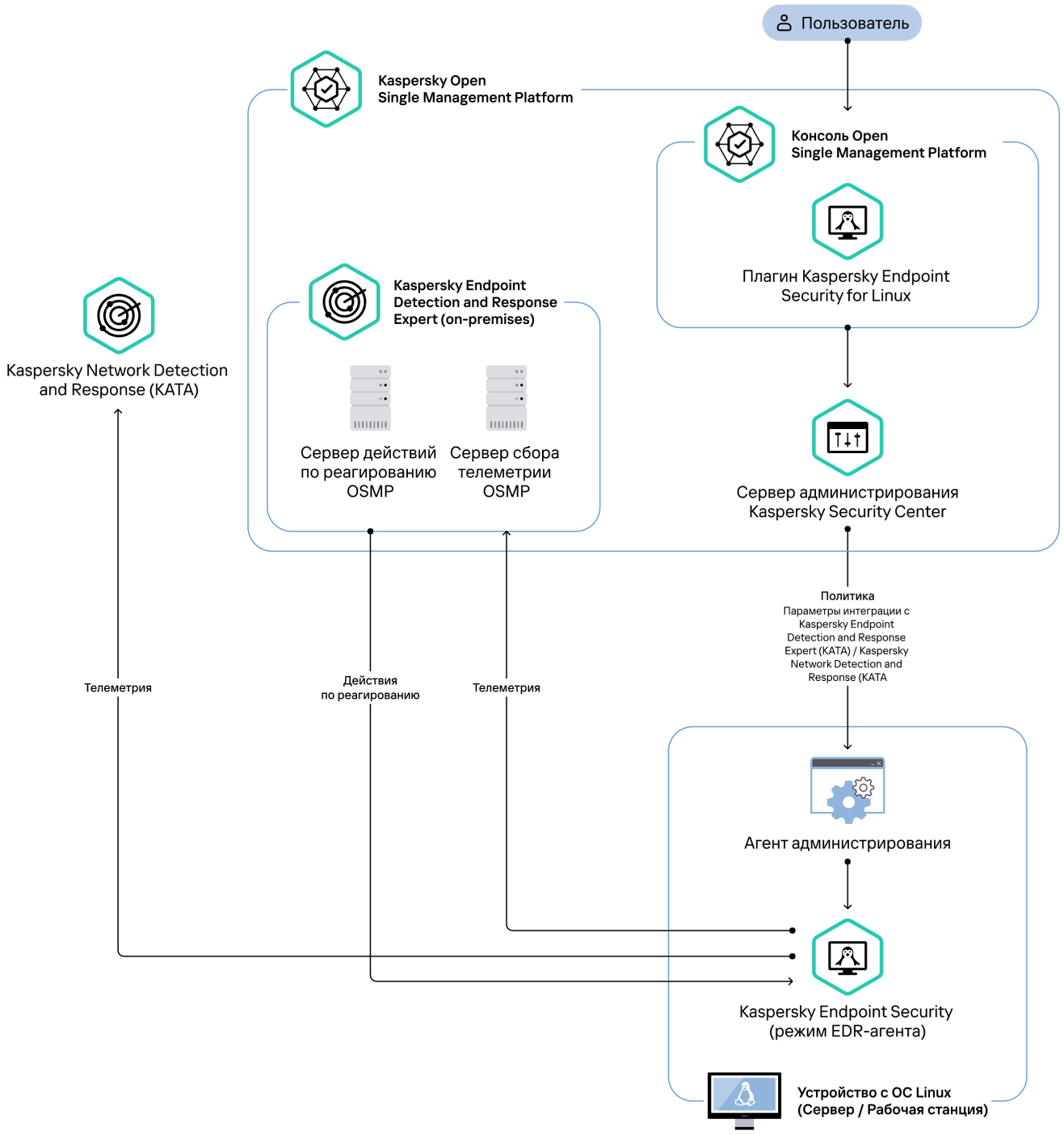


Схема развертывания Kaspersky Endpoint Security в режиме EDR-агента совместно с Kaspersky Endpoint Detection and Response Expert (on-premises)

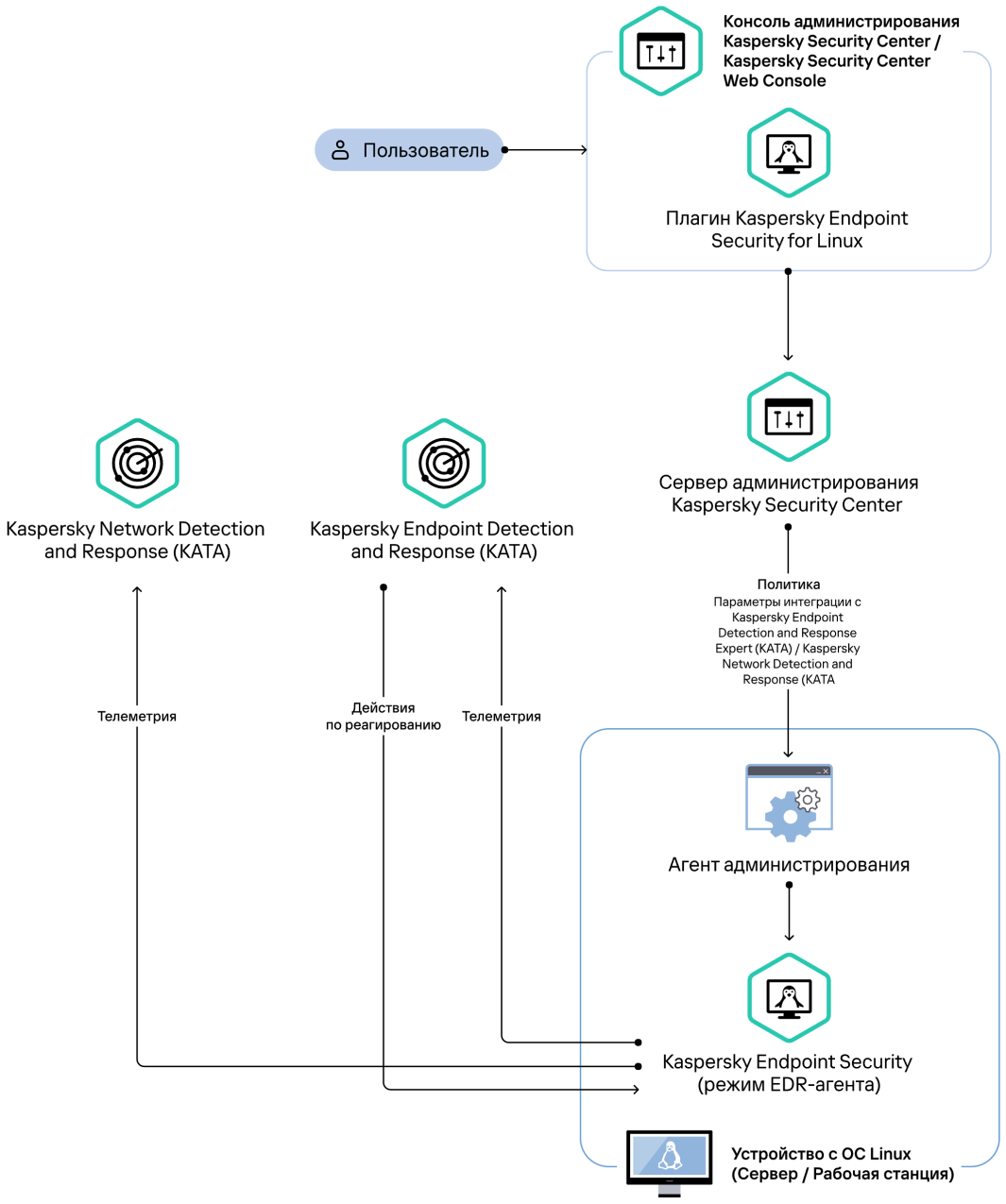


Схема развертывания Kaspersky Endpoint Security в режиме EDR-агента совместно с Kaspersky Endpoint Detection and Response и Kaspersky Network Detection and Response

Режим Легкого агента

Kaspersky Endpoint Security в режиме Легкого агента входит в состав решения Kaspersky Security для виртуальных сред Легкий агент и оптимизирован для защиты виртуальных машин с гостевыми операционными системами Linux.

В этом режиме доступны те же компоненты защиты и контроля, что и для стандартного режима. Отличие заключается в том, что проверку объектов на наличие вирусов, добавление лицензионных ключей и обновление баз и модулей выполняет компонент решения, установленный на отдельную виртуальную машину – SVM (Secure Virtual Machine). В результате уменьшается нагрузка на гипервизор, так как приложение в режиме Легкого агента использует ресурсы SVM для обеспечения безопасности инфраструктуры, а не ресурсы виртуальных машин.

Для работы Kaspersky Endpoint Security в режиме Легкого агента требуется развернуть соответствующую инфраструктуру, информацию о ней смотрите в справке Kaspersky Security для виртуальных сред Легкий агент. Ознакомьтесь с особенностями работы в режиме Легкого агента в статье Известные проблемы и ограничения.

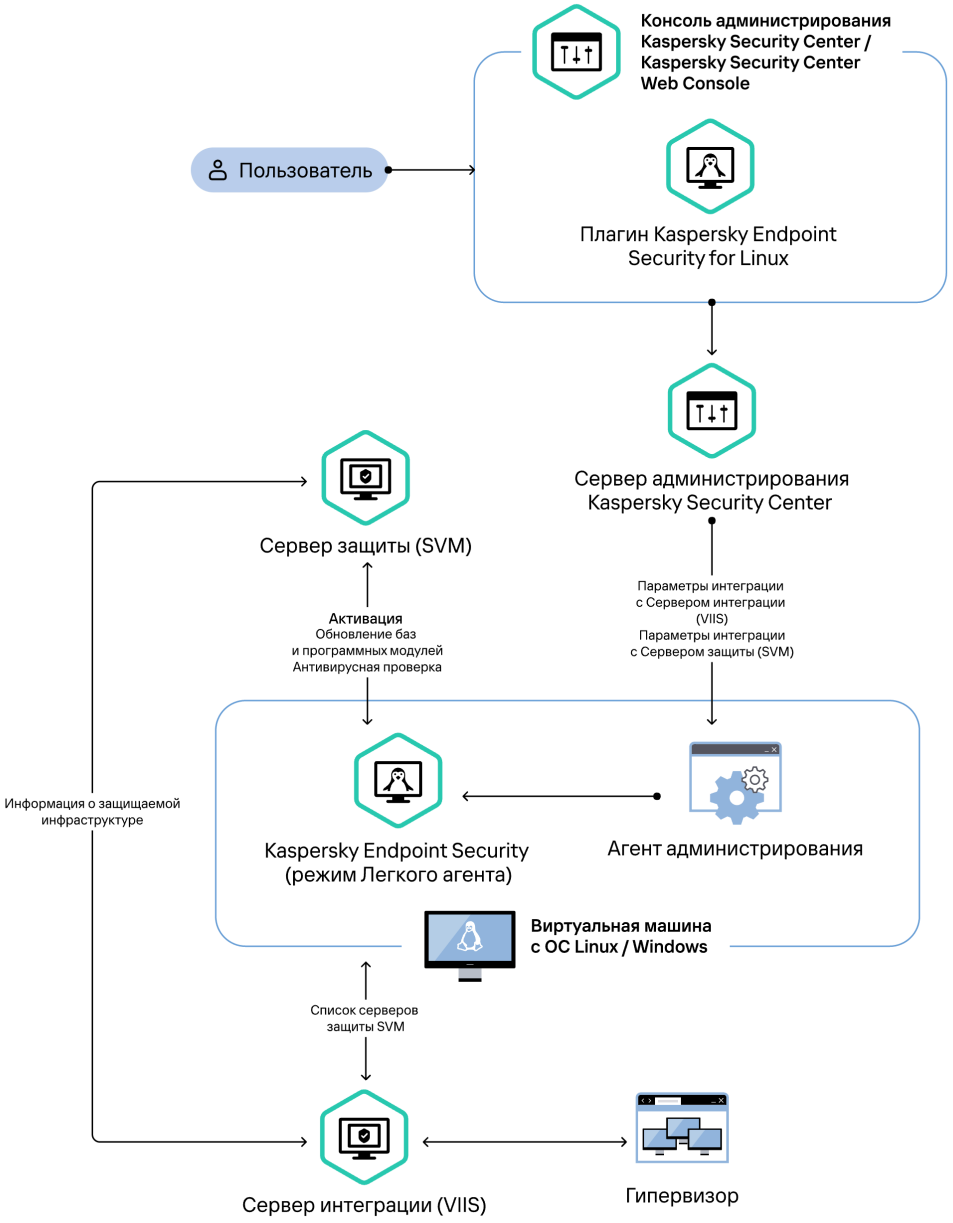


Схема развертывания Kaspersky Endpoint Security в режиме Легкого агента

После выбора режима использования приложения вы можете вернуться в сценарий развертывания и продолжить с этапа Подготовка среды.

Подготовка среды к установке приложения

Подготовка инфраструктуры

Kaspersky Security Center

Если вы планируете управлять приложением централизованно с помощью Kaspersky Security Center, установите в вашей инфраструктуре Kaspersky Security Center. Если у вас уже установлен Kaspersky Security Center Windows и вы планируете перейти на Kaspersky Security Center Linux, воспользуйтесь инструкцией Перенос данных в программу Kaspersky Security Center Linux.

Kaspersky Endpoint Security в режиме EDR-агента

Для работы Kaspersky Endpoint Security в режиме EDR-агента требуется развернуть соответствующую инфраструктуру, информацию о ней смотрите в справке выбранного вами решения Detection and Response.

Kaspersky Endpoint Security в режиме Легкого агента

Для работы Kaspersky Endpoint Security в режиме Легкого агента требуется развернуть решение Kaspersky Security для виртуальных сред Легкий агент:

1. Установите компоненты решения Kaspersky Security для виртуальных сред Легкий агент – Сервер интеграции и Сервер защиты.

2. Подготовьте Сервер защиты к работе, в том числе активируйте решение и настройте обновление баз для Сервера защиты и Легких агентов.

   Описание установки и настройки компонентов решения см. в справке Kaspersky Security для виртуальных сред Легкий агент.

3. Убедитесь в том, что виртуальные машины, которые вы хотите защищать, соответствуют требованиям для режима Легкого агента.

4. Убедитесь в том, что в настройках сетевого оборудования или программного обеспечения, обеспечивающего контроль трафика между виртуальными машинами, разрешено прохождение сетевого трафика через порты, которые используются для взаимодействия приложения Kaspersky Endpoint Security в режиме Легкого агента с другими компонентами решения Kaspersky Security для виртуальных сред Легкий агент. Порты, используемые в работе Легкого агента, указаны в справке Kaspersky Security для виртуальных сред Легкий агент.

Не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента на устройствах на базе архитектуры Arm и с процессором Эльбрус.

Подготовка устройства к установке

- Проверьте соответствие вашего устройства аппаратным и программным требованиям приложения.

- Если вы хотите установить Kaspersky Endpoint Security в стандартном режиме или режиме Легкого агента, убедитесь в том, что на вашем устройстве не установлено стороннее антивирусное программное обеспечение. В режиме EDR-агента приложение может работать совместно с антивирусным приложением Dr. Web.

- Убедитесь в том, что на вашем устройстве не установлено приложение Kaspersky Endpoint Agent для Linux. Если приложение Kaspersky Endpoint Agent для Linux установлено, его нужно удалить.

- Убедитесь, что на вашем устройстве установлена утилита iptables. Утилита iptables требуется для перехвата приложением сетевого трафика.

- Убедитесь в том, что учетная запись root является владельцем следующих директорий и только владелец имеет право на запись в них: /var, /var/opt, /opt, /usr/bin, /usr/lib, /usr/lib64. Это требуется для запуска и корректной работы приложения.

- При работе приложения потребление файловых дескрипторов в операционной системе может существенно увеличиться. Убедитесь в том, что ограничение на максимальное количество дескрипторов имеет достаточный запас. Для проверки ограничения запустите команду `cat /proc/sys/fs/file-max`. В общем случае рекомендуется выключить ограничение, указав в файле /etc/sysctl.conf значение параметра `fs.file-max=9223372036854775807`. После изменения перезагрузите операционную систему.

- Убедитесь в том, что в операционной системе значение параметра `kernel.yama.ptrace_scope=0`. Другие значения параметра `kernel.yama.ptrace_scope` могут повлиять на работу приложения Kaspersky Endpoint Security, подробнее см. в разделе Известные проблемы и ограничения.

Дополнительно для установки графического интерфейса приложения

- Устанавливаемая версия пакета графического интерфейса kesl-gui должна совпадать с устанавливаемой версией пакета kesl.

- Для корректной работы графического интерфейса Kaspersky Endpoint Security в операционной системе должна быть установлена утилита Zenity.

- Если ваше устройство имеет доступ к репозиториям пакетного менеджера, все необходимые зависимости будут установлены автоматически в процессе установки графического интерфейса приложения. Если устройство находится в закрытом контуре и не имеет доступа к репозиториям пакетного менеджера:

  1. Проверьте перечень зависимостей на эталонном устройстве (libice6, libsm6, zlib1g, kesl).

  2. Выполните одно из следующих действий:

     - Перед установкой графического интерфейса скачайте пакеты на все устройства, а затем установите их с помощью пакетного менеджера.

     - Обеспечьте скачивание пакетов на устройства во время установки графического интерфейса.

Дополнительно для поддержки MMC-плагина

Если для управления приложением вы планируете использовать Консоль администрирования Kaspersky Security Center, установите Microsoft® Visual C++® 2015 Redistributable Update 3 RC на устройстве, где установлен Сервер администрирования (см. https://www.microsoft.com/ru-ru/download/details.aspx?id=52685). Это требуется для работы MMC-плагина управления Kaspersky Endpoint Security.

Дополнительно для отдельных ОС

ОС Astra Linux в режиме замкнутой программной среды

Установка пакета совместимости

Установите пакет совместимости в следующих случаях:

- Перед установкой приложения в режиме замкнутой программной среды.
- После установки приложения при изменении режима операционной системы на режим замкнутой программной среды.

Установить пакет

```
apt install astra-digsig-oldkeys
```

Это обеспечит запуск приложения в операционных системах Astra Linux Special Edition (очередные обновления 4.7 для архитектуры Arm, 1.6, 1.7 и 1.8) в режиме замкнутой программной среды.

Выключение запрета трассировки ptrace

В операционных системах Astra Linux по умолчанию включен запрет трассировки ptrace (Disable ptrace capability), который может влиять на работу приложения Kaspersky Endpoint Security. Для корректной работы Kaspersky Endpoint Security рекомендуется выключить запрет трассировки ptrace при установке Astra Linux. Если Astra Linux уже установлена, инструкцию по включению и выключению этого режима см. на сайте Справочного центра Astra Linux (**Настройка механизмов защиты и блокировок**, раздел **Блокировка трассировки ptrace**).

ОС SUSE Linux Enterprise Server 15

Перед установкой приложения на устройстве с операционной системой SUSE Linux Enterprise Server 15 установите пакет insserv-compat.

ОС Альт СП в режиме замкнутой программной среды

Перед установкой приложения на устройстве с операционной системой Альт СП в режиме замкнутой программной среды:

1. Выключите режим замкнутой программной среды:

   ```
   integrity-remover
   ```

2. Создайте группу kesl для дальнейшего внесения изменений в политику IMA:

   ```
   groupadd kesl
   ```

3. Узнайте уникальный идентификатор (GID) созданной группы:

   ```
   cat /etc/group | grep kesl
   ```

4. Внесите изменения в политику IMA, чтобы исключить группу kesl из проверки целостности компонентов приложения с помощью утилиты, для обеспечения корректной работы приложения. Для этого:

   a. Скопируйте файл /usr/share/integrity/policy:

   ```
   cp /usr/share/integrity/policy /etc/integrity/policy
   ```

b. Откройте на редактирование файл /etc/integrity/policy с помощью текстового редактора (например, vim):

```
vim /etc/integrity/policy
```

c. После строки `dont_measure fsmagic=0xf97cff8c` (обычно это последняя строка блока `dont_measure`) добавьте строку:

```
dont_measure fgroup=<GID>
```

где `<GID>` – уникальный идентификатор группы, созданной на шаге 2 этой инструкции.

d. После строки `dont_appraise fsmagic=0x27e0eb` (обычно это последняя строка блока `dont_appraise`) добавьте строку:

```
dont_appraise fgroup=<GID>
```

где `<GID>` – уникальный идентификатор группы, созданной на шаге 2 этой инструкции.

e. Сохраните изменения.

5. В файле /usr/sbin/integrity-sign внесите изменения в функцию list_all_files, чтобы включить приложение Kaspersky Endpoint Security в список разрешенных для запуска в режиме замкнутой программной среды. Для этого:

a. Откройте на редактирование файл /usr/sbin/integrity-sign с помощью текстового редактора (например, vim):

```
vim /usr/sbin/integrity-sign
```

b. Найдите функцию list_all_files и в теле функции в строках, начинающихся с `find -P`, в конце каждого перечисления директорий добавьте директории приложения Kaspersky Endpoint Security /var/opt и /opt.

c. Сохраните изменения.

Во время первоначальной настройки приложения не запускайте обновление баз приложения.

> После завершения установки включите режим замкнутой программной среды и выполните действия, необходимые для запуска приложения.

ОС ОСнова

Если вы планируете использовать Kaspersky Security Center для установки и управления приложением, перед установкой приложения подготовьте устройство к установке Агента администрирования:

1. Откройте файл /usr/lib/systemd/logind.conf.d/10-enable-kill-user-processes.conf и в секции `[Login]` закомментируйте строку KillUserProcesses=yes.

```
#KillUserProcesses=yes
```

2. Откройте файл /usr/lib/NESS/pam-user-session и закомментируйте строку loginctl terminate-session "$XDG_SESSION_ID".

```
#loginctl terminate-session "$XDG_SESSION_ID"
```

ОС с поддержкой SELinux

Если в вашей операционной системе не установлена утилита semanage, перед установкой приложения установите пакет policycoreutils-python или policycoreutils-python-utils в зависимости от типа менеджера пакетов.

Пакет policycoreutils-python-utils актуален для следующих типов пакетных менеджеров: dnf, apt и yum, для ОС Fedora, Debian, Ubuntu и RHEL 7 и выше.

Пакет policycoreutils-python актуален для следующих типов пакетных менеджеров: yum и ОС CentOS/RHEL 7 и ниже.

ОС Kylin

Перед установкой приложения на устройстве с операционной системой Kylin выполните следующие действия:

1. В пользовательском интерфейсе UKUI (Ubuntu Kylin User Interface) выключите Firewall. Для этого перейдите в раздел **Kylin Security Center** → **Firewall and Network Protection** и в блоке **Firewall** выключите переключатели **Public Network** и **Private Network**.

2. В пользовательском интерфейсе UKUI выключите Application Network Control. Для этого перейдите в раздел **Kylin Security Center** → **Firewall and Network Protection** и в блоке **Application Network Control** выберите вариант **Disable**.

3. В пользовательском интерфейсе UKUI выключите Application Source Check. Для этого перейдите в раздел **Kylin Security Center** → **Application Protection** и в блоке **Application Source Check** выберите вариант **Disable**.

4. Выключите механизм безопасности KYSEC. Для этого выполните следующие действия в терминале:

   a. Проверьте текущий статус:

   ```
   getstatus
   ```

   b. Выключите механизм безопасности KYSEC:

   ```
   setstatus disable -p
   ```

   c. Проверьте, что механизм безопасности KYSEC выключен:

   ```
   getstatus
   ```

5. Удалите встроенное антивирусное приложение. Для этого выполните следующую команду в терминале:

```
sudo dpkg -P pksav
```

6. Если у вас на устройстве установлен антивирус Qaxsafe, вам нужно его удалить. Для этого выполните следующие действия:

   a. Выключите самозащиту:

      1. Найдите значок приложения в области уведомлений панели задач и двойным щелчком мыши по значку приложения откройте контекстное меню.

      2. В контектном меню выберите **Settings** → **Protection Center**.

      3. В открывшемся окне снимите флажок **Enable Self-Protection** и введите пароль, если требуется.

   b. Удалите антивирус Qaxsafe. Для этого выполните следующую команду в терминале:

   ```
   sudo dpkg -P qaxsafe
   ```

   c. Удалите остаточные файлы. Для этого выполните следующую команду в терминале:

   ```
   sudo rm -rf /opt/qaxsafe
   ```

ОС, не поддерживающие технологию fanotify

Перед началом установки приложения убедитесь в том, что на устройстве установлены:

- пакеты для компиляции программ и запуска задач (gcc, binutils, glibc, glibc-devel, make);
- пакет с заголовочными файлами ядра операционной системы для компиляции модулей Kaspersky Endpoint Security.

Полезные статьи

Решение проблем на ОС Kylin

После подготовки среды к установке вы можете вернуться в сценарий развертывания и продолжить с этапа Выбор механизма перехвата системных событий.

Выбор механизма перехвата системных событий

Для полноценной работы приложение должно использовать перехват системных событий об операциях с файлами и запуске процессов. Перехват системных событий необходим во всех режимах использования приложения (стандартный режим, режим Легкого агента и режим EDR-агента). Если приложение не использует перехват системных событий, проверка файлов в режиме реального времени не выполняется, что снижает защиту устройства.

Механизм перехвата системных событий

Приложение может использовать следующие механизмы перехвата системных событий:

- **Системный механизм перехвата на основе технологии fanotify**. *Fanotify* – это подсистема ядра Linux, которая отслеживает события в файловой системе (например, открытие, чтение, запись или закрытие файлов) и позволяет приложениям перехватывать их в режиме реального времени.

- **Механизм перехвата на основе обновляемого модуля ядра**. *Обновляемый модуль ядра* работает совместно с системным механизмом перехвата на основе технологии fanotify. Это позволяет оптимизировать перехват файловых операций и перехват запуска процессов приложением Kaspersky Endpoint Security за счет обработки системных событий в пространстве ядра (англ. kernel space), а не в пользовательском пространстве (англ. user space). Обновляемый модуль ядра перехватывает файловые операции при открытии, переименовании и изменении файлов. Производительность приложения увеличивается за счет использования кеша результатов проверки файлов и процессов.

  Обновляемый модуль ядра также используется для следующих задач и компонентов:

  - Защита от файловых угроз
  - Защита от шифрования
  - Защита от эксплойтов
  - Анализ поведения
  - Контроль приложений
  - Запрет запуска объектов (при интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) и Kaspersky Endpoint Detection and Response Optimum)

  При использовании обновляемого модуля ядра вы можете более точно настраивать глобальные исключения. Механизм перехвата на основе технологии fanotify позволяет исключать из перехвата файловых операций указанные точки монтирования целиком. Использование обновляемого модуля ядра позволяет исключать конкретные локальные или удаленные директории, смонтированные на устройстве.

  Обновляемый модуль ядра входит в комплект поставки приложения.

- **Модуль ядра для защиты от файловых угроз на ОС без fanotify**. Если операционная система на устройстве не поддерживает технологию fanotify (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6), приложение скомпилирует и будет использовать для перехвата системных событий специальный модуль. Этот модуль автоматически компилируется при запуске Защиты от файловых угроз при наличии необходимых пакетов и утилит компиляции.

Как выбрать механизм перехвата системных событий

Если операционная система поддерживает технологию fanotify, в процессе развертывания приложения вы можете выбрать механизм перехвата системных событий: только механизм перехвата на основе технологии fanotify или обновляемый модуль ядра совместно с механизмом перехвата на основе технологии fanotify. По умолчанию используется механизм перехвата на основе технологии fanotify. После установки вы можете изменить механизм перехвата системных событий в настройках приложения.

Для операционных систем, не поддерживающих технологию fanotify, выбор механизма перехвата недоступен.

Приложение может использовать механизм перехвата на основе обновляемого модуля ядра, если операционная система соответствует требованиям для установки обновляемого модуля ядра.

Программные требования для установки обновляемого модуля ядра

Для установки и работы обновляемого модуля ядра на устройстве должна быть установлена одна из следующих 64-битных операционных систем:

- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6.5, 1.6.6).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7.3, 1.7.4, 1.7.6, 1.7.7, 1.7.8, 1.7.9).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.2, 1.8.3, 1.8.4, 1.8.5).

  Если приложение Kaspersky Endpoint Security используется в стандартном режиме, обновляемый модуль ядра можно использовать на устройствах с операционными системами Astra Linux в режиме замкнутой программной среды.

- CentOS 7.x.
- CentOS 8.x.
- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12.
- Red Hat Enterprise Linux 7.4.
- Red Hat Enterprise Linux 8.10.
- SberLinux 8.10.
- SberLinux 9.0.1.
- SberLinux 9.1.
- SberLinux 9.6.
- SberLinux 9.7.
- SberOS 3.4.
- SberOS 3.5.
- Ubuntu 16.04 LTS.
- Ubuntu 18.04 LTS.
- Ubuntu 20.04 LTS.
- Ubuntu 22.04 LTS.
- Ubuntu 24.04 LTS.

- Альт СП Рабочая Станция релиз 10.
- Альт СП Сервер релиз 10.
- Альт Образование 10.
- Альт Рабочая Станция 11.
- Альт Сервер 11.
- Альт Образование 11.
- РЕД ОС 7.3.
- РЕД ОС 8.0.
- РОСА "Кобальт" 7.9 Рабочая станция.
- РОСА "Кобальт" 7.9 Сервер.
- РОСА "Хром" 12 Рабочая станция.
- РОСА "Хром" 12 Сервер.

32-битные операционные системы, операционные системы для архитектуры Arm и операционные системы для архитектуры Эльбрус не поддерживаются.

Возможны конфликты в работе обновляемого модуля ядра на устройствах с некоторыми версиями ядер ОС Linux, а также при совместной работе с некоторыми сторонними приложениями.

Проверка возможности установки обновляемого модуля ядра

Версия обновляемого модуля ядра не зависит от версии Kaspersky Endpoint Security. Функциональность обновляемого модуля ядра регулярно расширяется вместе с обновлением баз и модулей приложения Kaspersky Endpoint Security. Поэтому приведенный выше список поддерживаемых операционных систем может быть неполным. Чтобы проверить соответствие вашего устройства требованиям для установки обновляемого модуля ядра, используйте утилиту Kaspersky ULKM tool.

Как проверить удаленно с помощью Web Console или Консоли администрирования

1. Скачайте архив ulkmtool.zip на странице загрузки приложений в разделе **Kaspersky Endpoint Security для Linux**.
2. Создайте инсталляционный пакет для утилиты.

Как создать инсталляционный пакет в Web Console

1. Поместите скачанный архив ulkmtool.zip в папку, доступную для Сервера администрирования Kaspersky Security Center.

2. В главном окне Web Console выберите один из следующих разделов:

   - **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

   - **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, доступных на Сервере администрирования.

3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета.

4. Выберите способ создания инсталляционного пакета: **Создать инсталляционный пакет из файла**.

5. Введите имя нового инсталляционного пакета, нажмите на кнопку **Обзор** и укажите путь к архиву ulkmtool.zip, который вы скачали.

6. Завершите работу мастера.

Инсталляционный пакет будет создан и добавлен в список инсталляционных пакетов.

Как создать инсталляционный пакет в Консоли администрирования

1. Распакуйте архив ulkmtool.zip в папку, доступную для Сервера администрирования Kaspersky Security Center.

2. В дереве консоли выберите **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, доступных на Сервере администрирования.

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

   Запустится мастер создания инсталляционного пакета.

4. Нажмите на кнопку **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.

5. Введите имя нового инсталляционного пакета и перейдите к следующему шагу мастера.

6. Нажмите на кнопку **Обзор** и укажите путь к файлу ulkmtool.kud. Файл находится в папке, в которую вы распаковали архив ulkmtool.zip.

   Перейдите к следующему шагу мастера.

7. Дождитесь окончания загрузки файла и завершите работу мастера.

Инсталляционный пакет будет создан и добавлен в список инсталляционных пакетов.

3. Установите Агент администрирования Kaspersky Security Center на устройства, которые вы хотите проверить на соответствие требованиям для установки обновляемого модуля ядра. Подробнее см. в справке Kaspersky Security Center.

4. В Kaspersky Security Center Web Console или в Консоли администрирования создайте и запустите задачу удаленной установки приложений для устройств, которые вы хотите проверить на соответствие требованиям. В параметрах задачи выберите инсталляционный пакет, который вы создали.

   В результатах выполнения задачи для каждого устройства, на котором запускалась задача, указано, поддерживается ли на устройстве установка и работа обновляемого модуля ядра.

По результатам работы задачи каждому устройству автоматически присваивается тег:

- *UpdatableKernelModule=No* – на устройстве не поддерживается установка обновляемого модуля ядра.
- *UpdatableKernelModule=Yes* – устройство соответствует требованиям для установки и работы обновляемого модуля ядра.

Вы можете использовать эти теги для формирования выборок устройств. Например, вы можете выбрать устройства, которые соответствуют требованиям обновляемого модуля ядра, и установить на них Kaspersky Endpoint Security с обновляемым модулем ядра.

Как проверить локально на устройстве

1. Скачайте архив ulkmtool.zip на странице загрузки приложений в разделе **Kaspersky Endpoint Security для Linux**.
2. Установите Агент администрирования Kaspersky Security Center на устройства, которые вы хотите проверить на соответствие требованиям для установки обновляемого модуля ядра. Подробнее см. в справке Kaspersky Security Center.
3. Запустите утилиту Kaspersky ULKM tool локально на устройствах, которые вы хотите проверить.

   ```
   ulkmtool --check remote
   ```

4. Проверьте код возврата.

   ```
   echo $?
   ```

   Утилита вернет в командной строке следующие коды возврата:

   0 = Success – устройство соответствует требованиям для установки и работы обновляемого модуля ядра.

   1 = NotSupported – на устройстве не поддерживается установка обновляемого модуля ядра.

Проверка статуса работы обновляемого модуля ядра

В Kaspersky Security Center Web Console или в Консоли администрирования можно проверить статус работы обновляемого модуля ядра на устройствах с Kaspersky Endpoint Security. Для этого вы можете посмотреть назначенные устройствам теги:

- *UpdatableKernelModule=Use* – на устройстве установлен и работает обновляемый модуль ядра.
- *UpdatableKernelModule=Error* – на устройстве установлен обновляемый модуль ядра, но при запуске модуля произошла ошибка, модуль не работает.

Подробнее о просмотре тегов, назначенных устройствам, см. в справке Kaspersky Security Center.

Поддержка технологии Secure Boot

Обновляемый модуль ядра поддерживает технологию Secure Boot. Для использования механизма перехвата на основе обновляемого модуля ядра на операционных системах с включенной технологией Secure Boot вам нужно добавить в операционную систему публичный сертификат Kaspersky Endpoint Security для подписи модуля и перезапустить ее.

Скачать сертификат

Пример добавления сертификата для ОС Ubuntu

1. Убедитесь, что технология Secure Boot включена на вашей операционной системе:

```
mokutil --sb-state
```

2. Добавьте в ОС скачанный сертификат с помощью утилиты mokutil:

```
mokutil --import <path to certificate>
```

3. Перезапустите приложение Kaspersky Endpoint Security.

4. Проверьте работоспособность обновляемого модуля ядра с помощью команды:

```
kesl-control --app-info
```

После выбора механизма перехвата системных событий вы можете вернуться в сценарий развертывания и продолжить с этапа Подготовка дистрибутивов.

Подготовка дистрибутивов

Дистрибутив Kaspersky Endpoint Security – это комплект файлов для установки и обновления приложения, а также тексты пользовательских соглашений (Лицензионное соглашение и Политика конфиденциальности, Положения о Kaspersky Security Network). Вы также можете отдельно скачать дистрибутив с графическим интерфейсом для удобства локального управления и мониторинга работы приложения.

Дистрибутивы потребуются при создании инсталляционного пакета для развертывания на устройствах в сети организации с помощью Kaspersky Security Center, а также для развертывания приложения через командную строку.

Для развертывания с помощью Kaspersky Security Center вам также потребуется *дистрибутив для удаленной установки приложения*. Дистрибутив содержит файлы, необходимые для удаленного развертывания приложения, и тексты пользовательских соглашений.

> Тексты пользовательских соглашений доступны на сайте "Лаборатории Касперского" (раздел **EULA**), а также в директории `/opt/kaspersky/kesl/doc/` после установки приложения.

Дистрибутивы для развертывания Kaspersky Endpoint Security вы можете выбрать самостоятельно или с помощью Kaspersky Security Center на этапе "Создание инсталляционного пакета".

Как выбрать дистрибутив для развертывания Kaspersky Endpoint Security

Выбор дистрибутивов зависит от следующих факторов:

- Версия Kaspersky Endpoint Security: сертифицированная или несертифицированная.
- Способ развертывания: с помощью Kaspersky Security Center или через командную строку.
- Формат пакета в зависимости от ОС.
- Архитектура ОС и тип процессора.
- Способ управления Kaspersky Endpoint Security.
- Необходимость установки графического интерфейса приложения.

1. **Определите версию приложения – сертифицированная или несертифицированная**

   - Если вам нужна **сертифицированная** версия, скачайте набор дистрибутивов со страницы Жизненного цикла сертифицированных приложений для бизнеса.

     Сертифицированная версия содержит основные файлы приложения и файлы графического интерфейса (директория `kesl`), архив для удаленной установки приложения (директория `remote install`), MMC-плагин (`SCPlugin`) и веб-плагин (`web plugin`).

     Перейдите к пункту 3.

   - Если вам нужна **несертифицированная** версия, перейдите к следующему пункту.

2. **Определите способ развертывания приложения – с помощью Kaspersky Security Center или через командную строку**

   Для **развертывания с помощью Kaspersky Security Center** скачайте дистрибутив с одного из источников:

   - С сайта "Лаборатории Касперского"
   - Через запрос в Службу технической поддержки, если у вас есть Kaspersky CompanyAccount

   Для **развертывания через командную строку** скачайте дистрибутив с сайта "Лаборатории Касперского":

   - Основной дистрибутив приложения (`Distributive`)
   - Если необходимо, дистрибутив с графическим интерфейсом (`Product GUI`)

   Если вы скачиваете дистрибутивы с сайта "Лаборатории Касперского", вам потребуются:

   - Основной дистрибутив приложения (`Distributive`).
   - Если необходимо, дистрибутив с графическим интерфейсом (`Product GUI`).

- Дистрибутив для удаленной установки приложения с помощью Kaspersky Security Center (**Дополнительный дистрибутив** → `Files for Product remote installation`).

- Дистрибутив Агента администрирования Kaspersky Security Center (секция дистрибутивов для Kaspersky Security Center → `Network agent`).

Дистрибутив приложения единый для всех локализаций. Язык приложения определяется при первоначальном конфигурировании Kaspersky Endpoint Security. Поддержка локализации приложения зависит от языков, которые установлены в ОС.

3. **Определите формат пакета в зависимости от операционной системы защищаемого устройства**

Операционная система	Формат пакета
Debian, Ubuntu, Astra Linux, Linux Mint	`.deb`
Red Hat Enterprise Linux, CentOS, Oracle Linux, РЕД ОС, SUSE Linux Enterprise, openSUSE, Rocky Linux, AlmaLinux, ОС из линейки Альт, Гослинукс, ОС из линейки РОСА Linux, Amazon Linux 2023	`.rpm`

Если в таблице нет нужной операционной системы, выберите формат пакета в соответствии с официальной документацией ОС.

4. **Определите архитектуру операционной системы и тип процессора**

Тип процессора и разрядность операционной системы	Дистрибутив
Процессор с архитектурой Arm, 64-битная операционная система	`arm64` `aarch64`
Процессор Эльбрус	`e2k`
Другие процессоры, 32-битная операционная система	`i386`

Другие процессоры, 64-битная операционная система	`x86_64`
	`x64`
	`amd64`

Для установки приложения Kaspersky Endpoint Security на операционные системы с ограниченной поддержкой (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6) выбирайте дистрибутив с пометкой `OLD`.

Самостоятельное изменение конфигурационных файлов приложения способами, не описанными в документации к приложению или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе приложения и операционной системы, снижению уровня защиты вашего устройства, нарушению доступности и целостности обрабатываемой информации, а также включению отправки дополнительных статистик в KSN.

После подготовки дистрибутивов вы можете вернуться в сценарий развертывания и продолжить с этапа Подготовительные действия в Kaspersky Security Center.

Подготовительные действия в Kaspersky Security Center

Перед установкой приложения Kaspersky Endpoint Security рекомендуем выполнить следующие действия в Kaspersky Security Center.

1 Настройка перемещения устройств в группы администрирования

Чтобы управлять приложением с помощью Kaspersky Security Center, нужно поместить устройства с установленным приложением в группы администрирования. По умолчанию Kaspersky Security Center помещает все устройства с установленным Агентом администрирования, подключенным к Серверу администрирования, в группу **Нераспределенные устройства**.

Рекомендуется заранее настроить правила автоматического перемещения устройств в группы администрирования и распределять устройства по группам в соответствии с их типом: для каждого типа устройств создавать отдельную группу. Это позволит вам применять различные настройки приложения в зависимости от особенностей устройства.

Также вы можете помещать устройства в группы администрирования вручную.

2 Установка и первоначальная настройка Агента администрирования

Агент администрирования обеспечивает связь устройства с Сервером администрирования Kaspersky Security Center. Поэтому его требуется установить на каждое устройство, которое будет подключено к Kaspersky Security Center.

1. Подготовьте устройства с ОС Linux для установки Агента администрирования. Набор необходимых действий зависит от операционной системы.

2. Выполните установку и первоначальную настройку Агента администрирования. Описание см. в справке Kaspersky Security Center.

В результате устройства с установленным Агентом администрирования отобразятся в группе, соответствующей настроенным для этих устройств правилам перемещения. Если вы не настроили правила перемещения, устройства отобразятся в группе **Нераспределенные устройства**.

3 Установка плагина управления Kaspersky Endpoint Security

Установите плагин управления Kaspersky Endpoint Security в зависимости от консоли управления Kaspersky Security Center, которую вы используете:

- **MMC-плагин управления Kaspersky Endpoint Security** позволяет управлять работой приложения через Консоль администрирования Kaspersky Security Center. MMC-плагин устанавливается на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

  Как установить MMC-плагин Kaspersky Endpoint Security

  > Перед установкой MMC-плагина управления Kaspersky Endpoint Security убедитесь, что установлены Kaspersky Security Center и Redist C++ 2015 (Microsoft Visual C++ 2015 Redistributable).

  Чтобы установить MMC-плагин:

  1. Скачайте файл klcfginst.msi на странице загрузки приложений в разделе **Kaspersky Endpoint Security для Linux** (**Build** → **Administration Plug-In**).
  2. На устройстве, где установлена Консоль администрирования Kaspersky Security Center, запустите файл klcfginst.msi.

  После установки MMC-плагин управления отображается в списке установленных MMC-плагинов управления в свойствах Сервера администрирования Kaspersky Security Center.

  Чтобы посмотреть список установленных MMC-плагинов управления:

  1. В дереве Консоли администрирования Kaspersky Security Center выберите узел **Сервер администрирования <имя сервера>** и откройте окно свойств Сервера администрирования одним из следующих способов:
     - откройте контекстное меню узла **Сервер администрирования <имя сервера>** и выберите пункт **Свойства**;
     - перейдите по ссылке **Свойства Сервера администрирования**, расположенной в рабочей области узла **Сервер администрирования <имя сервера>** в блоке **Сервер администрирования**.
  2. В списке слева в разделе **Дополнительно** выберите раздел **Информация об установленных плагинах управления программами**.

     В правой части окна в списке установленных плагинов управления отображается MMC-плагин управления Kaspersky Endpoint Security: **Kaspersky Endpoint Security <номер версии> для Linux**.

  Если для управления приложением Kaspersky Endpoint Security вы используете Консоль администрирования Kaspersky Security Center и у вас установлено несколько версий приложения, вам нужно установить плагины управления для разных версий приложения Kaspersky Endpoint Security. Таким образом вы сможете управлять приложением, используя политики, созданные с помощью разных версий плагина управления. Вы также можете конвертировать политики и задачи, созданные с помощью предыдущих версий плагина управления, в новые версии.

- **Веб-плагин управления Kaspersky Endpoint Security** позволяет управлять работой приложения через Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console. Веб-плагин устанавливается на устройстве с установленным приложением Kaspersky Security Center Web Console. Функции веб-плагина доступны всем администраторам, у которых есть доступ к Kaspersky Security Center Web Console в браузере.

  Как установить веб-плагин Kaspersky Endpoint Security

  Вы можете установить веб-плагин:

  - С помощью мастера первоначальной настройки Kaspersky Security Center Web Console.

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

  - Вручную, используя дистрибутив из списка веб-плагинов "Лаборатории Касперского" или из файла.

  Чтобы установить веб-плагин Kaspersky Endpoint Security вручную из Kaspersky Security Center:

  1. В главном окне Kaspersky Security Center Web Console выберите **Параметры** → **Веб-плагины**.

     Откроется список установленных веб-плагинов.

  2. Нажмите на кнопку **Добавить**.

     Откроется список доступных плагинов управления. Список обновляется автоматически после выпуска новых версий веб-плагинов.

  3. В списке доступных плагинов выберите веб-плагин **Kaspersky Endpoint Security <номер версии> для Linux**.

  4. В открывшемся окне с описанием веб-плагина нажмите на кнопку **Установить плагин**.

  5. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

  Новый плагин отобразится в списке установленных веб-плагинов (**Параметры** → **Веб-плагины**).

  Чтобы установить веб-плагин Kaspersky Endpoint Security вручную из файла:

  1. Скачайте архив с веб-плагином на странице загрузки приложений в разделе **Kaspersky Endpoint Security для Linux** (**Дополнительный дистрибутив** → **Web console Plug-In**).

  2. Локально распакуйте скачанный архив.

  3. В главном окне Kaspersky Security Center Web Console выберите **Параметры** → **Веб-плагины**.

     Откроется список установленных веб-плагинов.

  4. Нажмите на кнопку **Добавить из файла**.

  5. В открывшемся окне укажите путь к файлу plugin.zip и путь к файлу с signature.txt. Файлы находятся в папке, куда вы распаковали архив с веб-плагином.

6. Нажмите на кнопку **Добавить**.

7. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новый плагин отображается в списке установленных веб-плагинов (**Параметры** → **Веб-плагины**).

Если в свойствах Сервера администрирования Kaspersky Security Center вы выбрали язык, которого нет в дистрибутиве приложения Kaspersky Endpoint Security, то Лицензионное соглашение и весь интерфейс в Kaspersky Security Center Web Console будут отображаться на английском языке.

Видео: установка веб-плагина управления с помощью мастера

Видео: установка веб-плагина управления в изолированных сетях

4 Создание политики Kaspersky Endpoint Security

Создайте политику для приложения Kaspersky Endpoint Security в Kaspersky Security Center Web Console или в Консоли администрирования (в зависимости от консоли управления Kaspersky Security Center, которую вы используете).

Укажите следующие настройки в зависимости от режима, в котором вы хотите использовать приложение:

Для стандартного режима

Если вы создали политику в мастере Консоли администрирования, укажите режим использования приложения: **Стандартный режим или режим Агента Endpoint Detection and Response**. Если вы создали политику в мастере Kaspersky Security Center Web Console, пропустите выбор режима использования приложения.

Для режима EDR-агента

1. Если вы создали политику в мастере Консоли администрирования, укажите режим использования приложения: **Стандартный режим или режим Агента Endpoint Detection and Response**. Если вы создали политику в мастере Kaspersky Security Center Web Console, пропустите выбор режима использования приложения.

2. Завершите создание политики, следуя указаниям мастера.

3. Откройте свойства созданной политики в Kaspersky Security Center Web Console или в Консоли администрирования и включите интеграцию с решениями Detection and Response, которые вы хотите использовать для защиты устройства:

   - Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) на платформе OSMP вам нужно включить и настроить компонент EDR Expert (on-premises). Параметры доступны в Kaspersky Security Center Web Console.

   - Для интеграции с Kaspersky Endpoint Detection and Response на платформе Kaspersky Anti Targeted Attack Platform вам нужно включить и настроить компонент EDR Expert (on-premises). Параметры доступны в Kaspersky Security Center Web Console и в Консоли администрирования.

   - Для интеграции с Kaspersky Network Detection and Response на платформе Kaspersky Anti Targeted Attack Platform вам нужно включить и настроить компонент NDR (KATA). Параметры доступны в Kaspersky Security Center Web Console и в Консоли администрирования.

Для режима Легкого агента

В мастере создания политики:

1. Укажите режим использования приложения: **Режим Легкого агента для защиты виртуальных сред**.

2. Настройте параметры обнаружения SVM:

   a. Выберите способ, который используют Легкие агенты для обнаружения доступных для подключения SVM:

      - **Использовать Сервер интеграции**. Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них.

      - **Использовать список адресов SVM, заданный вручную**. Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.

      Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур, то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Игнорировать**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM. Подробнее см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

b. Если вы выбрали Сервер интеграции, в окне мастера отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. Если требуется, укажите новые параметры подключения: IP-адрес в формате IPv4 или полное доменное имя (FQDN) и порт для подключения к Серверу интеграции.

> Если в вашей инфраструктуре развернут отказоустойчивый кластер Серверов интеграции на базе Linux, в качестве адреса и порта для подключения к Серверу интеграции вам нужно указать адрес и порт балансировщика нагрузки. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент.

c. Если вы выбрали список адресов SVM, заданный вручную, сформируйте список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Чтобы добавить SVM в список, нажмите на кнопку **Добавить** и в открывшемся окне укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки.

> Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения.

Для остальных настроек политики можно использовать значения, установленные по умолчанию. Заданные по умолчанию настройки обеспечивают базовый уровень защиты. После установки приложения Kaspersky Endpoint Security вы можете настроить политику в соответствии с требованиями вашей организации. Для этого в разделе справки Работа с приложением воспользуйтесь сценариями настройки компонентов.

Видео: создание политики

5 Настройка централизованного обновления баз и модулей приложения

По умолчанию приложение Kaspersky Endpoint Security устанавливается на устройство без антивирусных баз. Приложение начинает выполнять свои функции только после загрузки баз на устройство. Чтобы обеспечить защиту сразу после установки приложения, настройте централизованное обновление баз.

В Kaspersky Security Center Web Console или в Консоли администрирования (в зависимости от консоли управления Kaspersky Security Center, которую вы используете):

1. Запустите задачу Сервера администрирования *Загрузка обновлений в хранилище Сервера администрирования*. Задача создается автоматически мастером первоначальной настройки Сервера администрирования.

   В результате выполнения задачи пакет обновлений для приложения Kaspersky Endpoint Security загружается в папку для хранения обновлений на Сервере администрирования.

2. Создайте групповую задачу для приложения Kaspersky Endpoint Security типа *Обновление*. В параметрах задачи укажите:

   - источник обновлений – Kaspersky Security Center;
   - расписание запуска задачи – минимум один раз в день. Рекомендуется запускать задачу 4-6 раз в день.

Видео: настройка централизованного обновления баз

6 Добавление лицензионных ключей и создание задачи активации

Для активации приложения в стандартном режиме нужно добавить в приложение лицензионный ключ. Если какие-то компоненты не включены в вашу лицензию, вам может потребоваться еще один лицензионный ключ.

Для активации приложения Kaspersky Endpoint Security в режиме EDR-агента вам потребуется лицензионный ключ EDR Expert (on-premises).

Вы можете использовать подходящий способ активации в зависимости от вашей инфраструктуры и требований вашей организации:

- Если на всех ваших устройствах установлено приложение с одним объемом функциональности, используйте механизм автоматического распространения лицензионных ключей. Перед распространением лицензионный ключ надо добавить в хранилище ключей Kaspersky Security Center с помощью файла ключа или кода активации. См. подробнее в справке Kaspersky Security Center.
- Если на ваших устройствах установлено приложение с разным объемом функциональности, то для активации требуются разные лицензионные ключи. В этом случае поместите защищаемые устройства в разные группы администрирования и настройте групповую задачу добавления ключа для каждой группы администрирования.

Kaspersky Endpoint Security в режиме Легкого агента получает информацию о лицензии от Сервера защиты после подключения к SVM. Отдельно активировать Kaspersky Endpoint Security в режиме Легкого агента не требуется.

Видео: активация приложения с помощью кода активации

Видео: активация приложения с помощью файла ключа

После того как вы подготовили Kaspersky Security Center, вы можете вернуться в сценарий развертывания и продолжить с этапа Установка приложения.

Установка с помощью Kaspersky Security Center

Особенности установки:

- На устройствах с процессором Эльбрус не поддерживается использование Kaspersky Endpoint Security в режиме EDR-агента и в режиме Легкого агента.
- На устройствах на базе архитектуры Arm не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента.

Рекомендуемый сценарий установки приложения с помощью Kaspersky Security Center состоит из следующих этапов.

Также вы можете установить приложение Kaspersky Endpoint Security с помощью Kaspersky Security Center, используя мастер первоначальной настройки и мастер развертывания защиты.

1 Создание инсталляционного пакета

Инсталляционный пакет приложения Kaspersky Endpoint Security содержит:

- основной дистрибутив,
- дистрибутив для удаленной установки приложения,
- дистрибутив с графическим интерфейсом приложения,
- параметры первоначальной настройки приложения, которые применяются в ходе установки.

Вы можете создать инсталляционный пакет следующими способами:

- **С помощью дистрибутива, размещенного на серверах "Лаборатории Касперского"**. В Kaspersky Security Center инсталляционный пакет создается автоматически из указанного дистрибутива.

  Видео: создание инсталляционного пакета автоматически в Kaspersky Security Center

  Для установки приложения Kaspersky Endpoint Security на операционные системы с ограниченной поддержкой (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6) выбирайте дистрибутив с пометкой `для устаревших ОС` / `for legacy OS`.

- **Вручную с помощью файлов, подготовленных на этапе Подготовка дистрибутивов**. Этот способ рекомендуется, если вы хотите задавать параметры первоначальной настройки приложения с помощью конфигурационного файла или если вы хотите использовать создаваемый инсталляционный пакет для разных операционных систем или разных менеджеров пакетов.

Видео: создание инсталляционного пакета вручную из файла в Kaspersky Security Center

Вы можете добавить в инсталляционный пакет предварительно скачанные базы приложения. Если для установки используется инсталляционный пакет с интегрированными базами, приложение устанавливается с рабочими базами, обновлять базы сразу после установки не требуется.

Вы можете использовать один и тот же инсталляционный пакет многократно.

Как подготовить инсталляционный пакет вручную

1. Локально распакуйте архив с файлами для удаленной установки Kaspersky Endpoint Security.

2. В ту же папку поместите пакеты с основными файлами приложения.

   Если вы хотите использовать создаваемый инсталляционный пакет для разных операционных систем или разных менеджеров пакетов, поместите в папку дистрибутивы для всех необходимых типов операционных систем и менеджеров пакетов.

3. Если вы планируете использовать графический интерфейс приложения, в ту же папку поместите пакеты с файлами графического интерфейса.

   Включите использование графического интерфейса, настроив соответствующий параметр в свойствах созданного инсталляционного пакета или в конфигурационном файле autoinstall.ini (`USE_GUI=Yes`). По умолчанию использование графического интерфейса выключено.

   > Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, графический интерфейс не поддерживается.

4. Если вы хотите задать параметры первоначальной настройки приложения с помощью конфигурационного файла, откройте конфигурационный файл autoinstall.ini и внесите необходимые изменения. Файл autoinstall.ini находится в папке, в которую вы распаковали архив с файлами для удаленной установки Kaspersky Endpoint Security.

   a. По умолчанию приложение используется в стандартном режиме.

      Чтобы использовать приложение в режиме EDR-агента, установите значение параметра `ENDPOINT_AGENT_MODE=Yes`.

      Чтобы использовать приложение в режиме Легкого агента, установите значение параметра `KSVLA_MODE=Yes`.

      > После установки Kaspersky Endpoint Security изменить режим использования приложения невозможно.

b. Для установки приложения в режиме Легкого агента:

- Если вы устанавливаете приложение на шаблон, из которого будут создаваться временные виртуальные машины, установите значение параметра `VDI_MODE=Yes`. Этот параметр включает режим защиты инфраструктуры VDI для оптимизации работы приложения на временных виртуальных машинах.

- Укажите роль виртуальных машин, которые вы хотите защищать, в виртуальной инфраструктуре: сервер или рабочая станция (`SERVER_MODE=Yes|No`). Роль виртуальной машины определяет, по какой лицензии будет использоваться приложение на этой виртуальной машине, и объем доступной функциональности.

Вы также можете изменить параметры первоначальной настройки приложения позже, в свойствах созданного инсталляционного пакета на вкладке **Параметры**.

5. Поместите все подготовленные файлы в архив формата ZIP, CAB, TAR или TAR.GZ с произвольным именем.

Как создать инсталляционный пакет в Web Console

1. В главном окне Web Console выберите один из следующих разделов:

   - **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

   - **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета.

3. Если вы работаете в Web Console, выберите способ создания инсталляционного пакета:

   - **Создать инсталляционный пакет из файла**. Инсталляционный пакет будет создан из архивного файла, который вы подготовили предварительно.

   - **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**. Инсталляционный пакет будет создан из дистрибутива, размещенного на серверах "Лаборатории Касперского".

   Если вы работаете в облачной консоли Kaspersky Security Center Cloud Console, инсталляционный пакет будет создан из дистрибутива, размещенного на серверах "Лаборатории Касперского"

4. В зависимости от способа создания пакета:

   - Укажите имя пакета, нажмите на кнопку **Обзор** и укажите путь к архиву, который вы подготовили для создания инсталляционного пакета.

   - Выберите дистрибутив приложения Kaspersky Endpoint Security. В окне справа ознакомьтесь с информацией о дистрибутиве и нажмите на кнопку **Скачать и создать инсталляционный пакет**. Запустится процесс создания инсталляционного пакета.

5. Ознакомьтесь с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и с Политикой конфиденциальности, которая описывает обработку и передачу данных. Для продолжения создания инсталляционного пакета требуется подтвердить, что вы полностью прочитали и принимаете условия Лицензионного соглашения и Политики конфиденциальности.

6. Завершите работу мастера.

   Инсталляционный пакет будет создан и добавлен в список инсталляционных пакетов.

7. Откройте свойства инсталляционного пакета и перейдите на вкладку **Параметры**.

   - Если вы устанавливаете приложение в режиме EDR-агента, для параметра **Режим использования приложения** выберите вариант **Агент Endpoint Detection and Response**.

   - Если вы устанавливаете приложение в режиме Легкого агента, настройте следующие параметры:

     Режим использования приложения – выберите вариант **Легкий агент для защиты виртуальных сред**.

     Включить режим защиты инфраструктуры VDI. Установите флажок, чтобы включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки приложения на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. По умолчанию флажок снят.

     Защищаемая виртуальная машина используется как сервер. Роль виртуальной машины, на которую будет установлено приложение: сервер или рабочая станция. По умолчанию флажок установлен (виртуальная машина используется в виртуальной инфраструктуре как сервер).

   - Если требуется, измените другие параметры первоначальной настройки приложения, заданные по умолчанию.

     Описание всех параметров первоначальной настройки приложения в инсталляционном пакете см. в Приложении 1.

Как создать инсталляционный пакет в Консоли администрирования

Чтобы создать инсталляционный пакет, используя предварительно подготовленные файлы:

1. В дереве консоли выберите **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

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

   Запустится мастер создания инсталляционного пакета.

3. Нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.

4. Введите имя нового инсталляционного пакета и перейдите к следующему шагу мастера.

5. Укажите путь к файлу kesl.kud. Файл находится в папке, в которую вы распаковали архив с файлами для удаленной установки приложения (kesl.zip) на этапе Подготовка дистрибутивов.

   В окне отобразится название и версия приложения. Перейдите к следующему шагу мастера.

6. Ознакомьтесь с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и с Политикой конфиденциальности, которая описывает обработку и передачу данных.

   Чтобы продолжить, подтвердите, что вы полностью прочитали и принимаете условия Лицензионного соглашения и Политики конфиденциальности. Для подтверждения установите оба флажка в открывшемся окне.

   Перейдите к следующему шагу мастера.

7. Мастер загружает файлы, необходимые для установки приложения, на Сервер администрирования Kaspersky Security Center. Дождитесь завершения загрузки и завершите работу мастера.

8. Откройте свойства инсталляционного пакета и перейдите на вкладку **Параметры приложения**.

   - Если вы устанавливаете приложение в режиме EDR-агента, для параметра **Режим использования приложения** выберите вариант **Агент Endpoint Detection and Response**.

   - Если вы устанавливаете приложение в режиме Легкого агента, настройте следующие параметры:

     Режим использования приложения – выберите вариант **Легкий агент для защиты виртуальных сред**

     Включить режим защиты инфраструктуры VDI. Установите флажок, чтобы включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки приложения на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. По умолчанию флажок снят.

     Защищаемая виртуальная машина используется как сервер. Роль виртуальной машины, на которую будет установлено приложение: сервер или рабочая станция. По умолчанию флажок установлен.

     В режиме Легкого агента недоступны:

     - настройка источников обновления баз приложения и запуск обновления;
     - настройка параметров прокси-сервера;
     - активация приложения.

     Приложение в режиме Легкого агента получает необходимые обновления баз и информацию о лицензии от Сервера защиты после подключения к SVM. Отдельно активировать Kaspersky Endpoint Security и настраивать обновление баз не требуется.

   - Если требуется, измените другие параметры первоначальной настройки приложения, заданные по умолчанию.

     Описание всех параметров первоначальной настройки приложения в инсталляционном пакете см. в Приложении 1.

   Вы можете настроить параметры первоначальной настройки приложения позже, в свойствах созданного инсталляционного пакета в разделе **Параметры приложения**.

Чтобы создать инсталляционный пакет, используя дистрибутив, размещенный на серверах "Лаборатории Касперского":

1. В дереве консоли выберите **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

2. Нажмите на кнопку **Дополнительные действия** → **Просмотреть актуальные версии программ "Лаборатории Касперского"**.

3. Выберите в списке дистрибутив приложения Kaspersky Endpoint Security и нажмите на кнопку **Загрузить и создать инсталляционный пакет**.

4. Ознакомьтесь с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и с Политикой конфиденциальности, которая описывает обработку и передачу данных.

   Чтобы продолжить, подтвердите, что вы полностью прочитали и принимаете условия Лицензионного соглашения и Политики конфиденциальности. Для подтверждения установите оба флажка в открывшемся окне и нажмите на кнопку **Принять все**.

5. Дождитесь завершения загрузки. Инсталляционный пакет будет создан и добавлен в список инсталляционных пакетов.

6. Откройте свойства инсталляционного пакета и перейдите в раздел **Параметры приложения**.

- Если вы устанавливаете приложение в режиме EDR-агента, для параметра **Режим использования приложения** выберите вариант **Агент Endpoint Detection and Response**.

- Если вы устанавливаете приложение в режиме Легкого агента, настройте следующие параметры:

  Режим использования приложения – выберите вариант **Легкий агент для защиты виртуальных сред**

  Включить режим защиты инфраструктуры VDI. Установите флажок, чтобы включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки приложения на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. По умолчанию флажок снят.

  Защищаемая виртуальная машина используется как сервер. Роль виртуальной машины, на которую будет установлено приложение: сервер или рабочая станция. По умолчанию флажок установлен.

  В режиме Легкого агента недоступны следующие параметры:

  - настройка источников обновления баз приложения и запуск обновления;
  - настройка параметров прокси-сервера;
  - активация приложения.

  Приложение в режиме Легкого агента получает необходимые обновления баз и информацию о лицензии от Сервера защиты после подключения к SVM. Отдельно активировать Kaspersky Endpoint Security и настраивать обновление баз не требуется.

- Если требуется, измените другие параметры первоначальной настройки приложения, заданные по умолчанию.

  Описание всех параметров первоначальной настройки приложения в инсталляционном пакете см. в Приложении 1.

Вы можете настроить параметры первоначальной настройки приложения позже, в свойствах созданного инсталляционного пакета в разделе **Параметры приложения**.

2 Установка приложения на устройствах в сети организации

Установите приложение через Kaspersky Security Center с помощью задачи удаленной установки приложений.

При необходимости вы можете посмотреть журнал удаленной установки приложения с помощью удаленной диагностики клиентского устройства Kaspersky Security Center.

Первоначальная настройка приложения выполняется автоматически в соответствии с параметрами в свойствах инсталляционного пакета или в конфигурационном файле, который включен в инсталляционный пакет.

Видео: установка, обновление баз и проверка работоспособности Kaspersky Endpoint Security

3 Обновление баз приложения

Если вы установили приложение в стандартном режиме или в режиме EDR-агента, запустите групповую задачу *Обновление*, созданную на этапе "Настройка централизованного обновления баз и модулей приложения", в Web Console или в Консоли администрирования (в зависимости от консоли управления Kaspersky Security Center, которую вы используете). Подробнее об обновлении баз Kaspersky Endpoint Security см. в разделе Обновление баз и модулей приложения.

4 Проверка работоспособности приложения

В результате приложение Kaspersky Endpoint Security установлено, активировано и обновлены базы приложения. После установки приложение запускается автоматически. По умолчанию включаются следующие компоненты:

- Защита от файловых угроз.
- Контроль устройств.
- Анализ поведения.
- Защита от веб-угроз – только если в операционной системе установлен один из поддерживаемых браузеров и на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в свойствах политики не установлен).
- Защита от сетевых угроз – только если параметры защиты от сетевых угроз на устройстве заданы через политику. По умолчанию в свойствах политики включена защита от сетевых угроз. Если на устройстве применяются локально настроенные параметры, по умолчанию защита от сетевых угроз выключена.

Убедитесь, что приложение готово к работе.

Как проверить состояние защиты устройства в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Чтобы выбрать вложенную группу, нажмите на кнопку **Показать иерархию** в верхней части окна.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. Нажмите на имя устройства.

   Откроется окно свойств управляемого устройства.

4. На вкладке **Общие** выберите раздел **Защита**. В поле **Статус устройства** должно отображаться *OK*.

   Если в поле **Статус устройства** отображается информация о том, что нет прав на системные директории, локально на этом устройстве проверьте права для следующих директорий: /var/opt/kaspersky, /var/log/kaspersky и /opt/kaspersky. Убедитесь, что владельцем является учетная запись root и только владелец имеет право на запись в эти директории.

5. Перейдите на вкладку **Приложения**.

6. В списке приложений, установленных на устройстве, нажмите на название приложения Kaspersky Endpoint Security.

   Откроется окно свойств приложения.

7. Посмотрите блок **Базы приложения** на вкладке **Общие** в разделе **Информация**. Убедитесь, что базы приложения обновлены.

8. Перейдите в раздел **Лицензии** на вкладке **Общие** и убедитесь, что приложение активировано.

9. Если вы установили приложение в режиме EDR-агента, перейдите в раздел **Компоненты** на вкладке **Общие** и убедитесь, что для интеграций, которые вы настроили на этапе "Создание политики Kaspersky Endpoint Security", отображается статус *Выполняется*.

10. Если вы установили приложение в режиме Легкого агента, перейдите в раздел **Компоненты** на вкладке **Общие** и убедитесь, что в строке **Режим Легкого агента для защиты виртуальных сред** отображается статус *выполняется*. Это означает, что приложение используется в режиме Легкого агента.

Как проверить состояние защиты устройства в Консоли администрирования

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.

2. В рабочей области выберите вкладку **Устройства**.

3. В списке управляемых устройств выберите нужное вам устройство и откройте окно **Свойства: <Имя устройства>** двойным щелчком мыши.

   Откроется окно свойств управляемого устройства.

4. Выберите раздел **Защита**. В поле **Статус устройства** должно отображаться *OK/Видим в сети*.

   Если в поле **Статус устройства** отображается информация о том, что нет прав на системные директории, локально на этом устройстве проверьте права для следующих директорий: /var/opt/kaspersky, /var/log/kaspersky и /opt/kaspersky. Убедитесь, что владельцем является учетная запись root и только владелец имеет право на запись в эти директории.

5. Перейдите в раздел **Программы**.

6. В списке приложений, установленных на устройстве, выберите приложение Kaspersky Endpoint Security и откройте окно свойств приложения двойным щелчком мыши.

7. Посмотрите поле **Базы программы** в разделе **Общие**. Убедитесь, что базы приложения обновлены.

8. Перейдите в раздел **Лицензионные ключи** и убедитесь, что приложение активировано.

9. Если вы установили приложение в режиме EDR-агента, перейдите в раздел **Компоненты** и убедитесь, что для интеграций, которые вы настроили на этапе "Создание политики Kaspersky Endpoint Security", отображается статус *Выполняется*.

10. Если вы установили приложение в режиме Легкого агента, перейдите в раздел **Компоненты** и убедитесь, что в строке **Режим Легкого агента для защиты виртуальных сред** отображается статус *Выполняется*. Это означает, что приложение используется в режиме Легкого агента.

Полезные статьи

Что делать, если не выполняются задачи или не применяются политики

Что делать, если устройство в статусе "Недопустимые параметры политики. Политика не была применена"

Ошибка "Приложение не поддерживается текущей версией Kaspersky Security Center Web Console или не установлен веб-плагин для приложения"

Как решить проблему при установке графического интерфейса

Описание кодов ошибок установки

Ошибки после установки Kaspersky Endpoint Security

После того как вы установили Kaspersky Endpoint Security, вы можете вернуться в сценарий развертывания и продолжить с этапа Дополнительная настройка после установки в отдельных ОС.

Установка с помощью командной строки

Особенности установки:

- На устройствах с процессором Эльбрус не поддерживается использование Kaspersky Endpoint Security в режиме EDR-агента и в режиме Легкого агента.
- На устройствах на базе архитектуры Arm не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента.
- Установку приложения и графического интерфейса требуется выполнять с root-правами.
- Мастер первоначальной настройки требуется запускать с root-правами.
- Если версия менеджера пакетов apt ниже 1.1.X, требуется использовать для установки менеджер пакетов dpkg (в зависимости от операционной системы).

Рекомендуемый сценарий установки приложения с помощью командной строки состоит из следующих этапов.

1 Установка приложения Kaspersky Endpoint Security

Перед началом установки поместите скачанный пакет с основными файлами приложения в директорию /tmp на устройстве.

Как установить приложение из пакета формата RPM

На 32-битную операционную систему

```
yum install kesl-12.5.0-<build number>.i386.rpm
```

На 64-битную операционную систему

```
yum install kesl-12.5.0-<build number>.x86_64.rpm
```

На 64-битную операционную систему из линейки Альт

```
apt-get install kesl-12.5.0-<build number>.x86_64.rpm
```

На 64-битную операционную систему для архитектуры Arm

```
yum install kesl-12.5.0-<build number>.aarch64.rpm
```

На 64-битную операционную систему из линейки Альт для архитектуры Arm

```
apt-get install kesl-12.5.0-<build number>.aarch64.rpm
```

На 64-битную операционную систему для архитектуры Эльбрус

```
yum install kesl-12.5.0-<build number>.2ek.rpm
```

На 64-битную операционную систему из линейки Альт для архитектуры Эльбрус

```
apt-get install kesl-12.5.0-<build number>.2ek.rpm
```

На 64-битную операционную систему с ограниченной поддержкой (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6)

```
rpm -i kesl-12.5.0-<build number>.x86_64.rpm
```

Для установки приложения на CentOS 5.2, CentOS 5.4, CentOS 6.4 или CentOS 6.6 вам нужно скачать с сайта дистрибутив с пометкой OLD.

Как установить приложение из пакета формата DEB

На 32-битную операционную систему

```
apt-get install ./kesl_12.5.0-<build number>_i386.deb
```

На 64-битную операционную систему

```
apt-get install ./kesl_12.5.0-<build number>_amd64.deb
```

На 64-битную операционную систему для архитектуры Arm

```
apt-get install ./kesl_12.5.0-<build number>_arm64.deb
```

На 64-битную операционную систему для архитектуры Эльбрус

```
apt-get install ./kesl_12.5.0-<build number>_2ek.deb
```

2 Установка графического интерфейса приложения

Если вы планируете управлять приложением через графический интерфейс, вам нужно установить графический интерфейс на устройстве, где установлено приложение.

Особенности графического интерфейса приложения:

- Невозможно установить графический интерфейс на устройстве, где не установлено приложение Kaspersky Endpoint Security.
- Если приложение используется в режиме Легкого агента, графический интерфейс не поддерживается.

Перед началом установки поместите скачанный пакет с файлами графического интерфейса приложения в директорию /tmp на устройстве.

Как установить графический интерфейс приложения из пакета формата RPM

На 32-битную операционную систему

```
yum install kesl-gui-12.5.0-<build number>.i386.rpm
```

На 64-битную операционную систему

```
yum install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

На 64-битную операционную систему из линейки Альт

```
apt-get install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

На 64-битную операционную систему для архитектуры Arm

```
yum install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

На 64-битную операционную систему из линейки Альт для архитектуры Arm

```
apt-get install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

На 64-битную операционную систему на архитектуры Эльбрус

```
yum install kesl-gui-12.5.0-<build number>.2ek.rpm
```

На 64-битную операционную систему из линейки Альт на архитектуры Эльбрус

```
apt-get install kesl-gui-12.5.0-<build number>.2ek.rpm
```

На 64-битную операционную систему с ограниченной поддержкой (CentOS 6.4, CentOS 6.6)

```
rpm -i kesl-gui-12.5.0-<build number>.x86_64.rpm
```

Для установки приложения на CentOS 6.4 или CentOS 6.6 вам надо скачать с сайта дистрибутив с пометкой OLD.

Как установить графический интерфейс приложения из пакета формата DEB

На 32-битную операционную систему

```
apt-get install ./kesl-gui_12.5.0-<build number>_i386.deb
```

На 64-битную операционную систему

```
apt-get install ./kesl-gui_12.5.0-<build number>_amd64.deb
```

На 64-битную операционную систему для архитектуры Arm

```
apt-get install ./kesl-gui_12.5.0-<build number>_arm64.deb
```

На 64-битную операционную систему для архитектуры Эльбрус

```
apt-get install ./kesl-gui_12.5.0-<build number>_2ek.deb
```

3 Первоначальная настройка приложения

Первоначальная настройка требуется для подготовки приложения к работе и включения защиты клиентского устройства.

Если не выполнена первоначальная настройка приложения на устройстве, вы не сможете использовать приложение и обновлять версию приложения на этом устройстве.

Первоначальная настройка приложения выполняется с помощью мастера первоначальной настройки, который входит в комплект поставки приложения Kaspersky Endpoint Security. Вы можете выполнить первоначальную настройку в интерактивном режиме или в автоматическом режиме.

Как выполнить первоначальную настройку в интерактивном режиме

Шаг 1. Запуск мастера

Запустить мастер первоначальной настройки

```
/opt/kaspersky/kesl/bin/kesl-setup.pl
```

По запросу мастера пошагово укажите значения параметров первоначальной настройки Kaspersky Endpoint Security.

Если на устройстве установлен Агент администрирования и вы устанавливаете приложение в стандартном режиме или режиме EDR-агента, шаги мастера первоначальной настройки, связанные с обновлением баз и активацией приложения, могут пропускаться.

Шаг 2. Выбор режима использования: стандартный или Легкий агент

Введите `yes`, чтобы использовать приложение в режиме Легкого агента.

Введите `no`, чтобы использовать приложение в стандартном режиме.

Если вы планируете использовать приложение в режиме EDR-агента, на этом шаге вам нужно ввести `no` и на следующем шаге выбрать режим EDR-агента.

После завершения первоначальной настройки изменить режим использования приложения невозможно.

Шаг 3. Выбор режима использования: стандартный или Агент Endpoint Detection and Response

Шаг отображается, если на шаге 2 вы выбрали использование приложение в стандартном режиме.

Введите `yes`, чтобы использовать приложение в режиме EDR-агента.

Введите `no`, чтобы использовать приложение в стандартном режиме.

После завершения первоначальной настройки изменить режим использования приложения невозможно.

Шаг 4. Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud)

Шаг отображается, если на шаге 3 вы выбрали использование приложение в стандартном режиме.

Введите `yes`, чтобы использовать интеграцию с Kaspersky Endpoint Detection and Response Expert (cloud).

Введите `no`, чтобы использовать интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises).

Шаг 5. Определение роли виртуальной машины

Шаг отображается, если на шаге 2 вы выбрали использование приложение в режиме Легкого агента.

Укажите роль виртуальной машины (сервер или рабочая станция), на которую вы устанавливаете приложение Kaspersky Endpoint Security:

- Введите `yes`, если вы используете виртуальную машину как сервер.
- Введите `no`, если вы используете виртуальную машину как рабочую станцию.

Роль виртуальной машины определяет, по какой лицензии будет использоваться приложение на этой виртуальной машине, и объем доступной функциональности.

Шаг 6. Включение режима защиты инфраструктуры VDI

Шаг отображается, если на шаге 2 вы выбрали использование приложение в режиме Легкого агента.

Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах. Если режим защиты инфраструктуры VDI включен, то обновления, требующие перезагрузки виртуальной машины, не устанавливаются. При получении обновлений, требующих перезагрузки, Легкий агент, установленный на виртуальной машине, отправляет в Kaspersky Security Center сообщение о необходимости обновить шаблон защищенных виртуальных машин.

Введите `yes`, если вы хотите включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки Kaspersky Endpoint Security на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины.

Введите `no`, если не требуется включать режим защиты инфраструктуры VDI. Рекомендуется в случае установки Kaspersky Endpoint Security на постоянную виртуальную машину или на шаблон виртуальных машин, из которого будут создаваться постоянные виртуальные машины.

Шаг 7. Выбор языкового стандарта

На этом шаге мастер выводит список поддерживаемых языковых стандартов в формате, определенном в RFC 3066.

Укажите языковой стандарт в том формате, в котором он приведен в списке. Этот стандарт будет использоваться:

- для локализации текстов Лицензионного соглашения, Политики конфиденциальности и Положения о Kaspersky Security Network, которые отображаются во время первоначальной установки;
- для локализации событий приложения, отправляемых в Kaspersky Security Center.

Для отображения графического интерфейса и командной строки приложения используется локализация, указанная в переменной окружения `LANG`. Если приложение не поддерживает указанную локализацию, то используется английская локализация.

Шаг 8. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге ознакомьтесь с текстами Лицензионного соглашения, которое заключается между вами и "Лабораторией Касперского" и Политики конфиденциальности, которая описывает обработку и передачу данных.

Шаг 9. Принятие Лицензионного соглашения

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`), если вы принимаете условия Лицензионного соглашения.
- `no` (или `n`), если вы не принимаете условия Лицензионного соглашения.

Если вы не приняли условия Лицензионного соглашения, настройка приложения Kaspersky Endpoint Security прерывается.

Шаг 10. Принятие Политики конфиденциальности

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`), если вы принимаете условия Политики конфиденциальности;
- `no` (или `n`), если вы не принимаете условия Политики конфиденциальности.

Если вы не приняли условия Политики конфиденциальности, настройка приложения Kaspersky Endpoint Security прерывается.

Шаг 11. Использование Kaspersky Security Network

На этом шаге примите или отклоните условия использования Kaspersky Security Network:

- введите `yes` (или `y`), если вы принимаете условия Положения о Kaspersky Security Network. Будет включен расширенный режим KSN.
- введите `no` (или `n`), если вы не принимаете условия Положения о Kaspersky Security Network.

Файл ksn_license.<ID языка> с текстом Положения о Kaspersky Security Network находится в директории /opt/kaspersky/kesl/doc/.

Отказ от использования Kaspersky Security Network не прерывает процесс первоначальной настройки приложения Kaspersky Endpoint Security. Вы можете включить, выключить или изменить режим Kaspersky Security Network в любой момент.

Если вы включили использование Kaspersky Security Network, автоматически включается облачный режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО.

Шаг 12. Удаление пользователей из привилегированных групп

Шаг отображается, если обнаружены пользователи в группе kesladmin и/или в группе keslaudit.

Укажите, следует ли удалить пользователей из привилегированных групп kesladmin и keslaudit. Пользователи, включенные в группы kesladmin и keslaudit, получают привилегированный доступ к функциям приложения.

Введите `yes`, чтобы удалить всех обнаруженных пользователей из группы kesladmin и/или keslaudit. Пользователи, для которых группа kesladmin или keslaudit является первичной, будут перемещены в группу nogroup. Если группа nogroup отсутствует, то установка будет прервана и вам будет предложено удалить пользователей из привилегированных групп вручную.

Введите `no`, если вы не хотите, чтобы приложение удаляло пользователей из привилегированных групп.

Шаг 13. Назначение пользователю роли администратора

На этом шаге мастер предлагает назначить роль администратора (admin).

Введите имя пользователя, которому вы хотите назначить роль администратора. Роль администратора требуется для управления параметрами приложения и параметрами задач через графический интерфейс и командную строку приложения без использования команды `sudo`.

Вы можете назначить пользователю роль администратора позже, после завершения первоначальной настройки приложения.

Шаг 14. Настройка механизма перехвата системных событий

Приложение может использовать механизм перехвата на основе обновляемого модуля ядра, если операционная система соответствует требованиям для его установки. Если операционная система не соответствует этим требованиям, но поддерживает технологию fanotify, то для перехвата системных событий приложение будет использовать технологию fanotify. Если операционная система не поддерживает технологию fanotify, приложение скомпилирует и будет использовать для перехвата системных событий специальный модуль ядра для защиты от файловых угроз. Если установлены все необходимые пакеты, компиляция модуля ядра запустится автоматически при запуске защиты от файловых угроз. Если необходимые пакеты на устройстве не обнаружены, приложение Kaspersky Endpoint Security предложит установить их. Если скачать пакеты не удалось, выводится сообщение об ошибке.

- Введите `yes`, если вы хотите использовать механизм перехвата на основе обновляемого модуля ядра.
- Введите `no`, если вы хотите использовать системный механизм перехвата на основе технологии fanotify.

Если вы выбрали механизм перехвата на основе обновляемого модуля ядра, укажите следующие параметры:

- Действие, которое приложение выполняет, если обновляемый модуль ядра не запускается:
  - Введите `yes`, если вы хотите, чтобы в случае ошибки запуска обновляемого модуля ядра приложение перешло к использованию технологии fanotify для перехвата системных событий.
  - Введите `no`, если вы хотите, чтобы в случае ошибки запуска обновляемого модуля ядра приложение продолжило работу без перехвата системных событий.

    Если приложение не использует перехват системных событий, проверка файлов в режиме реального времени не выполняется, уровень защиты устройства снижается.

- Режим перезапуска приложения при переходе к использованию обновляемого модуля ядра. Для запуска модуля требуется перезапустить приложение автоматически или вручную.

  Рекомендуется выполнять автоматический перезапуск приложения для перехода к использованию обновляемого модуля ядра. Запуск обновляемого модуля ядра после перезапуска приложения вручную может приводить к ошибкам в работе приложения.

Введите `yes`, чтобы разрешить автоматический перезапуск приложения для запуска модуля.

Шаг 15. Включение автоматической настройки SELinux

Шаг отображается, если в вашей операционной системе установлена система контроля доступа SELinux.

Введите `yes`, чтобы автоматически настроить систему SELinux для работы с приложением Kaspersky Endpoint Security. Если не удалось настроить систему SELinux автоматически (например, если отсутствует утилита semanage), мастер выводит сообщение об ошибке и предлагает пользователю настроить систему SELinux вручную.

Введите `no`, если вы не хотите выполнять автоматическую настройку системы SELinux.

По умолчанию мастер предлагает значение `yes`.

Если требуется, вы можете вручную настроить систему SELinux для работы с приложением позже, после завершения первоначальной настройки приложения.

Шаг 16. Настройка источника обновлений

Шаг отображается, если вы устанавливаете приложение Kaspersky Endpoint Security в стандартном режиме или режиме EDR-агента.

Укажите источник обновлений баз и модулей приложения. Базы приложения содержат описания сигнатур угроз и методов борьбы с ними. Приложение использует эти записи при поиске и нейтрализации угроз. Вирусные аналитики "Лаборатории Касперского" регулярно добавляют записи о новых угрозах.

Введите одно из следующих значений:

- `KLServers` – приложение получает обновления с одного из серверов обновлений "Лаборатории Касперского".
- `SCServer` – приложение загружает обновления на защищаемое устройство с установленного в вашей организации Сервера администрирования Kaspersky Security Center. Вы можете выбрать этот источник обновлений, если вы используете приложение Kaspersky Security Center для централизованного управления защитой устройств в вашей организации.
- `Custom` – приложение загружает обновления из пользовательского источника. Вы можете указать адрес пользовательского источника обновлений в виде локальной директории (например, /home/bases/) или удаленного HTTP- или HTTPS-сервера (например, http://example.com/bases/).

Шаг 17. Настройка параметров прокси-сервера

Шаг отображается, если вы устанавливаете приложение Kaspersky Endpoint Security в стандартном режиме или режиме EDR-агента.

Если вы используете прокси-сервер при подключении к интернету, укажите адрес прокси-сервера в одном из следующих форматов:

- `[<connection protocol>://]<address of proxy server>:<port>`, если для подключения к прокси-серверу не требуется аутентификация;
- `[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>`, если для подключения к прокси-серверу требуется аутентификация. Если вы указываете IP-адрес в формате IPv6, то вводите адрес в квадратных скобках.

> Подключение к прокси-серверу по протоколу HTTPS не поддерживается. Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.

Если вы не используете прокси-сервер, введите `no`.

По умолчанию приложение предлагает значение `no`.

Вы можете настроить параметры прокси-сервера позже, после завершения первоначальной настройки приложения.

Шаг 18. Запуск обновления баз приложения

Шаг отображается, если вы устанавливаете приложение Kaspersky Endpoint Security в стандартном режиме или режиме EDR-агента.

На этом шаге мастер предлагает запустить задачу обновления баз приложения на клиентском устройстве сразу после установки.

Если вы хотите отказаться от запуска обновления баз приложения, введите `no`.

По умолчанию мастер предлагает значение `yes`.

Если выбрано значение `yes`, приложение будет автоматически перезапущено после обновления баз.

> Kaspersky Endpoint Security обеспечивает защиту устройства только после обновления баз приложения.

Вы можете запустить задачу обновления позже, после завершения первоначальной настройки приложения.

Шаг 19. Включение автоматического обновления баз приложения

Шаг отображается, если вы устанавливаете приложение Kaspersky Endpoint Security в стандартном режиме или режиме EDR-агента.

Введите `yes`, чтобы включить автоматическое обновление баз приложения. По умолчанию приложение проверяет наличие обновлений баз каждые 60 минут. При наличии обновлений приложение загружает обновленные базы.

Введите `no`, если вы не хотите, чтобы приложение автоматически обновляло базы.

Вы можете включить автоматическое обновление баз позже, после завершения первоначальной настройки приложения, настроив расписание задачи обновления.

Шаг 20. Активация приложения

Шаг отображается, если вы устанавливаете приложение Kaspersky Endpoint Security в стандартном режиме или режиме EDR-агента.

Если вы хотите активировать приложение сразу после установки, введите код активации или укажите полный путь к файлу ключа.

> Если вы не указали код активации или файл ключа, приложение будет активировано с помощью пробного ключа на один месяц.

Вы можете активировать приложение позже, после завершения первоначальной настройки приложения.

Как выполнить первоначальную настройку в автоматическом режиме

1. Создайте конфигурационный файл, который содержит параметры первоначальной настройки. Вы можете скопировать параметры из конфигурационного файла autoinstall.ini, который используется для удаленной установки приложения с помощью Kaspersky Security Center, и внести необходимые изменения.

2. В конфигурационном файле задайте следующие обязательные параметры:

   - Согласие с условиями Лицензионного соглашения и Политики конфиденциальности:

     ```
     EULA_AGREED=Yes
     PRIVACY_POLICY_AGREED=Yes
     ```

     Вы можете ознакомиться с условиями Лицензионного соглашения и с Политикой конфиденциальности в файле license.<идентификатор языка>, который включен в комплект поставки приложения.

     > Если вы не приняли условия Лицензионного соглашения и и Политики конфиденциальности, настройка приложения прерывается.

   - По умолчанию приложение Kaspersky Security Network используется в стандартном режиме.

Чтобы использовать приложение в режиме EDR-агента, укажите параметр:

```
ENDPOINT_AGENT_MODE=Yes
```

Чтобы использовать приложение в режиме Легкого агента, укажите параметр:

```
KSVLA_MODE=Yes
```

- Использование Kaspersky Security Network. Примите или отклоните условия использования Kaspersky Security Network:

  ```
  USE_KSN=Yes|No
  ```

  Файл ksn_license.<ID языка> с текстом Положения о Kaspersky Security Network находится в директории /opt/kaspersky/kesl/doc/. Если вы принимаете условия Положения о Kaspersky Security Network, будет включен расширенный режим KSN. Вы можете включить, выключить или изменить режим Kaspersky Security Network в любой момент.

  > Если вы включили использование Kaspersky Security Network, автоматически включается облачный режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО.

- Автоматическое удаление пользователей из привилегированных групп kesladmin и keslaudit перед установкой приложения:

  ```
  GROUP_CLEAN=Yes|No
  ```

3. Выберите механизм перехвата системных событий, который приложение Kaspersky Endpoint Security использует в своей работе. Если вы хотите использовать обновляемый модуль ядра для перехвата системных событий, задайте значение:

   ```
   INTERCEPTOR_MODE=UseUpdatableKernelModule
   ```

   По умолчанию для перехвата системных событий используется технология fanotify.

4. Если вы устанавливаете приложение в стандартном режиме или в режиме EDR-агента, укажите следующие параметры:

   - Параметры прокси-сервера. Если вы используете прокси-сервер при подключении к интернету, укажите адрес прокси-сервера в одном из следующих форматов:

     - `PROXY_SERVER=[<connection protocol>://]<address of proxy server>:<port>`, если для подключения к прокси-серверу не требуется аутентификация;

     - `PROXY_SERVER=[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>`, если для подключения к прокси-серверу требуется аутентификация. Если вы указываете IP-адрес в формате IPv6, то вводите адрес в квадратных скобках.

     > Подключение к прокси-серверу по протоколу HTTPS не поддерживается.

   - Установка и использование графического интерфейса приложения:

     ```
     USE_GUI=Yes|No
     ```

5. Если вы устанавливаете приложение в режиме Легкого агента, укажите следующие параметры:

   - Роль защищаемой виртуальной машины:

     - `SERVER_MODE=Yes`, если защищаемая виртуальная машина используется как сервер.

     - `SERVER_MODE=No`, если защищаемая виртуальная машина используется как рабочая станция.

   - Включение режима защиты инфраструктуры VDI для оптимизации работы приложения на временных виртуальных машинах. Если вы устанавливаете приложение на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины, задайте значение:

     `VDI_MODE=Yes`

6. Запустите мастер первоначальной настройки:

   ```
   /opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=<initial configuration file>
   ```

   Где `<initial configuration file>` – путь к конфигурационному файлу с параметрами первоначальной настройки.

Завершение работы мастера первоначальной настройки и освобождение консоли означает, что процесс первоначальной настройки приложения завершен.

Проверить код возврата

```
echo $?
```

Если команда вернула код 0, первоначальная настройка приложения успешно завершена.

4 Проверка работоспособности приложения

В результате приложение Kaspersky Endpoint Security установлено, активировано и обновлены базы приложения. После установки приложение запускается автоматически. По умолчанию включаются следующие компоненты:

- Защита от файловых угроз.
- Контроль устройств.
- Анализ поведения.
- Защита от веб-угроз – только если в операционной системе установлен один из поддерживаемых браузеров и на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в свойствах политики не установлен).
- Защита от сетевых угроз – только если параметры защиты от сетевых угроз на устройстве заданы через политику. По умолчанию в свойствах политики включена защита от сетевых угроз. Если на устройстве применяются локально настроенные параметры, по умолчанию защита от сетевых угроз выключена.

Проверка состояния защиты устройства для стандартного режима

```
Чтобы проверить состояние защиты устройства, выполните команду:

kesl-control --app-info [--json]
```

Где `--json` – выводить данные в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в консоль.

Убедитесь, что:

- Приложение активировано – строка **Информация о лицензии приложения**.
- Базы приложения обновлены – строки **Базы приложения загружены** и **Дата последнего выпуска баз приложения**.
- Защита от файловых угроз включена – строка **Защита от файловых угроз**.
- В строке **Статус приложения** отображается `OK`.

  Если в строке **Статус приложения** отображается информация о том, что нет прав на системные директории, локально на этом устройстве проверьте права для следующих директорий: /var/opt/kaspersky, /var/log/kaspersky и /opt/kaspersky. Убедитесь, что владельцем является учетная запись root и только владелец имеет право на запись в эти директории.

Проверка состояния защиты устройства для режима EDR-агента

```
Чтобы проверить состояние защиты устройства, выполните команду:

kesl-control --app-info [--json]
```

Где `--json` – выводить данные в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в консоль.

Убедитесь, что:

- Приложение активировано – строка **Информация о лицензии EDR Expert (on-premises)**.
- Базы приложения обновлены – строки **Базы приложения загружены** и **Дата последнего выпуска баз приложения**.
- Приложение используется в режиме EDR-агента – строка **Режим Агента Endpoint Detection and Response**.
- Для интеграций, которые вы настроили в политике Kaspersky Endpoint Security, отображается статус "Задача доступна и выполняется".
- В строке **Статус приложения** отображается `OK`.

  Если в строке **Статус приложения** отображается информация о том, что нет прав на системные директории, локально на этом устройстве проверьте права для следующих директорий: /var/opt/kaspersky, /var/log/kaspersky и /opt/kaspersky. Убедитесь, что владельцем является учетная запись root и только владелец имеет право на запись в эти директории.

Проверка состояния защиты устройства для режима Легкого агента

1. Выполните команду:

   ```
   kesl-control --ksvla-info
   ```

   Убедитесь, что приложение используется в режиме Легкого агента – строка **Режим Легкого агента для защиты виртуальных сред**.

2. Если в политике вы выбрали Сервер интеграции для обнаружения доступных для подключения SVM, выполните команду:

   ```
   kesl-control --viis-info
   ```

   Убедитесь, что Легкий агент подключен к Серверу интеграции – строка **Статус подключения к Серверу интеграции**.

3. Выполните команду:

   ```
   kesl-control --svm-info
   ```

   Убедитесь, что Легкий агент подключен к SVM: отображается информация об SVM, к которой выполнено подключение.

4. Выполните команду:

   ```
   kesl-control --app-info [--json]
   ```

   Где `--json` – выводить данные в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в консоль.

   Убедитесь, что:

   - Легкий агент получает информацию о лицензии, по которой активировано решение Kaspersky Security для виртуальных сред Легкий агент – строка **Информация о лицензии приложения**.
   - Базы приложения обновлены – строки **Базы приложения загружены** и **Дата последнего выпуска баз приложения**.
   - В строке **Статус приложения** отображается `OK`.

     Если в строке **Статус приложения** отображается информация о том, что нет прав на системные директории, локально на этом устройстве проверьте права для следующих директорий: /var/opt/kaspersky, /var/log/kaspersky и /opt/kaspersky. Убедитесь, что владельцем является учетная запись root и только владелец имеет право на запись в эти директории.

Полезные статьи

Что делать, если не выполняются задачи или не применяются политики

Что делать, если устройство в статусе "Недопустимые параметры политики. Политика не была применена"

Ошибка "Приложение не поддерживается текущей версией Kaspersky Security Center Web Console или не установлен веб-плагин для приложения"

Как решить проблему при установке графического интерфейса

Описание кодов ошибок установки

Ошибки после установки Kaspersky Endpoint Security

После того как вы установили Kaspersky Endpoint Security, вы можете вернуться в сценарий развертывания и продолжить с этапа Дополнительная настройка после установки в отдельных ОС.

Дополнительная настройка после установки в отдельных ОС

После того как вы подготовили среду к установке приложения и установили Kaspersky Endpoint Security, в некоторых операционных системах требуется выполнить дополнительную настройку.

Настройка SELinux вручную для работы с приложением

Если в вашей операционной системе используется система контроля доступа SELinux в режиме `Enforcing`, ее настройка для работы с приложением по умолчанию выполняется автоматически во время установки.

Если приложению не удалось настроить систему SELinux автоматически (например, в случае отсутствия утилиты semanage), мастер выводит сообщение об ошибке и предлагает пользователю настроить систему SELinux вручную. В этом случае или если вы отказались от автоматической настройки, после завершения первоначальной настройки приложения вручную настройте систему SELinux для работы с приложением Kaspersky Endpoint Security.

Настройку требуется выполнять с root-правами.

Чтобы вручную настроить систему SELinux для работы с приложением:

1. Переведите систему SELinux в неблокирующий режим:
   - Если SELinux активирован, выполните команду:

     ```
     setenforce Permissive
     ```

   - Если SELinux выключен, в конфигурационном файле /etc/selinux/config задайте значение параметра `SELINUX=permissive` и перезагрузите операционную систему.
2. Убедитесь, что в системе установлена утилита semanage. Если утилита не установлена, установите пакет policycoreutils-python или policycoreutils-python-utils в зависимости от типа менеджера пакетов.

3. Если вы используете пользовательскую политику SELinux, то есть отличную от заданной по умолчанию targeted policy, назначьте метку для каждого исходного исполняемого файла приложения Kaspersky Endpoint Security в соответствии с используемой политикой SELinux.

```
semanage fcontext -a -t bin_t <executable file>
restorecon -v <executable file>
```

Где `<executable file>`:

- /var/opt/kaspersky/kesl/<build number_*>/opt/kaspersky/kesl/libexec/kesl
- /var/opt/kaspersky/kesl/<build number_*>/opt/kaspersky/kesl/bin/kesl-control
- /var/opt/kaspersky/kesl/<build number_*>/opt/kaspersky/kesl/libexec/kesl-gui
- /var/opt/kaspersky/kesl/<build number_*>/opt/kaspersky/kesl/shared/kesl
- /var/opt/kaspersky/kesl/<build number_*>/opt/kaspersky/kesl/bin/response

4. Запустите следующие задачи:

Запустить задачу Защита от файловых угроз

```
kesl-control --start-task 1
```

Запустить задачу Проверка важных областей

```
kesl-control --start-task 4 -W
```

Рекомендуется запустить все задачи, которые вам потребуются при использовании приложения Kaspersky Endpoint Security.

5. Запустите графический пользовательский интерфейс, если вы планируете его использовать.

6. Убедитесь, что в файле audit.log нет ошибок.

Посмотреть файл audit.log

```
grep kesl /var/log/audit/audit.log
```

7. Если в файле audit.log присутствуют ошибки, создайте и загрузите новый модуль правил на основе блокирующих записей, чтобы устранить ошибки, затем снова запустите задачи, которые вам потребуются при использовании приложения Kaspersky Endpoint Security.

Создать и загрузить новый модуль правил на основе блокирующих записей

```
grep kesl /var/log/audit/audit.log | audit2allow -M kesl
semodule -i kesl.pp
```

В случае появления новых audit-сообщений, связанных с Kaspersky Endpoint Security, требуется обновить файл модуля правил.

8. Переведите систему SELinux в блокирующий режим.

```
setenforce Enforcing
```

Если вы используете пользовательскую политику SELinux, то после установки обновлений приложения вам нужно вручную назначить метку для исходных исполняемых файлов приложения Kaspersky Endpoint Security (выполните шаги 1, 3–8).

Дополнительную информацию вы можете найти в документации для используемой операционной системы.

Настройка SELinux для выполнения действий по реагированию

Если вы планируете использовать в вашей ОС систему SELinux в режиме `Enforcing` и инструменты, для которых не настроена политика SELinux, для выполнения действий по реагированию при интеграции с решениями Detection and Response вам нужно дополнительно настроить систему SELinux.

Настройку SELinux требуется выполнять с root-правами.

Чтобы настроить систему SELinux для выполнения действий по реагированию:

1. Переведите систему SELinux в неблокирующий режим:

   - Если SELinux активирован, выполните команду:

     Перевести SELinux в неблокирующий режим

     ```
     setenforce Permissive
     ```

   - Если SELinux выключен, в конфигурационном файле /etc/selinux/config задайте значение параметра `SELINUX=permissive` и перезагрузите операционную систему.

2. Убедитесь, что в системе установлена утилита semanage. Если утилита не установлена, установите пакет policycoreutils-python или policycoreutils-python-utils в зависимости от типа менеджера пакетов.

3. Запустите все задачи для выполнения действий по реагированию, которые вы планируете использовать при интеграции приложения с решениями Detection and Response.

4. Для сбора форензики с помощью задачи получения дампа памяти (Get memory dump) и задачи получения дампа памяти процесса (Get process memory dump) в системе SELinux разрешите приложению Kaspersky Endpoint Security обращаться к указанным в задачах SMB-серверам.

5. Убедитесь, что в файле audit.log нет ошибок.

   Посмотреть файл audit.log

   ```
   grep kesl /var/log/audit/audit.log
   ```

6. Если в файле audit.log присутствуют ошибки, создайте и загрузите новый модуль правил на основе блокирующих записей, чтобы устранить ошибки, и снова запустите задачи для выполнения действия по реагированию.

Создать и загрузить новый модуль правил на основе блокирующих записей

```
grep kesl /var/log/audit/audit.log | audit2allow -M kesl
semodule -i kesl.pp
```

7. Переведите систему SELinux в блокирующий режим.

```
setenforce Enforcing
```

Настройка запуска приложения в ОС ОСнова

После установки приложения выполните действия, необходимые для запуска приложения и его графического интерфейса:

1. Откройте файл `/etc/NESS/systemd/kesl.service.config` и задайте значение параметра `NESSCTX_MODIFY="t+ADDEQUSOCK,OMIT,OMIT_PID,SSUID_SAVE_CTX_PERMANENT"`.

2. Откройте файл `/etc/sysctl.d/30-disable-ptrace.conf` и проверьте значение параметра `kernel.yama.ptrace_scope=0`. Другие значения параметра `kernel.yama.ptrace_scope` могут повлиять на работу приложения Kaspersky Endpoint Security, подробнее см. в разделе Известные проблемы и ограничения.

3. Если вы хотите запускать проверку памяти процессов и памяти ядра, вам нужно выключить средство защиты памяти mprotect (или PaX) в ядре. Для этого добавьте в командную строку запуска ядра параметр `mprotect=off`. Подробнее см. в документации ОСнова.

4. Перезагрузите операционную систему.

Настройка запуска приложения в ОС Альт СП в режиме замкнутой программной среды

После установки приложения выполните действия, необходимые для запуска приложения:

1. Назначьте наследование группы kesl и права на директории для обновляемых компонентов приложения Kaspersky Endpoint Security:

```
cd /var/opt/kaspersky/kesl/<build number_*>/var/opt/kaspersky/kesl/private
chown -R root:kesl updates/
find updates -type d -exec chmod g+s {} \;
cd /opt/kaspersky/kesl/lib64
chown -R root:kesl updatable_modules/
find updatable_modules -type d -exec chmod g+s {} \;
cd /var/opt/kaspersky/kesl/common/
chown -R root:kesl temp/
find temp -type d -exec chmod g+s {} \;
```

2. Назначьте наследование группы kesl и права на директории для обновляемых компонентов Агента администрирования:

```
cd /var/opt/kaspersky/
chown -R root:kesl klnagent/
find klnagent/ -type d -exec chmod g+s {} \;
cd /opt/kaspersky/
chown -R root:kesl klnagent64/
find klnagent64/ -type d -exec chmod g+s {} \;
```

3. Включите режим замкнутой программной среды, выполнив запуск подписания системы:

```
integrity-applier -i -A
```

4. Убедитесь, что подсистема IMA активирована:

```
cat /proc/cmdline
```

Вывод команды должен содержать строки `lsm=integrity ima_hash=sha512 ima_appraise=enforce`.

5. Запустите задачу обновления баз:

```
kesl-control --start 6 -W
```

Если по завершении задачи обновления баз в выводе присутствует событие *EventType=BasesApplied*, то обновление баз выполнено корректно.

6. Перезапустите приложение:

```
systemctl restart kesl
```

Сценарий миграции на Kaspersky Security Center Linux с использованием скрипта быстрой установки

Сценарий включает примеры миграции решения с переносом данных на новое устройство с установленным Сервером администрирования для:

- Миграции с Kaspersky Security Center Windows (СУБД MS SQL и PostgreSQL) на Kaspersky Security Center Linux (СУБД PostgreSQL).
- Переноса Kaspersky Security Center Linux (СУБД PostgreSQL) для замены оборудования.

Развертывание нового Сервера администрирования выполяется с использованием скрипта быстрой установки.

Другие способы переноса данных изложены в [разделе по миграции на Kaspersky Security Center Linux](#).

1 Предварительные действия перед созданием резервной копии

Этот шаг содержит инструкции по подготовке ранее настроенного Сервера администрирования для дальнейшей миграции на новый Сервер администрирования Kaspersky Security Center Linux. Подготовка состоит из следующих этапов:

1. Проверка версии Сервера администрирования для создания совместимой с Kaspersky Security Center Linux резервной копии.

Все актуальные версии **Kaspersky Security Center Linux** поддерживают перенос данных с обновлением на более новую версию приложения. Создание и восстановление резервных копий возможно только в рамках одного типа СУБД.

Для **Kaspersky Security Center Windows** необходимо проверить версию Сервера администрирования в **Свойства** → **Общие** → **Версия**. Если версия ниже, чем 15.1.0.22239, обновите Kaspersky Security Center Windows до последней версии.

Обновление Kaspersky Security Center Windows до последней версии

1. На сайте "Лаборатории Касперского" скачайте дистрибутив, соответствующий языку локализации установленного Сервера администрирования: `Version 15.1.0.22239 | Windows | Full distributive`.

   Исполняемый файл сохраняется в папку **Загрузки** со следующим названием: `ksc_15.1_<build number>_full_<language>.exe`.

2. Скопируйте дистрибутив на Сервер администрирования.

3. Запустите от администратора исполняемый файл `ksc_15.1_<build number>_full_<language>.exe`.

4. В открывшемся окне нажмите на ссылку **Установить Kaspersky Security Center**.

   Запустится мастер установки Сервера администрирования.

5. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения следующих документов** установите флажки:

   - **Условия и положения настоящего Лицензионного соглашения**.
   - **Политику конфиденциальности, которая описывает обработку данных**.

6. Выберите **Обновить Сервер администрирования и консоль на основе веб-интерфейса (рекомендуется)** и перейдите к следующему шагу.

7. Создайте новую резервную копию, выберите опцию **Я хочу создать резервную копию данных** и пройдите мастер создания резервной копии.

8. Нажмите **Обновить**.

9. Во время обновления в мастере установки Web Console подтвердите все шаги мастера для обновления версии.

   Процесс установки обновления Сервера администрирования займет некоторые время. После завершения мастера установки Консоль администрирования может не принимать подключения до завершения инициализации базы данных.

10. Дождитесь полного завершения процедуры обновления.

2. Проверка выполнения требований к сертификату Сервера администрирования.

   Перед созданием резервной копии вам нужно убедиться, что сертификат содержит альтернативное имя субъекта (Subject Alternative Name, SAN). Если нет, важно заменить сертификат, иначе вы не сможете войти в Web Console после восстановления из резервной копии.

Чтобы проверить, что сертификат включает альтернативное имя субъекта:

- Для устройств с операционной системой Windows:

  a. В Консоли администрирования выберите Сервер администрирования, для которого требуется проверка.

  b. В контекстном меню выберите пункт **Свойства** → **Общие** → **Просмотреть сертификат Сервера**.

  c. В открывшемся окне проверьте значение пункта **Альтернативное имя субъекта**.

- Для устройств с операционной системой Linux выполните команду:

```
sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
```

Убедитесь, что альтернативное имя субъекта содержит доменное имя (DNS) устройства Сервера администрирования.

Если значение содержит только внешний IP-адрес без доменного имени (DNS) или значение полностью отсутствует, вручную замените сертификат на соответствующий требованиям работы с Kaspersky Security Center Linux. Замените общий сертификат Сервера администрирования с помощью утилиты klsetsrvcert.

Замена общего сертификата Сервера администрирования с помощью утилиты klsetsrvcert

1. Создайте новый сертификат с отложенной датой начала использования на устройствах, выполнив команду:

   - Для Kaspersky Security Center Windows:

```
"%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
<oldksc.example.internal>" -o "RsaKeyLen:2048"
```

   - Для Kaspersky Security Center Linux:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
```

   где `"<oldksc.example.internal>"` – FQDN-адрес подключения к Серверу администрирования.

   > Не используйте IP-адрес для этого значения.

2. Назначьте дату начала использования нового сертификата на всех устройствах, выполнив команду:

   - Для Kaspersky Security Center Windows:

```
"%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
```

   - Для Kaspersky Security Center Linux:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
```

где дата `"DD-MM-YYYY hh:mm"` минимум на 30 дней больше текущей. По умолчанию период распространения нового сертификата (`CR`) составляет 90 дней.

> После наступления назначенного времени потребуется переустановить Web Console чтобы восстановить к ней доступ и актуализировать сертификат в ее составе.

3. Если необходимо, после миграции на новый Сервер администрирования запустите утилиту klmover, чтобы восстановить соединение устройств с Сервером администрирования. Запуск утилиты может понадобиться, если устройство было выключено весь период распространения сертификата или не подключалось к Серверу администрирования.

2 Создание резервной копии предыдущей установки Сервера администрирования

Создание резервной копии Kaspersky Security Center Windows

1. Из меню **Пуск** → **Kaspersky Security Center** → **Kaspersky Backup Utility** запустите утилиту `klbackup.exe`, расположенную в папке установки Kaspersky Security Center Linux.

   Запустится мастер установки. На ОС Microsoft Windows в режиме Server Core используйте консольную версию утилиты klbackup.

2. На первом шаге выберите **Выполнить резервное копирование данных Сервера администрирования**.

3. На шаге **Параметры резервного копирования** выполните следующие действия:

   a. Нажмите на кнопку **Обзор** и создайте новую папку для сохранения резервной копии отдельно от директории по умолчанию, например `C:\kscbackups`.

   b. Если вы используете Microsoft SQL Server, выберите опцию **Перенос базы данных** → **Перенос в формат Postgres** для использования со скриптом быстрой установки. При обычном способе развертывания Kaspersky Security Center Linux, также возможен перенос данных в базу данных MySQL/MariaDB.

   c. Задайте пароль к резервной копии для защиты от несанкционированного доступа к данным.

4. Дождитесь создания резервной копии и завершите работу утилиты.

   В директории создана новая директория с отметкой времени создания резервной копии.

Создание резервной копии Kaspersky Security Center Linux

1. На устройстве с Сервером администрирования в командной строке введите следующую команду:

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. Дождитесь завершения создания резервной копии.

   В директории, указанной после параметра `-path`, будет создана новая директория с отметкой времени создания резервной копии.

После создания резервной копии предыдущего Сервера администрирования, выведите из эксплуатации устройство с Сервером администрирования.

Вывод устройства с Сервером администрирования из эксплуатации

1. Скопируйте полученную резервную копию для переноса данных на устройство администратора.
2. Завершите работу операционной системы Сервера администрирования.
3. Отключите сетевой адаптер от корпоративной сети.
4. Освободите IP-адрес устройства, если планируете использовать его для новой установки Kaspersky Security Center Linux.
5. Убедитесь, что устройство полностью отключено.

Нахождение в сети прежнего Сервера администрирования может вызывать сбои управления устройствами и нарушение входа в Web Console нового Сервера администрирования, а также запуск задачи установки Агента администрирования с подключением к старому серверу.

3 Первоначальная установка Kaspersky Security Center Linux с помощью скрипта быстрой установки

Эта инструкция описывает первоначальное развертывание экземпляра Kaspersky Security Center Linux с использованием скрипта быстрой установки.

Особенности:

- Установка всех компонентов Kaspersky Security Center выполняется на одном устройстве с Сервером администрирования.
- Операционной системой Сервера администрирования является одна из следующих:
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.5) с СУБД PostgreSQL 15.
  - Ubuntu Server 26.04 LTS с СУБД PostgreSQL 18.
  - CentOS Stream 10 с СУБД PostgreSQL 18.
  - РЕД ОС 8 с СУБД PostgreSQL 16.
- Скрипт быстрой установки автоматизирует только настройку и установку приложения Kaspersky Security Center. Администратор самостоятельно настраивает имя устройства с Сервером администрирования в операционной системе, работу сетевых адаптеров, сетевые экраны безопасности на уровне операционной системы и настраивает оборудование.

Первоначальная установка экземпляра Kaspersky Security Center Linux с использованием скрипта быстрой установки состоит из следующих этапов:

1. Подготовка к развертыванию

До начала действий по установке необходимо подготовить:

- Установочный образ диска операционной системы и репозиторий пакетов приложений.
- Приложение-аутентификатор для использования двухфакторной аутентификации (2FA) при входе в Web Console.
- Новый адрес FQDN (например, *ksclinux.example.com*). Вы можете использовать свой сценарий с присвоением прежнего адреса FQDN новому серверу при установке, если обладаете достаточным опытом настройки решений. В этом случае на шаге 5 "Настройка приложения после восстановления из резервной копии" пропустите этап 4. "Восстановление подключения управляемых устройств по адресу FQDN предыдущего Сервера администрирования".
- Устройство администратора с браузером для выхода в интернет для загрузки дистрибутивов и управления Web Console.
- Обеспечить доступность DNS и Сервера времени (NTP) для компонентов приложения.
- В зависимости от сценария освободить прежний IP-адрес, если для подключения управляемых устройств использовался IP-адрес.
- Настроить сетевое оборудование и прокси-сервер в соответствии с требованиями:
  - Порты для взаимодействия компонентов приложения.
  - Доступ к серверам "Лаборатории Касперского".
  - Рекомендации по Усилению защиты.

2. Выбор конфигурации и настройка операционной системы

1. Сконфигурируйте оборудование в зависимости от количества устройств, которыми будет управлять Сервер администрирования.

   Каждый расчет включает значения доступных ресурсов для работы приложений "Лаборатории Касперского". В расчет входит одновременная работа Сервера администрирования, Агента администрирования, СУБД, Сервера Web Console и Kaspersky Endpoint Security для Linux на одном устройстве. В расчет не входит хранение резервных копий Сервера администрирования.

   > Используйте внешний файловый ресурс в качестве точки монтирования для хранения резервных копий на отдельном устройстве, либо увеличьте свободное место на жестком диске с учетом хранения резервных копий.

   Рекомендуется добавить дополнительные 4–6 ГБ оперативной памяти и 20 ГБ свободного места на жестком диске для работы операционной системы.

   Расчет ресурсов устройства в зависимости от управляемых устройств:

   - **S** (до 1000 устройств): CPU – 8 ядер, 16 ГБ оперативной памяти, 70 ГБ свободного места на жестком диске для директории `/var`, 300 IOPS или выше.
   - **M** (до 10 000 устройств): CPU – 12 ядер, 24 ГБ оперативной памяти, 340 ГБ свободного места на жестком диске для директории `/var`, 300 IOPS или выше.

- **L** (до 30 000 устройств): CPU – 20 ядер, 40 ГБ оперативной памяти, 490 ГБ свободного места на жестком диске для директории `/var`, 300 IOPS или выше.

- **XL** (до 50 000 устройств): CPU – 28 ядер, 54 ГБ оперативной памяти, 640 ГБ свободного места на жестком диске для директории `/var`, 300 IOPS или выше.

2. Подготовьте оборудование для сервера Kaspersky Security Center в соответствии с выбранными характеристиками.

3. Установите операционную систему на сервер Kaspersky Security Center.

   При установке включите опцию **Средства удаленного подключения SSH**, если планируете управлять устройством Сервера администрирования с помощью удаленной командной строки.

   > Astra Linux должна быть установлена без включенной опции **Мандатное управление доступом**. Также для правильной работы Kaspersky Endpoint Security для Linux требуется отключить опцию **Запрет трассировки ptrace**.

4. Проверьте доступное пространство для директории `/var`, если она смонтирована отдельно, либо для корневой директории `/`.

   Примеры для конфигурации M:

   Astra Linux

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                 Size  Used Avail Use% Mounted on
   /dev/mapper/astra48242-01  406G  8,0G 377G    3% /
   <...>
   ```

   Ubuntu

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                         Size  Used Avail Use% Mounted on
   /dev/mapper/ubuntu--vg-ubuntu--lv  406G   11G  374G   3% /
   <...>
   ```

5. Настройте IP-адрес от прежнего Сервера администрирования на новом сервере, если для подключения управляемых устройств использовался IP-адрес.

Видео: настройка операционной системы

3. Загрузка файлов дистрибутива

1. Загрузите дистрибутивы нужной локализации с сайта "Лаборатории Касперского" и сохраните их в отдельную директорию (например, *kscdistr*).

   Для Ubuntu и Astra Linux

   - Дистрибутив deb Сервера администрирования:

     `Version 16.3.0.1207 | Debian x64 | Administration server`

   - Дистрибутив deb Web Console:

     `Version 16.3.0.1207 | Debian x64 | Web console`

   - Скрипт быстрой установки:

     `Version 16.3.0.1207 | Linux | KSC installation script`

   Для CentOS и РЕД ОС

   - Дистрибутив rpm Сервера администрирования:

     `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Administration server`

   - Дистрибутив rpm Web Console:

     `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Web console`

   - Скрипт быстрой установки:

     `Version 16.3.0.1207 | Linux | KSC installation script`

2. Для работы приложений "Лаборатории Касперского" в режиме Замкнутой программной среды (ЗПС) ОС Astra Linux скачайте файл публичного ключа kaspersky_astra_pub_key.gpg.

3. Скопируйте загруженные файлы на новое устройство с Сервером администрирования Kaspersky Security Center с помощью съемного носителя или по сети.

   Ниже представлены действия, выполняемые в командной строке для копирования по сети.

Возможность использования утилиты scp для копирования зависит от наличия установленного запущенного сервиса SSH на стороне операционной системы устройства с Сервером администрирования и параметров безопасности вашей организации.

a. В командной строке с помощью утилиты cd перейдите в директорию выше на один уровень директории *kscdistr*, например:

Для Linux

```
cd /home/administrator/Desktop
```

Для Windows

```
cd C:\Users\Administrator\Downloads
```

b. Скопируйте файлы дистрибутива по сети с помощью утилиты scp:

```
scp -r <kscdistr> <administrator>@<ksclinux.example.com>:
```

где:

`<kscdistr>` – локальная директория со скачанными дистрибутивами Kaspersky Security Center;

`<administrator>` – привилегированный пользователь на новом Сервере администрирования с правами подключения по протоколу SSH;

`<ksclinux.example.com>` – FQDN-адрес нового Сервера администрирования.

Файлы будут скопированы в корень директории профиля, указанного для подключения пользователя.

4. Настройка параметров установки

1. На новом устройстве с Сервером администрирования выполните вход под привилегированным пользователем и запустите командную строку.

2. Перейдите в директорию со скопированными дистрибутивами.

Пример

```
cd ~/kscdistr
```

3. Распакуйте архив скрипта быстрой установки в текущую директорию с файлами дистрибутивов.

Пример

```
tar -xf ./ksc_fast_install.tar.gz
```

4. Проверьте наличие всех файлов, выполнив команду:

```
ls -la
```

Пример вывода команды ls -la

```
administrator@ksclinux:~$ ls -la
drwxr-xr-x  3 administrator administrator      4096 jul 17 20:32 .
drwx------ 17 administrator administrator      4096 jul 17 17:54 ..
-rw-r--r--  1 administrator administrator       493 apr 20  2023 kaspersky_astra_pub_key.gpg
-rw-r--r--  1 administrator administrator 199128488 jul 10 21:38 ksc64_16.3.0-1207_amd64.deb
-rwxr-xr--  1 administrator administrator    143288 jul 22 17:22 ksc_fast_install.py
-rw-r--r--  1 administrator administrator 158144492 jul 10 21:37 ksc-web-console-16.3.12907.x86_64.deb
-rw-r--r--  1 administrator administrator     15561 jul 22 23:17 nwc_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 nwc_license.txt.sha256
-rw-r--r--  1 administrator administrator       493 jul 22 17:22 params.txt
-rw-r--r--  1 administrator administrator     70869 jul 22 23:17 server_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 server_license.txt.sha256
```

5. В директории с дистрибутивами откройте на редактирование [текстовый файл параметров скрипта установки](), например:

```
nano ./params.txt
```

6. Задайте подготовленные ранее значения и удалите первый символ комментирования (#) в нужных строках, либо добавьте новые строки со следующими значениями:

   - Расчетная конфигурация характеристик оборудования (доступные значения S/M/L/XL).

     Пример

     ```
     klfi_netsize=S
     ```

   - FQDN-адрес Сервера администрирования в двух параметрах файла.

     ```
     klfi_klserver_address=ksclinux.example.com
     ```

     ```
     klfi_kliam_address=ksclinux.example.com
     ```

Язык установленного Сервера администрирования зависит от локализации загруженного дистрибутива.

7. Проверьте правильность преобразования FQDN-адреса Сервера администрирования в петлевой (loopback) IP-адрес в операционной системе нового Сервера администрирования. Для этого:

   a. Выполните команду `ping` с адресом нового Сервера администрирования.

   Пример успешного получения петлевого IP-адреса

   ```
   administrator@ksclinux:~$ ping ksclinux.example.com
   ping ksclinux.example.com
   PING ksclinux.example.com (127.0.1.1) 56(84) bytes of data.
   64 bytes from ksclinux.example.com (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
   ```

b. Добавьте адрес Сервера администрирования в файл `/etc/hosts` операционной системы нового Сервера администрирования, если адрес не был получен или получен внешний IP-адрес.

   Для этого:

   - Откройте файл `/etc/hosts` на редактирование, выполнив команду:

     ```
     sudo nano /etc/hosts
     ```

   - Введите адрес сервера в качестве FQDN-адреса устройства Сервера администрирования, например:

     ```
     127.0.0.1       localhost
     127.0.1.1       ksclinux.example.com ksclinux
     <...>
     ```

> На управляемых устройствах FQDN-адрес Сервера администрирования должен преобразовываться во внешний IP-адрес сервера. Обеспечьте правильную настройку записей на DNS серверах.

5. Запуск скрипта быстрой установки

В случае использования режима замкнутой программной среды (ЗПС) в ОС Astra Linux необходимо:

- Использовать максимальный уровень целостности (Высокий – уровень 63) для пользователя, под которым выполняется установка в операционной системы Astra Linux с задействованным механизмом **Мандатный контроль целостности**.

- Выполнить дополнительные шаги:

  1. Перейдите в директорию со скопированными дистрибутивами, например:

     ```
     cd ~/kscdistr
     ```

  2. Создайте директорию для размещения файла публичного ключа в системной директории:

     ```
     sudo mkdir -p /etc/digsig/keys/legacy/kaspersky/
     ```

  3. Переместите файл публичного ключа `kaspersky_astra_pub_key.gpg` в системную директорию:

     ```
     sudo mv ./kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
     ```

  4. Установите пакет совместимости:

     ```
     sudo apt install -y astra-digsig-oldkeys
     ```

  5. Обновите загрузочный образ системы:

     ```
     sudo update-initramfs -u -k all
     ```

6. Перезагрузите операционную систему:

```
sudo reboot
```

Чтобы запустить скрипт быстрой установки:

1. После перезагрузки устройства вернитесь в директорию с дистрибутивами:

```
cd ~/kscdistr
```

2. Назначьте права выполнения для файла скрипта быстрой установки командой:

```
chmod +x ./ksc_fast_install.py
```

3. Ознакомьтесь с текстами условий Лицензионных соглашений вашей локализации до запуска скрипта, так как текст скрипта быстрой установки доступен только на английском языке.

4. Подключите сетевые репозитории пакетов в ОС или установочный образ диска ОС для скачивания пакетов во время установки.

5. Запустите скрипт быстрой установки:

```
sudo ./ksc_fast_install.py
```

6. Следуйте шагам мастера установки.

> Если на шаге определения доступных ресурсов скрипт ошибочно определяет, что объем доступной оперативной памяти недостаточный, отключите использование оперативной памяти в динамическом режиме на время установки.

7. Дождитесь успешного завершения установки. Из текстового вывода скрипта сохраните имя пользователя (`User`) и пароль (`Pass`) для входа в Web Console.

Пример

```
[+] Creating KSC user 'kscadmin' ...
[+] An internal user has been created:
[+]     User: kscadmin
[+]     Pass: ############
[!] If the password is lost, you must create a user by running the command:
        /opt/kaspersky/ksc64/sbin/kladduser -n <user>
[+] OK
[+] Success
```

Видео: Запуск скрипта быстрой установки для Astra Linux

Видео: Запуск скрипта быстрой установки для Ubuntu

6. Первый вход в Web Console

1. В браузере откройте адрес для подключения к Web Console: `https://<FQDN>:8080`

   где `<FQDN>` – это адрес Сервера администрирования из параметров установки скрипта, например, *https://ksclinux.example.com:8080*.

2. Для входа в Web Console используйте имя пользователя и пароль из вывода скрипта.

3. Настройте приложение-аутентификатор:

   a. Скопируйте в приложение секретный ключ для получения одноразовых кодов подтверждений или отсканируйте QR-код из мастера настройки аутентификации Web Console.

   b. Введите сгенерированный код подтверждения для проверки и входа в Web Console.

4. Ознакомьтесь и подтвердите ознакомление с Руководством по усилению защиты.

5. Выполните настройку Сервера администрирования в Мастере первоначальной настройки, если не планируете восстановить данные Сервера администрирования из резервной копии.

4 Восстановление резервной копии Сервера администрирования

В сценариях миграции с Kaspersky Security Center Windows и в случае переноса данных Kaspersky Security Center Linux на новое оборудование может потребоваться восстановить резервную копию от предыдущей установки Сервера администрирования.

> Версия СУБД PostgreSQL нового сервера должна быть не ниже версии в резервной копии.

Пропустите этот шаг, если восстановление данных не требуется.

Если создание резервной копии не было выполнено ранее:

- Создайте резервную копию предыдущей установки Сервера администрирования с типом формата данных PostgreSQL.
- Установите новый сервер Kaspersky Security Center Linux и выполните первый вход в Web Console.

Восстановление резервной копии Сервера администрирования состоит из следующих этапов:

1. Перенос резервной копии на Сервер администрирования

Перенесите резервную копию предыдущего Сервера администрирования на новое устройство с Сервером администрирования с помощью съемного носителя или по сети.

Чтобы перенести резервную копию на Сервер администрирования по сети:

> Возможность использования утилиты scp для копирования зависит от наличия установленного запущенного сервиса SSH на стороне операционной системы устройства с Сервером администрирования и параметров безопасности вашей организации.

1. В командной строке на устройстве с помощью утилиты *cd* перейдите в директорию, в которой расположена директория с файлами резервной копии предыдущего Сервера администрирования, например:

   Windows
   ```
   cd C:\kscbackups
   ```

   Linux
   ```
   cd /root/kscbackups
   ```

2. Выполните копирование директории с файлами резервной копии с помощью утилиты scp:

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   где:

   `<klbackup202x-xx-xx>` – директория с непосредственно файлами резервной копии;

   `<administrator>` – привилегированный пользователь на новом Сервере администрирования с правами подключения по протоколу SSH;

`<ksclinux.example.com>` – FQDN-адрес нового Сервера администрирования.

Директория с резервной копией будет скопирована в корень директории профиля указанного пользователя.

2. Процедура восстановления резервной копии

1. На новом устройстве с Сервером администрирования откройте командную строку.

2. На время восстановления данных из резервной копии предоставьте права суперпользователя PostgreSQL для стандартных учетных записей klserver и kliam, которые Сервер администрирования использует для подключения к СУБД:

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
```

3. С помощью утилиты klbackup запустите восстановление данных из резервной копии предыдущего Сервера администрирования:

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
```

где `</home/administrator/klbackup202x-xx-xx>` – полный путь к директории с непосредственно файлами резервной копии.

4. Если пароль на резервную копию не был задан, в запросе пароля от резервной копии нажмите клавишу **`Enter`** без ввода пароля.

5. Дождитесь окончания работы утилиты.

   В крупных инсталляциях может требоваться значительное время.

6. Восстановите исходные права у учетных записей PostgreSQL, которые Сервер администрирования использует для подключения к СУБД.

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

5 Настройка приложения после восстановления из резервной копии

Пропустите этот шаг, если вы не восстанавливали данные из резервной копии.

Настройка приложения после восстановления из резервной копии состоит из следующих этапов:

1. Восстановление работы Web Console

1. Получите значение адреса прежнего сервера из конфигурационного файла Сервера IAM:

```
sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Пример

```
ksc_address: "oldksc.example.internal"
```

2. Проверьте правильность преобразования FQDN-адреса прежнего Сервера администрирования в петлевой (loopback) IP-адрес нового Сервера администрирования. Для этого:

   a. Выполните команду `ping` с адресом прежнего Сервера администрирования.

   Пример успешного получения петлевого IP-адреса

```
administrator@ksclinux:~$ ping oldksc.example.internal
ping oldksc.example.internal
PING ksclinux (127.0.1.1) 56(84) bytes of data.
64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
```

   b. Добавьте адрес прежнего Сервера администрирования в файл `/etc/hosts` ОС нового Сервера администрирования, если адрес не был получен или получен внешний IP адрес. Для этого:

   - Откройте /etc/hosts на редактирование:

```
sudo nano /etc/hosts
```

   - Введите имя прежнего сервера в качестве дополнительного псевдонима адреса устройства Сервера администрирования.

   Пример

```
127.0.0.1       localhost
127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
<...>
```

3. Переустановите Web Console:

   a. Удалите локальный Сервер Web Console:

   В зависимости от вашего дистрибутива Kaspersky Security Center Linux выполните одну из следующих команд:

   - На устройстве с операционной системой на базе Debian:

```
sudo apt remove ksc-web-console -y
```

   - На устройстве с операционной системой на базе Red Hat Enterprise Linux:

```
sudo dnf remove ksc-web-console -y
```

b. Запустите установку пакета Web Console из директории с дистрибутивами:

- На устройстве с операционной системой на базе Debian:

```
sudo apt install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.deb -y
```

- На устройстве с операционной системой на базе Red Hat Enterprise Linux:

```
sudo dnf install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.rpm -y
```

2. Восстановление доступа пользователя kscadmin для перехода с Kaspersky Security Center Windows

База пользователей была перезаписана, повторите создание пользователя kscadmin и настройку двухфакторной аутентификации.

1. Откройте командную строку в операционной системе устройства с Сервером администрирования, выполните команду создания пользователя:

   ```
   sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
   ```

   После нажатия **Enter** задайте пароль, затем повторите его.

2. В браузере откройте адрес для подключения к Web Console:

   ```
   https://<FQDN>:8080
   ```

   где `<FQDN>` – это адрес Сервера администрирования из параметров установки скрипта, например, *https://ksclinux.example.com:8080*.

3. Используйте созданные имя пользователя и пароль для входа в Web Console.

4. Настройте приложение-аутентификатор. Для этого:

   a. Удалите устаревший профиль учетной записи пользователя kscadmin, который был настроен в приложении-аутентификаторе до восстановления резервной копии Сервера администрирования.

   b. Скопируйте в приложение секретный ключ для получения одноразовых кодов подтверждений или отсканируйте QR-код из мастера настройки аутентификации Web Console.

   c. Введите сгенерированный код подтверждения для проверки и входа в Web Console.

3. Проверка работы Сервера администрирования

1. Проверьте работоспособность интерфейса Web Console под пользователем kscadmin и другими пользователями.

2. Последовательно запустите следующие задачи:

   - Загрузка обновлений в хранилище Сервера администрирования.
   - Обслуживание Сервера администрирования.
   - Резервное копирование данных Сервера администрирования.

   > Замените Windows-пути в параметрах задач на Linux-директории нового Сервера администрирования, либо удалите и сконфигурируйте задачи повторно.

3. Проверьте результат выполнения задач и если необходимо, внесите изменения в параметры работы задач, политик управления и настроек Сервера администрирования.

4. Восстановление подключения управляемых устройств по адресу FQDN предыдущего Сервера администрирования

Если вы присвоили новый адрес FQDN новому Серверу администрирования (например, ksclinux.example.com), добавьте один из следующих типов записей DNS:

- Запись CNAME, связывающая старое имя Сервера администрирования с новым именем Сервера администрирования.

  Дополнительную информацию о настройке требуемых записей см. в документации DNS-сервера.

- Запись A и AAAA для прежнего адреса Сервера администрирования, указывающая на новый IP-адрес Сервера администрирования.

  Для службы DNS на базе Windows Server выполняйте команды с использованием значений, применимых к вашей инфраструктуре.

Чтобы добавить DNS-запись A для службы DNS на базе Windows Server выполняйте команды с использованием значений, применимых к вашей инфраструктуре:

1. Подключитесь к DNS-серверу.

2. Откройте PowerShell и получите IP-адрес из существующей записи A, выполнив команду:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

3. Измените IP-адрес в A-записи, выполнив команды:

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP-address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. Убедитесь, что IP-адрес в записи A обновлен, выполнив команду:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

В выводе команды отобразится IP-адрес сервера администрирования Kaspersky Security Center Linux. Управляемые устройства восстановят подключение после обновления локального кеша DNS.

6 Настройка антивирусной защиты Сервера администрирования

Чтобы выполнить рекомендации по усилению защиты в части обеспечения Сервера администрирования антивирусной защитой, установите приложения "Лаборатории Касперского" на Сервер администрирования и настройте политики управления. Для развертывания Kaspersky Endpoint Security для Linux используйте руководство по развертыванию.

Установка и настройка состоит из следующих этапов:

1. Создание отдельной группы администрирования

1. В главном окне Web Console выберите **Управление активами** → **Иерархия групп**.
2. Установите флажок рядом с группой **Управляемые устройства**.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне укажите имя новой группы (например, *kscserver*) и подтвердите ее создание нажатием на кнопку **Добавить**.

2. Создание политики для Агента администрирования без наследования параметров

1. В главном окне Web Console перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на кнопку **Добавить**.
3. В Мастере создания новой политики выберите приложение **Агент администрирования Kaspersky Security Center** и нажмите **Далее**.
4. Отключите опцию **Наследовать параметры родительской политики** и нажмите **Сохранить**.

3. Установка плагина управления Kaspersky Endpoint Security для Linux из Kaspersky Security Center или вручную

Вы можете установить плагин управления Kaspersky Endpoint Security для Linux следующими способами:

- Установка из списка доступных дистрибутивов в Web Console.
- Установка вручную из файла.

Чтобы установить плагин управления Kaspersky Endpoint Security из списка доступных дистрибутивов в Web Console:

1. В главном окне Web Console выберите **Параметры** → **Веб-плагины**.

   Откроется список установленных веб-плагинов.

2. Нажмите на кнопку **Добавить**.

   Откроется список доступных плагинов управления. Список обновляется автоматически после выпуска новых версий веб-плагинов.

3. В списке доступных плагинов выберите последнюю доступную версию веб-плагина Kaspersky Endpoint Security для Linux.

4. В открывшемся окне с описанием веб-плагина нажмите на кнопку **Установить плагин**.

5. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новый плагин отобразится в списке установленных веб-плагинов.

Видео: установка веб-плагина управления с помощью мастера

Чтобы установить плагин управления Kaspersky Endpoint Security вручную из файла:

1. Скачайте архив с веб-плагином на странице загрузки приложений в разделе Kaspersky Endpoint Security для Linux: **Плагин контроля приложений** → **Web console Plug-In**.

2. Локально распакуйте скачанный архив.

3. В главном окне Web Console выберите **Параметры** → **Веб-плагины**.

   Откроется список установленных веб-плагинов.

4. Нажмите на кнопку **Добавить из файла**.

5. В открывшемся окне укажите путь к файлу plugin.zip и путь к файлу signature.txt.

   Файлы находятся в папке, куда вы распаковали архив с веб-плагином.

6. Нажмите на кнопку **Добавить**.

7. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новый плагин отобразится в списке установленных веб-плагинов (**Параметры** → **Веб-плагины**).

Видео: установка веб-плагина управления в изолированных сетях

4. Создание политики для Kaspersky Endpoint Security для Linux без наследования параметров

При совместной работе Kaspersky Endpoint Security для Linux и Kaspersky Security Center Linux вам нужно настроить параметры политики в соответствии с рекомендациями специалистов "Лаборатории Касперского".

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

2. Выберите группу администрирования для Сервера администрирования.

3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.

4. В открывшемся окне в списке выберите название приложения Kaspersky Endpoint Security для Linux.

5. Укажите **Стандартный режим или режим Агента Endpoint Detection and Response** приложения Kaspersky Endpoint Security для Linux.

6. Примите решение об использовании Kaspersky Security Network.

7. Ознакомьтесь с рекомендациями по оптимизации для управляемых устройств.

8. В названии политики укажите принадлежность политики к Серверу администрирования.

9. Отключите опцию **Наследовать параметры родительской политики**.

10. Сохраните внесенные изменения.

Видео: создание политики

5. Создание групповой задачи Обновление для Kaspersky Endpoint Security для Linux

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

2. Выберите группу администрирования для Сервера администрирования.

3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задач.

4. В открывшемся окне в списке выберите название приложения Kaspersky Endpoint Security для Linux.

5. Укажите тип задачи *Обновление* и пройдите следующие шаги без изменения параметров.

   Запустится окно свойств задачи.

6. В разделе **Параметры приложения** → **Источники обновлений** включите источник Kaspersky Security Center и поднимите его приоритет.

В изолированных сетях используйте утилиту Kaspersky Update Utility для формирования хранилища для задач обновления.

Видео: настройка централизованного обновления баз

6. Добавление лицензионного ключа в хранилище Сервера администрирования с функцией автоматического распространения

1. В главном окне Kaspersky Security Center Web Console выберите раздел **Лицензии**.
2. Нажмите на кнопку **Добавить**.
3. Укажите опцию **Код активации** и нажмите **Отправить**.

   В изолированных сетях используйте файл ключа, который можно запросить с помощью сервиса https://keyfile.kaspersky.com/ru-RU.
4. В списке лицензий нажмите на название лицензии.
5. Установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**.
6. Сохраните изменения.

Видео: активация приложения с помощью кода активации

Видео: активация приложения с помощью файла ключа

7. Создание инсталляционных пакетов Агента администрирования и Kaspersky Endpoint Security для Linux

1. В главном окне Web Console выберите **Управление программным обеспечением** → **Инсталляционные пакеты**.

2. Нажмите на кнопку **Добавить**.

   Запустится Мастер создания инсталляционного пакета.

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

4. В списке приложений найдите последнюю версию Kaspersky Endpoint Security для Linux и нажмите на название.

5. В боковой панели инициируйте загрузку кнопкой **Скачать и создать инсталляционный пакет**.

   Ознакомьтесь и примите лицензионные соглашения для начала использования приложений.

6. Вернитесь в список приложений и загрузите последнюю версию Агента администрирования (Kaspersky Network Agent for Linux).

   Ознакомьтесь и примите лицензионные соглашения для начала использования приложений.

7. В главном окне Web Console в списке загруженных приложений нажмите на названия приложений.

В изолированных сетях скачайте дистрибутивы с сайта "Лаборатории Касперского" и выберите в Мастере создания инсталляционного пакета опцию **Создать инсталляционный пакет из файла**.

Видео: создание инсталляционного пакета автоматически в Kaspersky Security Center

Видео: создание инсталляционного пакета вручную из файла в Kaspersky Security Center

8. Установка Агента администрирования для Linux

1. В главном окне Web Console выберите **Управление программным обеспечением** → **Инсталляционные пакеты**.

2. Установите флажок напротив пакета **Агента администрирования (Kaspersky Network Agent for Linux)**.

3. Нажмите **Развернуть**.

   Запустится Мастер развертывания защиты.

4. Выберите вариант **С использованием автономного инсталляционного пакета**.

5. На шаге **Перемещение устройств в папку Управляемые устройства** пропустите настройку правил перемещения устройств в группу администрирования. Эта опция не применяется для устройства Сервера администрирования.

6. На шаге **Результат формирования автономного инсталляционного пакета** выделите и скопируйте полный путь размещения скрипта установки приложения.

7. В операционной системе Сервера администрирования откройте командную строку.

8. Запустите установку автономного пакета:

```
sudo bash "</var/opt/.../stand-alone_package_sh>"
```

где `</var/opt/.../stand-alone_package_sh>` – это ранее скопированный полный путь к файлу скрипта автономного инсталляционного пакета приложения.

В случае успешной установки отобразится соответствующее уведомление.

9. Переместите устройство Сервера администрирования (например, *ksclinux*) из группы **Управляемые устройства** в ранее подготовленную группу администрирования (например, *kscserver*).

9. Установка Kaspersky Endpoint Security для Linux

1. В главном окне Web Console выберите **Управление программным обеспечением** → **Инсталляционные пакеты**.

2. Установите флажок напротив пакета Kaspersky Endpoint Security для Linux.

3. Нажмите **Развернуть**.

   Запустится Мастер развертывания защиты.

4. Выберите вариант **С использованием автономного инсталляционного пакета**.

5. На шаге **Результат формирования автономного инсталляционного пакета** выделите и скопируйте полный путь размещения скрипта установки приложения.

6. В операционной системе Сервера администрирования откройте командную строку.

7. Запустите установку автономного пакета:

```
sudo bash "</var/opt/.../stand-alone_package_sh>"
```

   где `</var/opt/.../stand-alone_package_sh>` – это ранее скопированный полный путь к файлу скрипта автономного инсталляционного пакета приложения.

   В случае успешной установки отобразится соответствующее уведомление.

8. В главном окне Web Console в разделе **Задачи** выберите корневой узел в списке групп администрирования с названием Сервера администрирования.

9. Из списка задач Сервера администрирования последовательно запустите следующие задачи:

   - Загрузка обновлений в хранилище Сервера администрирования.

   - Обновление (Kaspersky Endpoint Security для Linux).

10. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

11. Нажмите на имя объекта устройства Сервера администрирования.

12. Проверьте значения основных показателей состояния устройства:

    - Последнее обновление антивирусных баз (актуально).

    - Подключено к Серверу администрирования (актуально).

- Состояние защиты (Выполняется).
- Событие *Ключ успешно добавлен* (есть).

Используйте руководство по развертыванию Kaspersky Endpoint Security для Linux для развертывания приложения на устройствах сети.

Обновление предыдущей версии приложения

Обновление приложения Kaspersky Endpoint Security выполняется путем удаленной или локальной установки новой версии приложения на защищаемые устройства.

Вы можете обновить до версии Kaspersky Endpoint Security 12.5 для Linux только версию Kaspersky Endpoint Security 12.4 для Linux.

Обновление Kaspersky Endpoint Security более ранних версий до версии 12.5 не предусмотрено. Если у вас установлена более ранняя версия Kaspersky Endpoint Security, вам нужно сначала удалить ее, а затем установить Kaspersky Endpoint Security 12.5 для Linux.

Следуя этому сценарию, вы можете обновить приложение.

1 Подготовка среды

Перед началом обновления приложения Kaspersky Endpoint Security выполните необходимые подготовительные действия в зависимости от вашей инфраструктуры.

2 Подготовка дистрибутивов

Выберите нужный дистрибутив в зависимости от ОС, ее архитектуры и типа процессора.

3 Обновление плагина управления Kaspersky Endpoint Security

Если вы управляете приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, обновите веб-плагин или MMC-плагин управления Kaspersky Endpoint Security, в зависимости от используемой консоли управления Kaspersky Security Center.

4 Обновление приложения и графического интерфейса на защищаемых устройствах

Установите новую версию приложения на защищаемые устройства. Для обновленного приложения сохраняется тот режим использования приложения, который был выбран во время установки. Если вы хотите использовать приложение в другом режиме, вам нужно удалить приложение и затем выполнить процедуру установки и первоначальной настройки приложения.

Если Kaspersky Endpoint Security используется в стандартном режиме или в режиме EDR-Агента и вы используете графический интерфейс приложения, также обновите графический интерфейс.

Вы можете обновить приложение и графический интерфейс приложения следующими способами:

- Удаленно с помощью Kaspersky Security Center
- Локально из командной строки

Как обновить приложение из пакета формата RPM с помощью командной строки

Обновление приложения с помощью командной строки выполняется путем установки на устройство новой версии приложения.

> Обновление приложения требуется выполнять с root-правами.

Для обновления приложения на выполните команду:

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] rpm -U --replacefiles --
replacepkgs kesl-12.5.0-<build number>.<arch>.rpm [kesl-gui-12.5.0-<build number>.<arch>.rpm]
```

Приложение Kaspersky Endpoint Security будет автоматически перезапущено.

Условные обозначения

Параметры команды

Параметр	Описание
`KESL_EULA_AGREED=yes`	Принять условия условия Лицензионного соглашения.
`KESL_PRIVACY_POLICY_AGREED=yes`	Принять условия Политики конфиденциальности.
`KESL_USE_KSN=yes/no`	Использование Kaspersky Security Network: `yes` – принять условия Положения о Kaspersky Security Network и включить использование Kaspersky Security Network. `no` – отклонить условия Положения о Kaspersky Security Network и выключить использование Kaspersky Security Network.
`<arch>`	Тип архитектуры: `i386` – для 32-битных операционных систем; `x86_64` – для 64-битных операционных систем; `aarch64` – для 64-битных операционных систем для архитектуры Arm.

Приложение Kaspersky Endpoint Security будет автоматически перезапущено.

Пример:

```
Обновить пакет приложения в формате RPM с пакетом графического пользовательского интерфейса для 64-битных
операционных систем:
```

```
# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes rpm -U --replacefiles --replacepkgs kesl-
12.5.0-<build number>.x86_64.rpm kesl-gui-12.5.0-<build number>.x86_64.rpm
```

> Изменения параметров приложения, сделанные после завершения обновления и до перезапуска приложения, не сохраняются.

Как обновить приложение из пакета формата DEB с помощью командной строки

Обновление приложения с помощью командной строки выполняется путем установки на устройство новой версии приложения.

Обновление приложения требуется выполнять с root-правами.

Для обновления приложения на выполните команду:

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] apt-get install ./kesl_12.5.0-<build number>_<arch>.deb [./kesl-gui_12.5.0-<build number>_<arch>.deb]
```

Приложение Kaspersky Endpoint Security будет автоматически перезапущено.

Условные обозначения

Параметры команды

Параметр	Описание
`KESL_EULA_AGREED=yes`	Принять условия условия Лицензионного соглашения.
`KESL_PRIVACY_POLICY_AGREED=yes`	Принять условия Политики конфиденциальности.
`KESL_USE_KSN=yes/no`	Использование Kaspersky Security Network: `yes` – принять условия Положения о Kaspersky Security Network и включить использование Kaspersky Security Network. `no` – отклонить условия Положения о Kaspersky Security Network и выключить использование Kaspersky Security Network.
`<arch>`	Тип архитектуры: `i386` – для 32-битных операционных систем; `amd64` – для 64-битных операционных систем; `arm64` – для 64-битных операционных систем для архитектуры Arm.

Пример:

Обновить пакет приложения в формате DEB с пакетом графического пользовательского интерфейса для 64-битных операционных систем:

```
# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes apt-get install ./kesl_12.5.0-<build number>_amd64.deb [./kesl-gui_12.5.0-<build number>_amd64.deb]
```

Изменения параметров приложения, сделанные после завершения обновления и до перезапуска приложения, не сохраняются.

5 Обновление Агента администрирования Kaspersky Security Center

Необязательный этап. Если вы централизованно управляете приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, обновите Агент администрирования на защищаемых устройствах. Обновление выполняется путем установки новой версии Агента администрирования.

> На устройстве с операционной системой Astra Linux Special Edition рекомендуется обновлять Агент администрирования удаленно с помощью Kaspersky Security Center, так как при обновлении с помощью командной строки в консоли управления Kaspersky Security Center создается новый экземпляр того же управляемого устройства, а старый становится недоступным. Подробнее см. справку Kaspersky Security Center.

Во время обновления Агента администрирования приложение продолжает корректно работать.

Особенности обновления предыдущей версии приложения

- Если во время обновления приложения произошла ошибка, обновление откатывается и запускается предыдущая версия приложения. В этом случае отображается сообщение об ошибке, но в менеджере пакетов указывается новая версия (rpm/dpkg).

- Если на операционной системе с менеджером пакетов типа `rpm` установлены пакет приложения и пакет графического интерфейса, не рекомендуется обновлять только один из пакетов.

  Если на операционной системе с менеджером пакетов типа `dpkg` установлены пакет приложения и пакет графического интерфейса, невозможно обновить только один из пакетов.

- Если в новой версии приложения изменились условия Лицензионного соглашения и/или Политики конфиденциальности, вам нужно принять новые условия в ходе обновления приложения. Тексты пользовательских соглашений доступны на веб-сайте "Лаборатории Касперского" (раздел **EULA**), а также в директории `~/.kesl/12.5/license.<language ID>`.

  Если вы не согласитесь с условиями Лицензионного соглашения и/или Политики конфиденциальности, приложение не будет обновлено.

- Если в новой версии приложения изменились условия Положения о Kaspersky Security Network, вам нужно принять или отклонить новые условия использования Kaspersky Security Network. Текст Положения о Kaspersky Security Network доступен в директории ~/.kesl/12.5/ksn_license.<language ID>. Отказ от использования Kaspersky Security Network не прерывает процесс обновления приложения. Вы можете включить, выключить или изменить режим Kaspersky Security Network позже.

  Если в прошлой версии приложения вы использовали KSN и приняли условия Положения о Kaspersky Security Network, при обновлении версии приложения вам нужно принять условия Положения о Kaspersky Security Network, в противном случае использование KSN будет выключено.

- Независимо от того, было ли приложение Kaspersky Endpoint Security запущено до начала процесса обновления, при успешном обновлении запустится новая версия приложения.

- При обновлении версии приложения файлы дампов предыдущей версии удаляются.

- При обновлении версии приложения файл журнала событий предыдущей версии становится первым файлом с событиями в наборе файлов текущей версии. Этот файл будет хранится до тех пор, пока количество событий в остальных файлах не достигнет заданного максимального количества (задается в параметре `MaxEventsNumber`). Поэтому возможна временная ситуация, когда приложение хранит в два раза больше событий, чем указано в параметре `MaxEventsNumber`.

- Если Kaspersky Endpoint Security используется в стандартном режиме или в режиме EDR-Агента, после обновления приложения рекомендуется запустить задачу обновления баз.

Об обновлении плагинов управления Kaspersky Endpoint Security

Обновление плагина управления Kaspersky Endpoint Security выполняется путем установки новой версии плагина управления. В зависимости от консоли управления Kaspersky Security Center, которую вы используете, вам нужно установить:

- веб-плагин управления Kaspersky Endpoint Security;

- MMC-плагин управления Kaspersky Endpoint Security.

Как установить веб-плагин управления

Вы можете установить веб-плагин:

- С помощью мастера первоначальной настройки Kaspersky Security Center Web Console.

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

- Вручную, используя дистрибутив из списка веб-плагинов "Лаборатории Касперского" или из файла.

Чтобы установить веб-плагин Kaspersky Endpoint Security вручную из Kaspersky Security Center:

1. В главном окне Kaspersky Security Center Web Console выберите **Параметры** → **Веб-плагины**.

   Откроется список установленных веб-плагинов.

2. Нажмите на кнопку **Добавить**.

   Откроется список доступных плагинов управления. Список обновляется автоматически после выпуска новых версий веб-плагинов.

3. В списке доступных плагинов выберите веб-плагин **Kaspersky Endpoint Security <номер версии> для Linux**.

4. В открывшемся окне с описанием веб-плагина нажмите на кнопку **Установить плагин**.

5. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новый плагин отобразится в списке установленных веб-плагинов (**Параметры** → **Веб-плагины**).

Чтобы установить веб-плагин Kaspersky Endpoint Security вручную из файла:

1. Скачайте архив с веб-плагином на странице загрузки приложений в разделе **Kaspersky Endpoint Security для Linux** (**Дополнительный дистрибутив** → **Web console Plug-In**).

2. Локально распакуйте скачанный архив.

3. В главном окне Kaspersky Security Center Web Console выберите **Параметры** → **Веб-плагины**.

   Откроется список установленных веб-плагинов.

4. Нажмите на кнопку **Добавить из файла**.

5. В открывшемся окне укажите путь к файлу plugin.zip и путь к файлу с signature.txt. Файлы находятся в папке, куда вы распаковали архив с веб-плагином.

6. Нажмите на кнопку **Добавить**.

7. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новый плагин отображается в списке установленных веб-плагинов (**Параметры** → **Веб-плагины**).

Если в свойствах Сервера администрирования Kaspersky Security Center вы выбрали язык, которого нет в дистрибутиве приложения Kaspersky Endpoint Security, то Лицензионное соглашение и весь интерфейс в Kaspersky Security Center Web Console будут отображаться на английском языке.

Как установить MMC-плагин управления

Перед установкой MMC-плагина управления Kaspersky Endpoint Security убедитесь, что установлены Kaspersky Security Center и Redist C++ 2015 (Microsoft Visual C++ 2015 Redistributable).

Чтобы установить MMC-плагин:

1. Скачайте файл klcfginst.msi на странице загрузки приложений в разделе **Kaspersky Endpoint Security для Linux** (**Build** → **Administration Plug-In**).

2. На устройстве, где установлена Консоль администрирования Kaspersky Security Center, запустите файл klcfginst.msi.

После установки MMC-плагин управления отображается в списке установленных MMC-плагинов управления в свойствах Сервера администрирования Kaspersky Security Center.

Чтобы посмотреть список установленных MMC-плагинов управления:

1. В дереве Консоли администрирования Kaspersky Security Center выберите узел **Сервер администрирования <имя сервера>** и откройте окно свойств Сервера администрирования одним из следующих способов:

   - откройте контекстное меню узла **Сервер администрирования <имя сервера>** и выберите пункт **Свойства**;

   - перейдите по ссылке **Свойства Сервера администрирования**, расположенной в рабочей области узла **Сервер администрирования <имя сервера>** в блоке **Сервер администрирования**.

2. В списке слева в разделе **Дополнительно** выберите раздел **Информация об установленных плагинах управления программами**.

   В правой части окна в списке установленных плагинов управления отображается MMC-плагин управления Kaspersky Endpoint Security: **Kaspersky Endpoint Security <номер версии> для Linux**.

Конвертация политик и задач

Политики и задачи, настроенные для предыдущих версий приложения Kaspersky Endpoint Security, не совместимы с обновленной версией приложения. Если для управления приложением вы используете Консоль администрирования Kaspersky Security Center, после обновления MMC-плагина управления вы можете сконвертировать политики и задачи с помощью мастера массовой конвертации политик и задач Kaspersky Security Center (см. подробнее в справке Kaspersky Security Center).

Сконвертированные политики и задачи имеют название "*<Название исходной политики или задачи> (конвертированная)*".

В сконвертированных политиках и задачах для большинства параметров используются значения, настроенные для предыдущей версии приложения. Для некоторых параметров устанавливаются особые значения. Параметры, которые отсутствовали в политиках и задачах предыдущей версии, в сконвертированных политиках и задачах принимают значения по умолчанию.

Конвертация политик и задач в Kaspersky Security Center Web Console недоступна.

Если для управления приложением вы используете Web Console, вам нужно создать новые политики и задачи для приложения в Kaspersky Security Center. Некоторые значения параметров политик и задач вы можете переносить из предыдущей версии политики или задачи в новую путем экспорта и импорта параметров.

Особенности работы плагинов управления

- Плагины управления предыдущей версии продолжают работать после установки новой версии плагинов управления Kaspersky Endpoint Security. С их помощью вы можете управлять приложением Kaspersky Endpoint Security предыдущей версии.

  Если вы обновили приложение на всех клиентских устройствах, вы можете удалить плагины управления Kaspersky Endpoint Security предыдущей версии.

- При установке новой сборки MMC-плагина управления той же версии приложения требуется сначала удалить уже установленный MMC-плагин этой версии, а затем установить новый MMC-плагин этой версии.

Параметры приложения после обновления версии

Если для управления приложением вы используете Консоль администрирования Kaspersky Security Center, вы можете выполнить *конвертацию политик*, чтобы в новой версии приложения использовать параметры политики, настроенные для предыдущей версии приложения (см. подробнее в справке Kaspersky Security Center).

Конвертация политик в Kaspersky Security Center Web Console недоступна.

После обновления приложения с помощью командной строки для большинства параметров значения переносятся из предыдущей версии приложения. Вы также можете перенести параметры приложения путем экспорта параметров в файл и импорта из файла.

Параметры, которые отсутствовали в предыдущей версии приложения, принимают значения по умолчанию. Для некоторых параметров устанавливаются особые значения.

Параметры перехвата системных событий

Если в предыдущей версии приложения был выбран механизм перехвата системных событий на основе обновляемого модуля ядра, после обновления приложение переходит к использованию технологии fanotify для перехвата системных событий. Затем после обновления баз и модулей приложения и автоматического перезапуска приложение возвращается к использованию обновляемого модуля ядра.

Параметры использования Kaspersky Security Network

После конвертации политики в MMC-плагине параметры использования Kaspersky Security Network в свойствах политики зависят от того, приняли вы или отклонили условия Положения о Kaspersky Security Network в мастере конвертации политик и задач:

- Если вы приняли условия Положения, выбран вариант **Расширенный режим KSN**.

- Если вы отклонили условия Положения, выбран вариант **Не использовать KSN**.

После обновления приложения с помощью командной строки для параметр `UseKSN` меняется следующим образом:

- Если при обновлении вы установили значение параметра `KESL_USE_KSN=No`: `UseKSN=No`.
- Если при обновлении вы установили значение параметра `KESL_USE_KSN=Yes`: `UseKSN=Extended`.
- В остальных случаях значение параметра `UseKSN` после обновления не меняется.

Параметры использования облачного режима

После конвертации политики в MMC-плагине параметр использования облачного режима может измениться в зависимости от того, приняли вы или отклонили условия Положения о Kaspersky Security Network в мастере конвертации политик и задач:

- Если вы приняли условия Положения, флажок **Включить облачный режим** будет установлен.
- Если вы отклонили условия Положения, флажок **Включить облачный режим** будет снят.

После обновления приложения с помощью командной строки для параметра `CloudMode` устанавливаются следующие значения:

- `CloudMode=No`, в случае если параметр `UseKSN=No` после обновления;
- `CloudMode=Yes`, если параметр `UseKSN=Basic/Extended` после обновления и до обновления было установлено значение `CloudMode=Yes`.

Облачный режим доступен, если включено использование KSN. Чтобы включить облачный режим:

- в Консоли администрирования или в Web Console выберите вариант **Расширенный режим KSN** и установите флажок **Включить облачный режим**.
- в командной строке задайте следующие значения параметров:

```
UseKSN=<Basic|Extended>
CloudMode=Yes
```

Параметры интеграции с Kaspersky Managed Detection and Response

Если компонент MDR был включен, после конвертации политики в MMC-плагине статус компонента MDR зависит от того, приняли вы или отклонили условия Положения о Kaspersky Security Network в мастере конвертации политик и задач:

- Если вы приняли условия Положения, компонент MDR останется включенным (установлен флажок **Включить Managed Detection and Response**).
- Если вы отклонили условия Положения, флажок **Включить Managed Detection and Response** будет снят.

После обновления приложения с помощью командной строки для параметра `UseMDR` устанавливаются следующие значения:

- `UseMDR=No`, в случае если параметр `UseKSN=No` после обновления;
- `UseMDR=Yes`, если параметр `UseKSN=Basic/Extended` после обновления и до обновления было установлено значение `UseMDR=Yes`.

Если вы хотите использовать функциональность Kaspersky Managed Detection and Response, вам нужно включить использование Kaspersky Security Network в расширенном режиме.

Параметры интеграции с Endpoint Detection and Response Expert

В новой версии приложения доступен режим интеграции с решением Kaspersky Endpoint Detection and Response Expert (cloud).

Интеграция Kaspersky Endpoint Security для Linux с решением Kaspersky Endpoint Detection and Response Expert (cloud) временно недоступна. Поддержка функциональности запланирована на конец 2026 года. Следите за нашими Release Notes, чтобы быть в курсе обновлений приложения и новых возможностей.

После конвертации политики в MMC-плагине интеграция с Endpoint Detection and Response Expert (cloud) выключена (флажок **Включить Endpoint Detection and Response Expert (cloud)** снят). Приложение использует интеграцию с Endpoint Detection and Response Expert (on-premises).

После обновления приложения с помощью командной строки для параметра `EDR_EXPERT_CLOUD_MODE` устанавливается значение `EDR_EXPERT_CLOUD_MODE=No` (значение по умолчанию).

Параметры прав пользователей

В новой версии приложения доступна Защита паролем.

После конвертации политики в MMC-плагине Защита паролем выключена.

После обновления приложения с помощью командной строки права пользователей сохраняются в соответствии с настроенными в предыдущей версии приложения ролями пользователей (*kesladmin*, *kesluser*, *keslaudit*, *nokesl*).

Удаление приложения

Следуя этому сценарию, вы можете удалить приложение Kaspersky Endpoint Security.

Особенности удаления Kaspersky Endpoint Security для Linux

- В процессе удаления приложения на устройстве будут остановлены все задачи Kaspersky Endpoint Security.
- После удаления приложения удаляется вся информация, сохраненная во время его работы, в том числе установленные сертификаты приложения. База данных лицензий сохраняется, вы можете использовать ее для повторной установки приложения. Также сохраняется уникальный идентификатор компьютера (SensorID).
- Если приложение было установлено в systemd-системе, то после удаления приложения параметры systemd возвращаются в исходное состояние.

1 Удаление приложения и графического интерфейса приложения

Удалите с защищаемых устройств пакеты приложения и графического интерфейса приложения.

Вы можете одновременно удалить пакет приложения и пакет графического интерфейса или удалить только пакет графического интерфейса. Невозможно удалить только пакет приложения, если установлен пакет графического интерфейса.

Вы можете удалять приложение и графический интерфейс приложения следующими способами:

Удаленно с помощью Kaspersky Security Center

Локально из командной строки

Удаление требуется выполнять с root-правами.

После завершения процедуры удаления выводится сообщение о результатах удаления.

Удаление пакета приложения и пакета графического интерфейса

Удалить приложение и графический интерфейс приложения, установленные из пакетов формата RPM

```
rpm -e kesl kesl-gui
```

Удалить приложение и графический пользовательский интерфейс, установленные из пакетов формата DEB

```
apt-get purge kesl kesl-gui
```

Удаление пакета приложения, который использовался без графического интерфейса

Удалить приложение, установленное из пакета формата RPM

```
rpm -e kesl
```

Удалить приложение, установленное из пакета формата DEB

```
apt-get purge kesl
```

Удаление пакета графического интерфейса

Удалить графический интерфейс приложения, установленный из пакета формата RPM

```
rpm -e kesl-gui
```

Удалить графический интерфейс приложения, установленный из пакета формата DEB

```
apt-get purge kesl-gui
```

Удаление выполняется в фоновом режиме.

2 Удаление Агента администрирования

Если вы использовали Kaspersky Security Center для управления приложением Kaspersky Endpoint Security, вам нужно удалить Агент администрирования с защищаемых устройств.

Вы можете удалять Агент администрирования следующими способами:

Удаленно с помощью Kaspersky Security Center

Локально из командной строки

Удаление требуется выполнять с root-правами.

После завершения процедуры удаления выводится сообщение о результатах удаления.

Удалить Агент администрирования, установленный на 32-битную операционную систему из пакета формата RPM

```
rpm -e klnagent
```

Удалить Агент администрирования, установленный на 64-битную операционную систему из пакета формата RPM

```
rpm -e klnagent64
```

Удалить Агент администрирования, установленный на 32-битную операционную систему из пакета формата DEB

```
apt-get purge klnagent
```

Удалить Агент администрирования, установленный на 64-битную операционную систему из пакета формата DEB

```
apt-get purge klnagent64
```

3 Удаление плагина управления Kaspersky Endpoint Security

Если вы использовали Kaspersky Security Center для управления приложением Kaspersky Endpoint Security, вам нужно удалить веб-плагин или MMC-плагин управления Kaspersky Endpoint Security, в зависимости от консоли управления Kaspersky Security Center, которую вы использовали.

Как удалить MMC-плагин управления Kaspersky Endpoint Security

1. Закройте Консоль администрирования Kaspersky Security Center.

2. На устройстве, где установлена Консоль администрирования Kaspersky Security Center, откройте редактор системного реестра Windows и перейдите в ветку:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins
   ```

   В этой ветке содержатся данные обо всех плагинах управления, установленных в Консоли администрирования. Название управляемого приложения находится в параметре **DisplayName**.

3. Выберите раздел, который соответствует плагину приложения Kaspersky Endpoint Security нужной версии.

4. Откройте параметр **UninstallString** и скопируйте его значение.

5. Откройте командную строку с правами администратора, вставьте скопированное значение и нажмите на клавишу **`Enter`**.

Как удалить веб-плагин управления Kaspersky Endpoint Security

1. В главном окне Kaspersky Security Center Web Console выберите **Параметры** → **Веб-плагины**.

   Откроется список установленных веб-плагинов.

2. Установите флажок напротив плагина **Kaspersky Endpoint Security <номер версии> для Linux**.

3. Нажмите на кнопку **Удалить**.

   Подтвердите удаление веб-плагина.

Работа с приложением

По умолчанию приложение Kaspersky Endpoint Security запускается автоматически при запуске операционной системы (на уровнях выполнения по умолчанию, принятых для каждой операционной системы).

При запуске приложения с конфигурацией по умолчанию запускаются следующие компоненты:

- Защита от файловых угроз.
- Контроль устройств.
- Анализ поведения.
- Защита от веб-угроз – только если в операционной системе установлен один из поддерживаемых браузеров и на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в свойствах политики не установлен).
- Защита от сетевых угроз – только если параметры защиты от сетевых угроз на устройстве заданы через политику. По умолчанию в свойствах политики включена защита от сетевых угроз. Если на устройстве применяются локально настроенные параметры, по умолчанию защита от сетевых угроз выключена.

При запуске приложения на устройстве автоматически запускаются служебные задачи, обеспечивающие работу дополнительных функций приложения: функции активации приложения и функции резервного хранилища.

По умолчанию приложение также запускает настроенные в командной строке пользовательские задачи, для которых задан режим запуска "после запуска приложения" (режим запуска `PS`).

Если вы остановите приложение, то все выполняющиеся на устройстве задачи будут прерваны. Прерванные пользовательские задачи с режимом запуска PS не продолжаются с места остановки. При следующем запуске приложения такая задача будет выполнена заново, а не возобновлена с прерванного места. Подробнее о типах задач см. в разделе Локальные задачи Kaspersky Endpoint Security.

Мониторинг статуса приложения Kaspersky Endpoint Security выполняется с помощью контрольной службы. Контрольная служба автоматически запускается при запуске приложения. В случае сбоя приложения создается файл дампа, и приложение автоматически перезапускается.

Как запустить и остановить приложение с помощью Web Console

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. В списке выберите устройство, на котором вы хотите запустить или остановить приложение, и по ссылке с названием устройства откройте окно свойств устройства.

3. Выберите вкладку **Приложения**.

4. Установите флажок напротив приложения Kaspersky Endpoint Security.

5. Выполните одно из следующих действий:

   - Если вы хотите запустить приложение, нажмите на кнопку **Запустить**.

   - Если вы хотите остановить работу приложения, нажмите на кнопку **Остановить**.

Вы можете контролировать статус работы приложения с помощью виджета **Состояние защиты** в окне **Мониторинг и отчеты / Панель мониторинга**.

Как запустить и остановить приложение с помощью Консоли администрирования

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.

2. В рабочей области выберите вкладку **Устройства**.

3. В списке управляемых устройств выберите устройство, на котором вы хотите запустить или остановить приложение, и в контекстном меню устройства выберите пункт **Свойства**.

4. В окне **Свойства: <Имя устройства>** выберите раздел **Приложения**.

   В правой части окна отобразится список приложений "Лаборатории Касперского", установленных на устройстве.

5. Выберите приложение Kaspersky Endpoint Security.

6. Выполните одно из следующих действий:

   – запуск приложения.

   – остановка приложения.

   Также вы можете управлять приложением из контекстного меню.

Как запустить и остановить приложение с помощью командной строки

Для запуска приложения требуется, чтобы учетная запись root была владельцем следующих директорий и только владелец имел право на запись в них: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

ОС с системой инициализации systemd

Запустить приложение

```
systemctl start kesl
```

Остановить приложение

```
systemctl stop kesl
```

Перезапустить приложение

```
systemctl restart kesl
```

Вывести текущий статус приложения

```
systemctl status kesl
```

ОС с системой инициализации init

Запустить приложение

```
service kesl start
```

Остановить приложение

```
service kesl stop
```

Перезапустить приложение

```
service kesl restart
```

Вывести текущий статус приложения

```
service kesl status
```

Лицензирование

Лицензия – это ограниченное по времени право на использование Kaspersky Endpoint Security, предоставляемое вам на условиях заключенного Лицензионного соглашения. Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Типы лицензии

Бесплатная

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

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

  Вы можете активировать приложение по пробной лицензии только один раз. Активировать приложение по пробной лицензии после того, как вы активировали приложение по коммерческой лицензии, невозможно.

- *Пробная лицензия Kaspersky Security Center Cloud Console* – лицензия, предназначенная для ознакомления с Cloud Console. С этой лицензией вы можете выполнять действия в рабочем пространстве в течение 30 дней. Все управляемые приложения, включая приложение Kaspersky Endpoint Security, активируются по пробной лицензии Kaspersky Security Center Cloud Console автоматически. При этом активировать приложение Kaspersky Endpoint Security по собственной пробной лицензии по истечении пробной лицензии Cloud Console невозможно.

  Пробное рабочее пространство будет автоматически удалено со всем его содержимым по истечении 30 дней.

Платная

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

  По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky Endpoint Security вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

- *Подписка* – это заказ на использование приложения с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку вы можете приобрести у поставщика услуг в вашем регионе.

  Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность приложения сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

  Управлять подпиской, в том числе отказаться от нее, вы можете на сайте поставщика услуг.

Как работает лицензирование

1. **Вы получите код активации**

   После того как вы купили решение "Лаборатории Касперского" на официальном сайте "Лаборатории Касперского" или у наших партнеров, вы получите письмо на адрес электронной почты, который указали при покупке. В письме будет код активации и информация о том, как получить файл ключа. Файл ключа вам может потребоваться, если на вашем предприятии не поддерживается онлайн-активация приложения с помощью кода.

   Если вы приобрели подписку на Kaspersky Endpoint Security, поставщик услуг предоставит вам только код активации.

2. **Активация приложения**

   Далее вам нужно *активировать приложение* – ввести в действие лицензию на использование приложения. Для этого требуется с помощью кода активации или файла ключа добавить в приложение лицензионный ключ.

Для активации предусмотрены следующие способы:

- Удаленно через Kaspersky Security Center
- В командной строке
- Через графический интерфейс

Стандартный режим

Для работы приложения в стандартном режиме предусмотрены лицензии с разным объемом функциональности. Если какие-то компоненты не включены в вашу лицензию, вам может потребоваться еще один лицензионный ключ:

- лицензионный ключ Kaspersky Endpoint Detection and Response Optimum Add-on (далее также *ключ EDR Optimum*) – для активации компонента EDR Optimum
- лицензионный ключ Kaspersky Unified Monitoring and Analysis Platform Add-on (далее также *ключ KUMA*) – для активации интеграции с Kaspersky Unified Monitoring and Analysis Platform
- лицензионный ключ Kaspersky Managed Detection and Response Optimum/Expert Add-on (далее также *ключ MDR*) – для активации компонента MDR
- лицензионный ключ Kaspersky Endpoint Detection and Response Expert (on-premises) Add-on (далее также *ключ EDR Expert (on-premises)*) – для активации компонента EDR Expert (on-premises)
- лицензионный ключ Kaspersky Endpoint Detection and Response Expert (cloud) Add-on (далее также *ключ EDR Expert (cloud)*) – для активации компонента EDR Expert (cloud)
- лицензионный ключ Kaspersky Workload Security Module Add-on (далее также *ключ KWSM*) – для активации компонентов Контроль целостности системы и Проверка контейнеров

Если эти компоненты не включены в вашу лицензию, активировать их вы можете только после активации приложения Kaspersky Endpoint Security.

Режим EDR-агента

Если вы используете приложение Kaspersky Endpoint Security в режиме EDR-агента, для активации вам потребуется лицензионный ключ EDR Expert (on-premises).

Режим Легкого агента

Если вы используете приложение Kaspersky Endpoint Security в режиме Легкого агента, добавлять ключ в приложение не требуется. Вы активируете решение Kaspersky Security для виртуальных сред Легкий агент на стороне Сервера защиты.

Активация компонента Endpoint Detection and Response Optimum и компонентов для интеграции с решениями "Лаборатории Касперского" также выполняется на стороне Сервера защиты.

Решение проблем с активацией приложения

3. **Продление срока действия лицензии или подписки**

Рекомендуется следить и своевременно продлевать срок действия лицензии или подписки. Рекомендуется продлевать срок действия не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

Для своевременного продления срока действия лицензии вы можете использовать резервный ключ. Подписку вы можете продлевать вручную или автоматически на сайте поставщика услуг. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Особенности добавления ключей

- Лицензионный ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве резервного ключа.
- Дата окончания срока действия резервного ключа должна быть больше даты окончания срока действия активного ключа.
- Если в приложение ранее были добавлены и активный ключ, и резервный ключ, и вы добавляете новый активный ключ, то он заменит ранее добавленный активный ключ; если вы добавляете новый резервный ключ, то он заменит ранее добавленный резервный ключ.
- Если в приложение ранее были добавлены активный ключ и ключи для активации компонента Endpoint Detection and Response Optimum и компонентов для интеграции с решениями "Лаборатории Касперского", и вы добавили один резервный ключ, лицензия которого включает в себя также компонент Endpoint Detection and Response Optimum и компоненты для интеграции, то по истечении срока действия активного ключа резервный ключ станет активным и освободит другие активные ключи. Вы можете использовать эти ключи для активации компонента Endpoint Detection and Response Optimum и компонентов для интеграции на другом устройстве.

4. **Просмотр информации о добавленных лицензионных ключах**

   Вы можете посмотреть информацию о лицензионных ключах, добавленных в приложение, удаленно с помощью Kaspersky Security Center или локально на защищенном устройстве с помощью командной строки или графического интерфейса.

Полезные статьи

Лицензионное соглашение

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

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом использования приложения.

Лицензионное соглашение и Политику конфиденциальности, которая описывает обработку и передачу данных, вы можете прочитать:

- Перед установкой приложения в файле license.<идентификатор языка>. Этот файл включен в комплект поставки приложения.
- Во время установки приложения Kaspersky Endpoint Security.

  Вы принимаете условия Лицензионного соглашения и Политики конфиденциальности, подтверждая свое согласие с текстом Лицензионного соглашения и Политики конфиденциальности во время создания инсталляционного пакета приложения (в случае установки с помощью Kaspersky Security Center) или во время первоначальной настройки приложения (в случае установки с помощью командной строки). Если вы не согласны с условиями Лицензионного соглашения и Политики конфиденциальности, вы должны прервать установку приложения и не должны использовать приложение.

- После установки приложения файлы с текстом Лицензионного соглашения и Политики конфиденциальности расположены на защищаемом устройстве в директории /opt/kaspersky/kesl/doc/license.<идентификатор языка>.

Код активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр.

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

Если код активации был потерян после активации приложения, свяжитесь с партнером "Лаборатории Касперского", у которого вы приобрели лицензию.

Файл ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Для активации приложения 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.

Лицензионный ключ

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

Ключ, используемый в текущий момент для работы приложения, становится *активным лицензионным ключом*. В качестве активного может быть добавлен лицензионный ключ для пробной лицензии, ключ для коммерческой лицензии (коммерческий ключ) или ключ по подписке.

Резервный ключ

Резервный лицензионный ключ – лицензионный ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. Резервный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Резервный ключ можно добавить только после добавления активного ключа.

Лицензионный ключ для пробной лицензии можно добавить только в качестве активного ключа. Лицензионный ключ для пробной лицензии нельзя добавить в качестве резервного ключа.

Как перейти на другое решение "Лаборатории Касперского"

Если приложение используется в режиме Легкого агента, управление лицензионными ключами выполняется на стороне решения Kaspersky Security для виртуальных сред Легкий агент.

Если в вашей организации развернуто решение "Лаборатории Касперского", приложение Kaspersky Endpoint Security используется в стандартном режиме или режиме EDR-агента, и вам требуется перейти на другое решение "Лаборатории Касперского", воспользуйтесь этим сценарием.

1. **Подготовьте новую лицензию**

   Купите другое решение "Лаборатории Касперского" на официальном сайте "Лаборатории Касперского" или у наших партнеров. Вы получите письмо на адрес электронной почты, который указали при покупке. В письме будет код активации и информация о том, как получить файл ключа.

   Если ранее вы активировали приложение Kaspersky Endpoint Security с помощью кода активации, сейчас вам также потребуется код активации. Если ранее вы активировали приложение с помощью файла ключа, вам потребуется файл ключа.

2. **Замените лицензию**

   Для замены лицензии предусмотрены следующие способы:

   - Удаленно с помощью Kaspersky Security Center. Добавьте лицензионный ключ в хранилище Сервера администрирования и распространите его на защищаемые устройства.
   - В командной строке с помощью команды `kesl-control [-L] --add-active-key <path to key file / activation code>`
   - В графическом интерфейсе удалите ключ, по которому используете приложение, и добавьте новый.

3. **Убедитесь, что лицензия заменена успешно**

   Для этого посмотрите информацию о лицензионном ключе, который используется на ваших защищаемых устройствах.

Полезные статьи

Код активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр.

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

Если код активации был потерян после активации приложения, свяжитесь с партнером "Лаборатории Касперского", у которого вы приобрели лицензию.

Файл ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Для активации приложения 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.

Управление лицензионными ключами

Если приложение используется в режиме Легкого агента, управление лицензионными ключами выполняется на стороне решения Kaspersky Security для виртуальных сред Легкий агент. Команды управления лицензионными ключами завершаются с ошибкой.

Управление ключами с помощью Kaspersky Security Center

В Kaspersky Security Center вы можете добавлять ключи на управляемые устройства следующими способами:

- С помощью задачи *Добавление ключа*. Этот способ позволяет добавлять ключи в приложение на конкретном устройстве или на всех устройствах, входящих в группу администрирования. При создании задачи используется ключ, добавленный в хранилище ключей Kaspersky Security Center. Вы можете добавить лицензионный ключ в хранилище ключей предварительно или во время создания задачи добавления ключа в приложение.
- Путем распространения на устройства ключа, размещенного на Сервере администрирования Kaspersky Security Center. Этот способ позволяет автоматически добавлять ключи на управляемые устройства, уже подключенные к Kaspersky Security Center, а также на новые управляемые устройства. Для использования этого способа требуется сначала добавить ключ в хранилище ключей Kaspersky Security Center.

  При автоматическом распространении ключа в качестве активного или резервного учитывается лицензионное ограничение на количество устройств, заданное в свойствах ключа. Если лицензионное ограничение достигнуто, распространение ключа на устройства автоматически прекращается. Вы можете просмотреть количество устройств, на которые добавлен ключ, и другие данные в свойствах ключа на вкладке **Устройства**.

Как добавить ключ в хранилище ключей Kaspersky Security Center с помощью Web Console

1. В главном окне Web Console выберите **Операции** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Добавить**.

3. В открывшемся окне выберите способ добавления ключа в хранилище:

   - **Ввести код активации**, если вы хотите добавить ключ с помощью кода активации.
   - **Добавить файл ключа**, если вы хотите добавить ключ с помощью файла ключа.

4. В зависимости от выбранного вами на предыдущем шаге способа добавления ключа, выполните одно из следующих действий:

   - Введите код активации и нажмите на кнопку **Отправить**.
   - Нажмите на кнопку **Выберите файл ключа** и в открывшемся окне выберите файл с расширением .key.

5. Нажмите на кнопку **Закрыть**.

Добавленный ключ отобразится в списке ключей.

Как добавить ключ в приложение через Web Console с помощью задачи Добавление ключа

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите название приложения Kaspersky Endpoint Security.

   b. В раскрывающемся списке **Тип задачи** выберите **Добавление ключа**.

   c. В поле **Название задачи** введите короткое описание, например, *Активация Kaspersky Endpoint Security*.

   d. В разделе **Устройства, которым будет назначена задача** выберите область действия задачи. Нажмите на кнопку **Далее**.

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

   Откроется окно **Выберите лицензию**.

5. Если вы добавили ключ в хранилище ключей Kaspersky Security Center предварительно, выберите ключ в списке и нажмите на кнопку **Далее**.

6. Если нужный ключ в хранилище ключей отсутствует, перейдите по ссылке **добавить новый лицензионный ключ**.

   a. В открывшемся окне выберите способ добавления ключа в хранилище:

      - **Ввести код активации**, если вы хотите добавить ключ с помощью кода активации.
      - **Добавить файл ключа**, если вы хотите добавить ключ с помощью файла ключа.

b. В зависимости от выбранного вами на предыдущем шаге способа добавления ключа, выполните одно из следующих действий:

- Введите код активации и нажмите на кнопку **Отправить**.
- Нажмите на кнопку **Выберите файл ключа** и в открывшемся окне выберите файл с расширением .key.

c. Ознакомьтесь с информацией о ключе и нажмите на кнопку **Закрыть**.

d. Добавленный ключ отобразится в списке ключей. Выберите его в списке и нажмите на кнопку **Далее**.

7. Ознакомьтесь с информацией о лицензии и нажмите на кнопку **Далее**.

8. На вкладке **Параметры приложения** вы можете установить флажок **Использовать ключ в качестве резервного**. Добавленный в качестве резервного ключ станет активным после окончания срока действия текущего ключа.

9. Завершите работу мастера.

   В списке задач отобразится новая задача.

10. Установите флажок напротив задачи. Нажмите на кнопку **Запустить**.

Как добавить ключ в приложение через Web Console путем распространения ключа на устройства

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

2. Откройте свойства ключа по ссылке с названием приложения, для активации которого предназначен ключ.

3. На вкладке **Общие** установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**.

4. Нажмите на кнопку **Сохранить**.

Лицензионный ключ будет автоматически распространяться на клиентские устройства, для которых он подходит.

Новый лицензионный ключ будет добавлен на устройство, только если приложение на этом устройстве еще не активировано или срок действия лицензии истекает менее, чем через 14 дней.

Управление ключами в командной строке

Для управления лицензионными ключами на устройстве вы можете использовать [команды управления лицензионными ключами](#).

Как добавить в приложение ключ

С помощью этих команд вы можете добавлять ключи для активации приложения и ключи для активации компонентов, которые не включены в вашу лицензию. Указывать тип ключа в команде не требуется.

Добавить в приложение активный лицензионный ключ

```
kesl-control [-L] --add-active-key <path to key file / activation code>
```

Где:

- `path to key file` – путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.
- `activation code` – код активации.

Добавить в приложение резервный лицензионный ключ

```
kesl-control [-L] --add-reserve-key <path to key file / activation code>
```

Если активный ключ еще не добавлен в приложение на устройстве, команда завершается с ошибкой.

Как удалить ключ

Для удаления ключей предусмотрены разные команды.

Удалить активный ключ

```
kesl-control [-L] --remove-active-key
```

Удалить резервный ключ

```
kesl-control [-L] --remove-reserve-key
```

Удалить активный ключ EDR Optimum

```
kesl-control [-L] --remove-active-key --edr-optimum
```

Удалить резервный ключ EDR Optimum

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

Удалить активный ключ KUMA

```
kesl-control [-L] --remove-active-key --kuma
```

Удалить резервный ключ KUMA

```
kesl-control [-L] --remove-reserve-key --kuma
```

Удалить активный ключ MDR

```
kesl-control [-L] --remove-active-key --mdr
```

Удалить резервный ключ MDR

```
kesl-control [-L] --remove-reserve-key --mdr
```

Удалить активный ключ EDR Expert (on-premises)

```
kesl-control [-L] --remove-active-key --edr-kata
```

Удалить резервный ключ EDR Expert (on-premises)

```
kesl-control [-L] --remove-reserve-key --edr-kata
```

Удалить активный ключ EDR Expert (cloud)

```
kesl-control [-L] --remove-active-key --cxdr
```

Удалить резервный ключ EDR Expert (cloud)

```
kesl-control [-L] --remove-reserve-key --cxdr
```

Удалить активный ключ KWSM

```
kesl-control [-L] --remove-active-key --khcs
```

Удалить резервный ключ KWSM

```
kesl-control [-L] --remove-reserve-key --khcs
```

Управление ключами в графическом интерфейсе

Как добавить активный лицензионный ключ

1. Откройте главное окно графического интерфейса приложения.
2. Выполните одно из следующих действия:
   - В нижней части главного окна нажмите на область окна, в которой отображается информация о лицензии и о ключе.
   - В нижней части главного окна нажмите на кнопку **Поддержка** и в открывшемся окне **Поддержка** перейдите по ссылке в поле **Лицензионный ключ** или по ссылке **Лицензии** в нижней части окна.

   Откроется окно **Лицензии**.

По кнопке **Приобрести лицензию** в этом окне вы можете открыть веб-сайт интернет-магазина "Лаборатории Касперского", где можно приобрести лицензию.

3. Если вы хотите активировать приложение по коммерческой лицензии:

   a. Нажмите на кнопку **Добавить** в блоке **Коммерческий ключ** и выполните следующие действия в зависимости от способа добавления ключа:

      - Если вы хотите добавить ключ с помощью кода активации, введите код активации и нажмите на кнопку **Далее**.

      - Если вы хотите добавить ключ с помощью файла ключа, откройте окно выбора файла по ссылке **Выбрать файл ключа** и в открывшемся окне выберите файл с расширением .key.

      В окне отобразится информация о ключе и связанной с ним лицензии.

   b. Нажмите на кнопку **Активировать**.

4. Если вы хотите активировать приложение по пробной лицензии, нажмите на кнопку **Активировать** в блоке **Пробный ключ**. В окне отобразится информация о пробной лицензии и связанном с ней ключе.

Как добавить резервный лицензионный ключ

1. Откройте главное окно графического интерфейса приложения.

2. Выполните одно из следующих действия:

   - В нижней части главного окна нажмите на область окна, в которой отображается информация о лицензии и о ключе.

   - В нижней части главного окна нажмите на кнопку **Поддержка** и в открывшемся окне **Поддержка** перейдите по ссылке в поле **Лицензионный ключ** или по ссылке **Лицензии** в нижней части окна.

   Откроется окно **Лицензии**. В окне отображается информация о ранее добавленных лицензионных ключах.

3. Нажмите на кнопку **Добавить** и выполните следующие действия в зависимости от способа добавления ключа:

   - Если вы хотите добавить ключ с помощью кода активации, введите код активации и нажмите на кнопку **Далее**.

   - Если вы хотите добавить ключ с помощью файла ключа, откройте окно выбора файла по ссылке **Выбрать файл ключа** и в открывшемся окне выберите файл с расширением key.

   В окне отобразится информация о ключе и связанной с ним лицензии.

4. Нажмите на кнопку **Добавить**.

Как удалить лицензионный ключ

1. Откройте главное окно графического интерфейса приложения.

2. Выполните одно из следующих действия:

   - В нижней части главного окна нажмите на область окна, в которой отображается информация о лицензии и о ключе.

   - В нижней части главного окна нажмите на кнопку **Поддержка** и в открывшемся окне **Поддержка** перейдите по ссылке в поле **Лицензионный ключ** или по ссылке **Лицензии** в нижней части окна.

   Откроется окно **Лицензии**. В окне отображается информация о ранее добавленных лицензионных ключах.

3. Нажмите на кнопку **Удалить**, расположенную справа от информации о ключе, который вы хотите удалить.

4. Подтвердите удаление в открывшемся окне.

Полезные статьи

Решение проблем с активацией приложения

Просмотр информации о лицензионных ключах

Информация о лицензионных ключах в Kaspersky Security Center

Вы можете просматривать информацию о лицензионных ключах, которые использует приложение Kaspersky Endpoint Security, следующими способами:

- В свойствах задачи *Добавление ключа*, с помощью которой вы активировали приложение, отображаются сведения о ключе, который добавляется в приложение в результате выполнения этой задачи.

- В свойствах приложения "Лаборатории Касперского", установленного на клиентском устройстве, отображается информация об активном и резервном ключах, добавленных в приложение на этом устройстве.

  Как посмотреть информацию о ключах на устройстве через Web Console

  1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

     Откроется список управляемых устройств.

  2. Выберите группу администрирования, содержащую нужное вам устройство. Чтобы выбрать вложенную группу, нажмите на кнопку **Показать иерархию** в верхней части окна.

     В списке отобразятся только управляемые устройства выбранной группы администрирования.

  3. Нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

5. В списке приложений, установленных на устройстве, нажмите на название приложения Kaspersky Endpoint Security.

6. В открывшемся окне свойств приложения перейдите в раздел **Лицензии** на вкладке **Общие**.

   В разделе отображается информация о лицензионных ключах, добавленных в приложение, и связанных с этими ключами лицензиях:

   - **Статус лицензионного ключа** – тип ключа: активный или резервный.
   - **Название приложения** – название лицензии, связанной с ключом, и информация об этой лицензии.
   - **Лицензионный ключ** – лицензионный ключ, уникальная буквенно-цифровая последовательность.
   - **Тип лицензии** – тип лицензии: пробная, коммерческая или подписка.
   - **Дата активации** – дата добавления этого ключа.
   - **Срок действия** – дата окончания срока использования приложения, активированного путем добавления этого ключа.

Как посмотреть информацию о ключах на устройстве через Консоль администрирования

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.

2. В рабочей области выберите вкладку **Устройства**.

3. В списке управляемых устройств выберите нужное вам устройство и откройте окно **Свойства: <Имя устройства>** двойным щелчком мыши.

4. В открывшемся окне свойств управляемого устройства выберите раздел **Программы**.

   В правой части окна отобразится список приложений "Лаборатории Касперского", установленных на устройстве.

5. Выберите приложение Kaspersky Endpoint Security и откройте окно свойств приложения двойным щелчком мыши или с помощью кнопки **Свойства** в нижней части окна.

6. В открывшемся окне перейдите в раздел **Лицензионные ключи**.

   В разделе отображается информация об активном и резервном лицензионных ключах:

   - **Серийный номер** – уникальная буквенно-цифровая последовательность.
   - **Статус** – статус лицензионного ключа, например, активный или резервный.
   - **Тип** – тип лицензии: коммерческая или пробная.
   - **Срок действия лицензии** – количество дней, в течение которых возможно использование приложения, активированного путем добавления этого ключа.
   - **Ограничения лицензии** – количество устройств, на которых вы можете использовать ключ.

    - **Дата активации** (поле доступно только для активного ключа) – дата добавления активного ключа.
    - **Срок действия** (поле доступно только для активного ключа) – дата окончания срока использования приложения, активированного путем добавления активного ключа.

- В отчете об использовании лицензионных ключей отображается информация обо всех ключах, добавленных с помощью Kaspersky Security Center. Вы можете просматривать отчет об использовании ключей с помощью Web Console (**Мониторинг и отчеты** → **Отчеты**), а также с помощью Консоли администрирования (вкладка **Отчеты**). Чтобы посмотреть отчет, вам нужно выбрать в списке отчетов шаблон "Отчет об использовании лицензионных ключей" и запустить формирование отчета.

- В хранилище лицензионных ключей Kaspersky Security Center отображается информация обо всех ключах, добавленных на Сервер администрирования Kaspersky Security Center. Вы можете открыть хранилище ключей с помощью Web Console (**Операции** → **Лицензии "Лаборатории Касперского"**), а также с помощью Консоли администрирования (папка **Лицензии Лаборатории Касперского**).

Вы также можете получать информацию об используемых лицензионных ключах и связанных с ними лицензиях с помощью уведомлений о событиях Kaspersky Security Center. Приложение отправляет на Сервер администрирования Kaspersky Security Center информацию об истечении срока действий лицензий и о нарушении лицензионных ограничений.

Информация о лицензионных ключах на защищаемом устройстве

Как посмотреть информацию о лицензии и ключе в командной строке

Посмотреть информацию о лицензионных ключах и лицензии на устройстве

```
kesl-control -L --query [--json]
```

Где `--json` – выводить данные в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в консоль.

В результате выполнения команды в консоль выводится следующая информация:

- Информация об активном лицензионном ключе:
    - Дата и время окончания срока действия лицензии.
    - Количество дней до окончания срока действия лицензии.
    - Информация об ограничении функций защиты (строка отображается только для ключа, которым активировано приложение Kaspersky Endpoint Security).
    - Информация об ограничении обновления баз приложения.
    - Информация о статусе лицензионного ключа.
    - Тип лицензии, связанной с ключом.
    - Лицензионное ограничение ключа (количество единиц лицензирования).
    - Название приложения, для активации которого предназначен ключ.

    - Активный лицензионный ключ (уникальная буквенно-цифровая последовательность).
    - Дата активации.
- Информация о резервном лицензионном ключе. Отображается, если приложение используется в стандартном режиме или режиме EDR-агента и резервный ключ добавлен. Если приложение используется в режиме Легкого агента, информация о резервном ключе не отображается.
    - Дата и время окончания срока действия лицензии.
    - Информация об ограничении функций защиты (строка отображается только для ключа, которым может быть активировано приложение Kaspersky Endpoint Security).
    - Информация об ограничении обновления баз приложения.
    - Информация о статусе лицензионного ключа.
    - Тип лицензии, связанной с ключом.
    - Лицензионное ограничение ключа (количество единиц лицензирования).
    - Название приложения, для активации которого предназначен ключ.
    - Резервный лицензионный ключ (уникальная буквенно-цифровая последовательность).
    - Дата и время окончания срока действия лицензии, связанной с активным ключом.

Вы также можете получить информацию о лицензии, по которой используется приложение, при просмотре информации о работе приложения:

```
kesl-control --app-info
```

Как посмотреть информацию о лицензии и ключе в графическом интерфейсе приложения

1. Откройте главное окно графического интерфейса приложения.
2. Выполните одно из следующих действия:
    - В нижней части главного окна нажмите на область окна, в которой отображается информация о лицензии и о ключе.
    - В нижней части главного окна нажмите на кнопку **Поддержка** и в открывшемся окне **Поддержка** перейдите по ссылке в поле **Лицензионный ключ** или по ссылке **Лицензии** в нижней части окна.

    Откроется окно **Лицензии**.

    В окне отображается информация об активных и резервных ключах, добавленных в приложение. По ссылке **Подробнее** вы можете просматривать полную информацию о лицензиях и ключах.

В блоке **Действующие лицензии** отображается информация о добавленных активных ключах и связанных с ними лицензиях:

- Тип лицензии, лицензионное ограничение и срок действия лицензии.
- **Лицензионный ключ** – уникальная буквенно-цифровая последовательность.

- **Статус ключа** – статус ключа или сообщение о каких-либо проблемах, связанных с ключом (при их наличии).
- **Действует с** – дата активации приложения путем добавления этого ключа.
- **Истекает** – количество дней до истечения срока действия лицензии и дата окончания срока действия лицензии (UTC).
- **Название** – название приложения, для активации которого предназначен ключ.
- **Защита** – информация об ограничении функций защиты и функции обновления баз приложения.

В блоке **Резервные ключи** отображается информация о добавленных резервных ключах и связанных с ними лицензиях:

- Тип резервного ключа, лицензионное ограничение и срок действия лицензии, связанной с ключом.
- **Лицензионный ключ** – уникальная буквенно-цифровая последовательность.
- **Тип лицензии** – тип лицензии, связанной с резервным ключом.
- **Название** – название приложения, для активации которого предназначен ключ.
- **Защита** – информация об ограничении функций защиты и функции обновления баз приложения.

Если приложение Kaspersky Endpoint Security используется в стандартном режиме или в режиме EDR-агента и для управления приложением вы используете Kaspersky Security Center, информация о добавлении и удалении лицензионных ключей и об истечении срока действия лицензий по умолчанию записывается в журнал операционной системы.

Интерфейсы управления приложением

Для управления приложением Kaspersky Endpoint Security вы можете использовать:

- Kaspersky Security Center;
- командную строку;
- графический интерфейс приложения.

> Набор действий, которые вы можете выполнять с помощью графического интерфейса приложения Kaspersky Endpoint Security, ограничен.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, управление приложением с помощью Kaspersky Security Center Cloud Console и графического интерфейса приложения недоступно.

Если приложение используется в режиме EDR-агента, набор доступных компонентов и задач приложения ограничен. Вы можете управлять некоторыми компонентами защиты, активировать приложение и обновлять базы. Ознакомьтесь с особенностями работы в режиме EDR-агента в статье Известные проблемы и ограничения.

Выбирайте инструмент управления в зависимости от IT-инфраструктуры вашей организации, а также роли и сценария работы администратора. Мы рекомендуем управлять приложением на клиентских устройствах удаленно и централизованно с помощью Kaspersky Security Center.

Управление через Kaspersky Security Center

Kaspersky Security Center позволяет вам удаленно и централизованно управлять работой приложения Kaspersky Endpoint Security на клиентских устройствах. Вы можете удаленно устанавливать и удалять, запускать и останавливать приложение Kaspersky Endpoint Security; настраивать параметры работы приложения, отдельных компонентов и задач приложения; запускать и останавливать задачи на управляемых устройствах.

Группы администрирования Kaspersky Security Center

Чтобы управлять через Kaspersky Security Center работой приложения Kaspersky Endpoint Security, установленного на устройствах, вам нужно поместить эти устройства в *группы администрирования*. Вы можете создать группы администрирования в Kaspersky Security Center перед началом установки приложения Kaspersky Endpoint Security и настроить правила автоматического перемещения устройств в группы администрирования. Или вы можете вручную переместить устройства в группы администрирования после установки приложения (см. подробнее в справке Kaspersky Security Center).

Консоли управления и плагины управления

Для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center вы можете использовать следующие консоли управления Kaspersky Security Center:

- Консоль администрирования Kaspersky Security Center (далее также "Консоль администрирования"). Представляет собой оснастку к Microsoft Management Console (MMC), которая устанавливается на рабочее место администратора и предоставляет пользовательский интерфейс к административным службам Сервера администрирования и Агента администрирования.

  Интерфейс для управления приложением Kaspersky Endpoint Security через Консоль администрирования Kaspersky Security Center обеспечивает MMC-плагин управления Kaspersky Endpoint Security (далее также "MMC-плагин").

  MMC-плагин требуется установить на устройство с установленной Консолью администрирования Kaspersky Security Center.

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

  Интерфейс для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center Web Console обеспечивает веб-плагин управления Kaspersky Endpoint Security (далее также "веб-плагин").

  Веб-плагин требуется установить на устройство с установленным приложением Kaspersky Security Center Web Console.

- Kaspersky Security Center Cloud Console. Представляет собой облачную консоль администрирования в составе облачной версии приложения Kaspersky Security Center, которое также называется Kaspersky Security Center Cloud Console. Облачная консоль имеет интерфейс, аналогичный интерфейсу Kaspersky Security Center Web Console. Интерфейс для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center Cloud Console также обеспечивает веб-плагин.

  Управление приложением с помощью Kaspersky Security Center Cloud Console недоступно, если приложение Kaspersky Endpoint Security используется в режиме Легкого агента.

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

Политики и задачи Kaspersky Security Center

MMC-плагин и веб-плагин позволяют создавать в Kaspersky Security Center политики и задачи для управления работой приложения Kaspersky Endpoint Security:

- *Политика* – это набор параметров, который применяется на всех устройствах группы администрирования. С помощью политик вы можете устанавливать одинаковые значения параметров приложения для всех клиентских устройств, входящих в состав группы администрирования.

  Политика Kaspersky Endpoint Security определяет общие параметры работы приложения Kaspersky Endpoint Security и параметры работы отдельных функциональных компонентов приложения на устройствах, где применяется политика.

- *Задачи* для Kaspersky Endpoint Security, созданные в Kaspersky Security Center, выполняются на защищаемых устройствах и реализуют такие функции Kaspersky Endpoint Security, как проверка по требованию, активация приложения, обновление баз и модулей приложения.

  В Kaspersky Security Center вы можете создавать как задачи, которые должны выполняться на отдельном устройстве (локальные задачи), так и задачи для всех устройств группы администрирования (групповые задачи) или задачи для произвольной выборки устройств (задачи для наборов устройств).

О политиках Kaspersky Security Center

Политика – это набор параметров приложения Kaspersky Endpoint Security, которые применяются для всех клиентских устройств, входящих в состав группы администрирования. Политика имеет один из следующих статусов:

Статус политики

Статус	Описание
Активная	Это текущая политика, которая применяется к устройству.
Неактивная	Политика, которая в настоящее время не применяется к устройству.
Для автономных пользователей	Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

Политики действуют по следующим правилам:

- Для одного приложения можно настроить несколько политик с различными параметрами.
- Для одного приложения может быть активна только одна политика.
- Политика может иметь дочерние политики.

Блокировка параметров

Каждый параметр политики имеет атрибут "замок". От статуса данного атрибута зависит, будет ли параметр передан на управляемые устройства, входящие в группу администрирования.

- "Замок" закрыт ( ) – параметр применяется к устройствам, на которых применяется политика. Пользователь не может изменять значения этих параметров в интерфейсе управляемого приложения. Такие параметры называются *заблокированными*.
- "Замок" открыт ( ) – параметр не указан в политике. Пользователь может изменить эти параметры в интерфейсе управляемого приложения. Такие параметры называются *разблокированными*.

Рекомендуется заблокировать параметры политики, которые вы хотите применить к управляемым устройствам. Разблокированные параметры политики могут быть переназначены на управляемом устройстве.

Количество параметров с "замками" в Web Console и в Консоли администрирования может отличаться.

Профиль политики

Чтобы не поддерживать большое число политик, например, когда в разных случаях предполагается изменение только нескольких параметров, вы можете использовать профили политик.

Профиль политики – это отдельные параметры политики, которые отличаются от параметров "базовой" политики и применяются на клиентских устройствах при выполнении настроенных вами условий (правил активации). Использование профилей политики позволяет более гибко настроить параметры работы приложения на разных устройствах.

Параметры профиля, закрытые "замком", преобладают над параметрами политики. То есть, если параметр профиля, закрытый "замком", отличается от параметра политики, приложение применит параметр профиля. При этом параметры, представленные в виде списков, объединяются, дополняя друг друга. То есть, если параметры в списке профиля отсутствуют в "базовой" политике, то они дополнят результирующий список параметров.

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.
- Профили политики содержат значения параметров, которые отличаются от параметров политики.

- Активация профиля политики изменяет эффективные параметры управляемого устройства (параметры, которые применяются к устройству в настоящее время).

- В политике может быть не более 100 профилей.

Наследование параметров

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

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

> Если параметры дочерней политики заблокированы (ошибка *Доступ запрещен*), проверьте права доступа пользователя. Если у пользователя есть права на изменение параметров политики, вам нужно запустить задачу для Kaspersky Security Center *Загрузка обновлений в хранилище Сервера администрирования* и выполнить повторную авторизацию. Такая ошибка может возникнуть после обновления плагинов управления в Kaspersky Security Center: после загрузки обновлений приложение получает необходимые файлы для новой версии плагина управления.

Для некоторых параметров, представленных списками (например, списки правил, списки исключений), вы можете включить объединение элементов списка. Для объединения элементов списка требуется выполнить следующие действия:

- В свойствах дочерней политики на вкладке **Общие** включить параметр **Наследовать параметры родительской политики**.

- В свойствах родительской политики закрыть "замком" (🔒) список.

- В свойствах родительской политики включить объединение параметров, установив флажок **Объединять значения при наследовании**. Если флажок установлен, элементы списка родительской политики Kaspersky Security Center отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик.

Удалить или изменить унаследованные элементы списка в дочерней политике невозможно. Элементы списка, объединенные при наследовании, доступны для удаления и изменения только в родительской политике. Добавление, изменение и удаление элементов списка возможно на нижестоящих уровнях. Таким образом, вы можете настроить список в родительской политике, который будет применяться ко всем дочерним политикам, при этом вы также можете дополнить список в дочерней политике.

> Если вы в родительской политике удаляете элемент из списка, объединенного при наследовании, то в дочерних политиках этот элемент не удаляется, а остается. Чтобы удалить этот элемент из дочерних политик, нужно открыть свойства этих политик и удалить элемент вручную.

Некоторые списки не объединяются, в этом случае параметры профиля преобладают над параметрами "базовой" политики:

- исключения по процессам в компонентах Защита от файловых угроз и Анализ поведения;
- области защиты в компонентах Защита от файловых угроз и Защита от шифрования;
- области мониторинга в компоненте Контроль целостности системы;
- список правил (в окне **Правила Контроля приложений**) в компоненте Контроль приложений;
- список правил в Веб-Контроле;
- исключения памяти процессов из проверки в параметры приложения;
- доверенные домены в параметрах сети;
- доверенные корневые сертификаты в параметрах сети;
- контролируемые порты в параметрах сети;
- список адресов SVM в параметрах обнаружения SVM.

Параметры работы приложения изменяются в соответствии с параметрами политики после первого применения политики.

Подробнее о политиках и профилях политик, а также о механизме наследования параметров см. в справке Kaspersky Security Center.

Управление политиками

Как создать политику в Web Console

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

   Откроется список политик и профилей политик.

2. Выберите группу администрирования, для которой должна применяться политика. Чтобы выбрать вложенную группу, нажмите на кнопку **Показать иерархию** в верхней части окна.

3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.

4. В открывшемся окне в списке выберите название приложения Kaspersky Endpoint Security.

   Перейдите к следующему шагу мастера.

5. Укажите, в каком режиме вы используете приложение Kaspersky Endpoint Security:

- **Стандартный режим или режим Агента Endpoint Detection and Response** – приложение используется для защиты устройств под управлением операционных систем Linux как автономное приложение или как приложение, обеспечивающее совместную работу решений Detection and Response от "Лаборатории Касперского" и антивирусных решений от сторонних поставщиков.

  Для выбора этого режима перейдите к следующему шагу мастера.

- **Легкий агент для защиты виртуальных сред** – приложение используется в составе решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.

6. Если вы используете приложение в режиме Легкого агента, настройте параметры обнаружения SVM:

   a. Выберите способ, который используют Легкие агенты для обнаружения доступных для подключения SVM:

   - **Использовать Сервер интеграции**. Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них.

   - **Использовать список адресов SVM, заданный вручную**. Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.

   Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур, то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Игнорировать**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM. Подробнее см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

   b. Если вы выбрали Сервер интеграции, в окне мастера отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. Если требуется, укажите новые параметры подключения:

      a. Нажмите на кнопку **Настроить** и укажите новые параметры подключения в открывшемся окне:

      - **Адрес**. IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции. Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

      - **Порт**. Порт для подключения к Серверу интеграции. По умолчанию указан порт 7271.

      Если в вашей инфраструктуре развернут отказоустойчивый кластер Серверов интеграции на базе Linux, в качестве адреса и порта для подключения к Серверу интеграции вам нужно указать адрес и порт балансировщика нагрузки. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент.

      b. Нажмите на кнопку **Проверить**.

c. Веб-плагин проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, в окне **Настройки подключения к Серверу интеграции** отображается сообщение об этом.

Вы можете посмотреть информацию о сертификате, полученном от Сервера интеграции, нажав на строку **Посмотреть полученный сертификат**.

> При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

Чтобы сохранить полученный сертификат и продолжить подключение к Серверу интеграции, в блоке **Выбор действия** выберите вариант **Игнорировать**.

d. Укажите пароль администратора Сервера интеграции (пароль учетной записи `admin`) и нажмите на кнопку **Проверить**.

Мастер создания политики выполняет подключение к Серверу интеграции. Если установить подключение не удалось, в окне отображается сообщение об ошибке. Если подключение установлено, окно **Подключение к Серверу интеграции** закрывается, в окне мастера создания политики в поле **Подключение к Серверу интеграции** отображается статус **Установлено**.

c. Если вы выбрали список адресов SVM, заданный вручную, сформируйте список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Чтобы добавить SVM в список, нажмите на кнопку **Добавить** и в открывшемся окне укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки.

> Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения.

Вы можете удалять выбранные в списке адреса по нажатию на кнопку **Удалить**.

Перейдите к следующему шагу мастера.

7. Примите решение об использовании Kaspersky Security Network. Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

- Если вы согласны со всеми пунктами Положения и хотите использовать Kaspersky Security Network в работе приложения, выберите вариант **Я принимаю условия использования Kaspersky Security Network**.

- Если вы не хотите принимать использовать Kaspersky Security Network, выберите вариант **Я не принимаю условия использования Kaspersky Security Network** и подтвердите свое решение в открывшемся окне.

Отказ от использования Kaspersky Security Network не прерывает процесс создания политики. Вы можете в любой момент включить, выключить использование Kaspersky Security Network или изменить режим Kaspersky Security Network для управляемых устройств в параметрах политики.

Перейдите к следующему шагу мастера.

8. Вам будет предложено ознакомиться с рекомендациями по настройке Kaspersky Endpoint Security. Ознакомьтесь с настройками, позволяющими оптимизировать потребление системных ресурсов приложением.

   Перейдите к следующему шагу мастера.

9. Откроется окно параметров созданной политики на вкладке **Общие**. Укажите название новой политики.

   Вы также можете настроить следующие параметры политики:

   - Состояние политики:

     - **Активна**. Политика, которая применяется к устройству в настоящий момент. Если выбран этот вариант, при следующей синхронизации устройства с Сервером администрирования эта политика станет активной на устройстве. Этот вариант выбран по умолчанию.

     - **Неактивна**. Если выбран этот вариант, политика не применяется к устройству, но сохраняется в папке **Политики**. Позже вы можете активировать неактивную политику.

     - **Для автономных пользователей**. Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

       > В действующей на устройстве политике Агента администрирования в разделе **Сеть** → **Профили соединений** должен быть включен параметр **Включить автономный режим, когда Сервер администрирования недоступен**.

   - Наследование параметров политики:

     - **Наследовать параметры родительской политики**. Если переключатель включен, значения параметров политики наследуются из групповой политики верхнего уровня. Параметры, которые в родительской политике закрыты "замком" (🔒), недоступны для изменения. По умолчанию переключатель включен.

     - **Принудительно наследовать в дочерней политике**. 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, для которых "замок" открыт (🔓). По умолчанию переключатель выключен.

   Общая информация о параметрах политик приведена в справке Kaspersky Security Center.

10. Если вы хотите настроить другие параметры политики, перейдите на вкладку **Параметры приложения** и внесите необходимые изменения.

    Вы также можете изменить параметры политики позже.

11. Нажмите на кнопку **Сохранить**.

Как создать политику в Консоли администрирования

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, содержащую устройства, на которых должна применяться политика.

   На вкладке **Устройства** папки с названием группы администрирования вы можете просмотреть список устройств, которые входят в состав этой группы администрирования.

2. В рабочей области выберите вкладку **Политики**.

3. Нажмите на кнопку **Новая политика**, чтобы запустить мастер создания политики.

   Вы также можете запустить мастер с помощью пункта **Создать** → **Политику** контекстного меню в списке политик.

4. На первом шаге мастера в списке выберите название приложения Kaspersky Endpoint Security.

   Перейдите к следующему шагу мастера.

5. Введите название новой политики.

6. Если вы хотите перенести в создаваемую политику параметры из политики предыдущей версии приложения Kaspersky Endpoint Security, установите флажок **Использовать параметры политики для предыдущей версии программы**.

   Перейдите к следующему шагу мастера.

7. Примите решение об использовании Kaspersky Security Network. Для этого внимательно ознакомьтесь с Положением о Kaspersky Security Network, затем выполните одно из следующих действий:

   - Если вы согласны со всеми пунктами Положения и хотите использовать Kaspersky Security Network в работе приложения, выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**.

   - Если вы не хотите принимать использовать Kaspersky Security Network, выберите вариант **Я не принимаю условия Положения о Kaspersky Security Network** и подтвердите свое решение в открывшемся окне.

   Отказ от использования Kaspersky Security Network не прерывает процесс создания политики. Вы можете в любой момент включить, выключить использование Kaspersky Security Network или изменить режим Kaspersky Security Network для управляемых устройств в параметрах политики.

   Перейдите к следующему шагу мастера.

8. Укажите, в каком режиме вы используете приложение Kaspersky Endpoint Security:

   - **Стандартный режим или режим Агента Endpoint Detection and Response** – приложение используется для защиты устройств под управлением операционных систем Linux как автономное приложение или как приложение, обеспечивающее совместную работу решений Detection and Response от "Лаборатории Касперского" и антивирусных решений от сторонних поставщиков.

   - **Режим Легкого агента для защиты виртуальных сред** – приложение используется в составе решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.

   Перейдите к следующему шагу мастера.

9. Если вы используете приложение в режиме Легкого агента, настройте параметры обнаружения SVM:

   a. Выберите способ, который используют Легкие агенты для обнаружения доступных для подключения SVM:

      - **Использовать Сервер интеграции**. Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них.

      - **Использовать список адресов SVM, заданный вручную**. Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.

Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур, то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Игнорировать**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM. Подробнее см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

b. Если вы выбрали Сервер интеграции, в окне мастера отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. Если требуется, укажите новые параметры подключения:

   a. Нажмите на кнопку **Изменить** и укажите новые параметры подключения в открывшемся окне:

      - **Адрес**. IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции. Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.

      - **Порт**. Порт для подключения к Серверу интеграции. По умолчанию указан порт 7271.

      Если в вашей инфраструктуре развернут отказоустойчивый кластер Серверов интеграции на базе Linux, в качестве адреса и порта для подключения к Серверу интеграции вам нужно указать адрес и порт балансировщика нагрузки. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент.

   b. Нажмите на кнопку **OK**.

   c. Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов, для аутентификации на Сервере интеграции используется учетная запись администратора Сервера интеграции.

      В открывшемся окне введите пароль администратора Сервера интеграции (пароль учетной записи `admin`) и нажмите на кнопку **OK**.

   d. MMC-плагин проверяет SSL-сертификат, полученный от Сервера интеграции. Если сертификат содержит ошибку или не является доверенным, откроется окно **Проверка сертификата Сервера интеграции**. С помощью ссылки в окне вы можете посмотреть информацию о полученном сертификате.

      При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

      Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

c. Если вы выбрали список адресов SVM, заданный вручную, сформируйте список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Чтобы добавить SVM в список, нажмите на кнопку **Добавить** и в открывшемся окне укажите IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки.

Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения.

Вы можете удалять выбранные в списке адреса по нажатию на кнопку **Удалить**.

Перейдите к следующему шагу мастера.

10. Если требуется, настройте основные параметры Защиты от файловых угроз.

    Перейдите к следующему шагу мастера.

11. Если требуется, измените настроенные по умолчанию параметры защиты от файловых угроз.

    Перейдите к следующему шагу мастера.

12. Если требуется, настройте исключения из защиты от файловых угроз.

    Перейдите к следующему шагу мастера.

13. Если требуется, измените настроенные по умолчанию действия при обнаружении угрозы.

    Перейдите к следующему шагу мастера.

14. Выберите состояние политики:

    - **Активная политика**. Политика, которая применяется к устройству в настоящий момент. Если выбран этот вариант, при следующей синхронизации устройства с Сервером администрирования эта политика станет активной на устройстве. Этот вариант выбран умолчанию.
    - **Неактивная политика**. Если выбран этот вариант, политика не применяется к устройству но сохраняется в папке **Политики**. Позже вы можете активировать неактивную политику.
    - **Политика для автономных пользователей**. Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

    В действующей на устройстве политике Агента администрирования в разделе **Сеть** → **Профили соединений** должен быть включен параметр **Включить автономный режим, когда Сервер администрирования недоступен**.

15. Завершите работу мастера создания политики.

    Созданная политика отобразится в списке политик группы администрирования на вкладке **Политики** и в папке **Политики** дерева консоли.

Общую информацию об управлении политиками см. в справке Kaspersky Security Center.

Полезные статьи

Что делать, если не выполняются задачи или не применяются политики

Что делать, если устройство в статусе "Недопустимые параметры политики. Политика не была применена"

Ошибка "Приложение не поддерживается текущей версией Kaspersky Security Center Web Console или не установлен веб-плагин для приложения"

Экспорт и импорт параметров политики

Kaspersky Endpoint Security позволяет экспортировать политику, ее параметры и профили в файл формата KLP. Вы можете использовать функцию экспорта / импорта политики для резервного копирования политик, переноса политик на другой сервер или, например, для переноса политик из Kaspersky Security Center Windows в Kaspersky Security Center Linux. Подробнее об управлении политиками см. в справке Kaspersky Security Center.

Как экспортировать / импортировать политику в Консоли администрирования (MMC)

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите вкладку **Политики**.
4. Для экспорта политики выполните следующие действия:
   a. Выберите политику, которую вы хотите экспортировать.
   b. Нажмите на ссылку **Экспортировать политику в файл** в правой части окна.
   c. В открывшемся окне введите имя файла формата KLP, в который вы хотите экспортировать политику, а также выберите папку для сохранения файла.
   d. Сохраните файл.
5. Для импорта политики выполните следующие действия:
   a. Нажмите на кнопку **Импортировать политику из файла**.
   b. В открывшемся окне выберите KLP-файл политики, который вы хотите импортировать.
   c. Откройте файл.

   В результате будет добавлена новая политика со статусом *Неактивная политика*.

Как экспортировать / импортировать политику в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Для экспорта политики выполните следующие действия:
   a. Установите флажок рядом с политикой, которую вы хотите экспортировать.
   b. Нажмите на кнопку **Экспортировать.**

c. В открывшемся окне введите имя файла формата KLP, в который вы хотите экспортировать политику, а также выберите папку для сохранения файла.

d. Сохраните файл.

3. Для импорта политики выполните следующие действия:

a. Нажмите на кнопку **Импортировать**.

b. Выберите KLP-файл политики, который вы хотите импортировать.

c. После успешной обработки политики выберите группу администрирования, к которой вы хотите применить политику.

d. Нажмите на кнопку **Завершить**, чтобы завершить импорт политики.

В результате будет добавлена новая политика со статусом *Неактивна*.

Экспорт и импорт отдельных параметров политики в Web Console

В Web Console вы можете экспортировать и импортировать отдельные параметры политики в файл формата JSON. Например, вы можете экспортировать список правил Веб-Контроля или области защиты от файловых угроз.

Для экспорта и импорта доступны следующие параметры:

- Области защиты от файловых угроз;
- Фильтры вложений Защиты от почтовых угроз;
- Сетевые пакетные правила;
- Правила Веб-Контроля;
- Правила Контроля приложений;
- Области мониторинга и исключений Контроля целостности системы;
- Настройки телеметрии;
- Некоторые исключения из Доверенной зоны.

Чтобы экспортировать / импортировать параметры в Web Console, выполните следующие действия:

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел, параметры из которого нужно экспортировать или импортировать.

5. Нажмите на кнопку .

6. Выберите действие: **Импортировать** или **Экспортировать**.

7. Если вы выбрали импорт параметров, выберите файл, из которого вы хотите импортировать параметры.

О задачах для Kaspersky Endpoint Security, созданных в Kaspersky Security Center

Вы можете создавать в Kaspersky Security Center задачи следующих типов для приложения Kaspersky Endpoint Security:

- локальные задачи для выполнения на отдельных устройствах;
- групповые задачи для выполнения на устройствах, входящих в группу администрирования;
- задачи для выборки устройств для выполнения на нескольких устройствах, независимо от их вхождения в группы администрирования.

Вы можете создавать любое количество задач.

Общая информация о задачах, созданных в Kaspersky Security Center, приведена в справке Kaspersky Security Center.

Типы задач

Для управления приложением Kaspersky Endpoint Security в Kaspersky Security Center предусмотрены следующие задачи:

- *Поиск вредоносного ПО*. Во время выполнения задачи приложение проверяет области устройства, указанные в параметрах задачи, на вирусы и другие вредоносные программы.
- *Проверка важных областей*. Во время выполнения задачи приложение проверяет загрузочные секторы, объекты автозапуска, память процессов и память ядра.
- *Проверка контейнеров*. Во время выполнения задачи приложение проверяет контейнеры и образы на вирусы и другие вредоносные программы.
- *Инвентаризация*. Во время выполнения задачи приложение получает информацию обо всех исполняемых файлах приложений, хранящихся на устройствах, а также управляет "Золотым образом" (Golden Image).
- *Проверка целостности системы*. Во время выполнения задачи приложение определяет изменение каждого объекта путем сравнения текущего состояния контролируемого объекта с исходным состоянием, зафиксированным ранее в качестве снимка состояния системы.
- *Добавление ключа*. Во время выполнения задачи приложение добавляет ключ, в том числе резервный, для активации приложения.

- *Обновление*. Во время выполнения задачи приложение обновляет базы в соответствии с настроенными параметрами обновления.
- *Откат обновления баз*. Во время выполнения задачи приложение откатывает последнее обновление баз.

Управление задачами в Web Console

Как создать задачу для группы или выборки устройств в Web Console

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. На первом шаге мастера выполните следующие действия:

   a. В раскрывающемся списке **Приложение** выберите название приложения Kaspersky Endpoint Security.

   b. В раскрывающемся списке **Тип задачи** выберите тип задачи, которую вы хотите создать.

   c. В поле **Название задачи** введите название новой задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите способ определения области действия задачи. Область действия задачи – это устройства, на которых будет выполняться задача:

      - Выберите вариант **Назначить задачу группе администрирования**, если задача должна выполняться на всех устройствах, входящих в определенную группу администрирования.
      - Выберите вариант **Задать адреса устройств вручную или импортировать из списка**, если задача должна выполняться на указанных устройствах.
      - Выберите вариант **Назначить задачу выборке устройств**, если задача должна выполняться на устройствах, входящих в выборку устройств по предопределенному критерию. О создании выборки устройств см. в справке Kaspersky Security Center.

   Перейдите к следующему шагу мастера.

4. В зависимости от выбранного способа определения области действия задачи выполните одно из следующих действий:

   - В дереве групп администрирования установите флажки рядом с нужными группами администрирования.

   - В списке устройств установите флажки рядом с нужными устройствами. Если нужные устройства отсутствуют в списке, вы можете добавить их следующими способами:

     - С помощью кнопки **Добавить устройства**. Вы можете добавить устройства по имени или IP-адресу, добавить устройства из указанного IP-диапазона или выбрать устройства из списка устройств, обнаруженных Сервером администрирования при опросе локальной сети организации.

     - С помощью кнопки **Импортировать устройства из файла**. Для импорта используется файл формата TXT с перечнем адресов устройств, где каждый адрес должен располагаться в отдельной строке.

   - В списке выберите название выборки, содержащей нужные устройства.

   Перейдите к следующему шагу мастера.

5. Чтобы настроить параметры задачи сразу после создания, на последнем шаге мастера установите флажок **Открыть окно свойств задачи после ее создания**. Задача создается с параметрами по умолчанию.

6. Завершите работу мастера.

В списке задач отобразится новая задача.

Как создать локальную задачу в Web Console

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на кнопку **Показать иерархию**, расположенную над списком управляемых устройств, и в открывшемся окне выберите группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. В списке найдите устройство, для которого вы хотите создать задачу, и нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Задачи**.

   Откроется список задач, созданных для этого устройства.

5. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

6. На первом шаге мастера выполните следующие действия:

   a. В раскрывающемся списке **Приложение** выберите название приложения Kaspersky Endpoint Security.

   b. В раскрывающемся списке **Тип задачи** выберите тип задачи, которую вы хотите создать.

   c. В поле **Название задачи** введите название новой задачи.

7. Чтобы настроить параметры задачи сразу после создания, на последнем шаге мастера установите флажок **Открыть окно свойств задачи после ее создания**. Задача создается с параметрами по умолчанию.

8. Завершите работу мастера.

В списке задач отобразится новая задача.

Как запустить, остановить, приостановить или возобновить задачу в Web Console

1. В главном окне Kaspersky Security Center Web Console выберите **Активы (Устройства)** → **Задачи**.

   Откроется список задач.

2. Выполните одно из следующих действий:

   - Если вы хотите запустить или остановить задачу, которая выполняется на всех устройствах, входящих в определенную группу администрирования, нажмите на кнопку **Показать иерархию** в верхней части окна и в открывшемся окне выберите группу администрирования.

     В списке отобразятся только задачи, созданные для выбранной группы администрирования.

   - Если вы хотите запустить или остановить задачу, которая выполняется на одном или нескольких устройствах (задачу для набора устройств), нажмите на кнопку **Показать иерархию** в верхней части окна и в открывшемся окне выберите верхний узел с именем Сервера администрирования.

     В списке отобразятся все задачи, созданные на Сервере администрирования.

3. В списке задач установите флажок рядом с названием нужной задачи и нажмите на кнопку нужного действия над списком задач.

> Задачу *Обновление* невозможно приостановить и возобновить, ее можно только запустить или остановить.

Управление задачами в Консоли администрирования

Как создать задачу для группы или выборки устройств в Консоли администрирования

1. В Консоли администрирования выполните одно из следующих действий:

   - Если вы хотите создать задачу, которая будет выполняться на устройствах, входящих в выбранную группу администрирования, в дереве консоли в папке **Управляемые устройства** выберите эту группу администрирования, затем в рабочей области выберите вкладку **Задачи** и нажмите на кнопку **Новая задача**.

     Запустится мастер создания задачи для устройств выбранной группы администрирования.

   - Если вы хотите создать задачу, которая будет выполняться на одном или нескольких устройствах (задачу для набора устройств), в дереве консоли выберите папку **Задачи** и нажмите на кнопку **Новая задача** в рабочей области.

     Запустится мастер создания задачи для набора устройств.

2. На первом шаге мастера выберите в списке название приложения Kaspersky Endpoint Security и тип задачи.

   Перейдите к следующему шагу мастера.

3. Если вы создаете задачу для набора устройств, мастер предложит определить область действия задачи. Область действия задачи – это устройства, на которых будет выполняться задача.

   a. Укажите способ определения области действия задачи: выбрать устройства из списка устройств, обнаруженных Сервером администрирования; задать адреса устройств вручную; импортировать список устройств из файла или указать ранее настроенную выборку устройств (см. подробнее в справке Kaspersky Security Center).

   b. В зависимости от указанного вами способа определения области действия в открывшемся окне выполните одно из следующих действий:

      - В списке обнаруженных устройств укажите устройства, на которых будет выполняться задача. Для этого установите флажок в списке слева от названия устройства.
      - Нажмите на кнопку **Добавить** или **Добавить IP-диапазон** и задайте адреса устройств вручную.
      - Нажмите на кнопку **Импортировать** и в открывшемся окне выберите файл формата TXT, содержащий перечень адресов устройств.
      - Нажмите на кнопку **Обзор** и в открывшемся окне укажите название выборки, содержащей устройства, на которых будет выполняться задача.

   Перейдите к следующему шагу мастера.

4. Настройте доступные параметры задачи, следуя указаниям мастера.

5. Введите название новой задачи и перейдите к следующему шагу мастера.

6. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера, на последнем шаге установите флажок **Запустить задачу после завершения работы мастера**.

7. Завершите работу мастера.

   В списке задач отобразится новая задача.

Как создать локальную задачу в Консоли администрирования

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.

2. В рабочей области выберите вкладку **Устройства**.

3. В списке управляемых устройств выберите нужное вам устройство и откройте окно **Свойства: <Имя устройства>** двойным щелчком мыши.

4. В открывшемся окне свойств управляемого устройства выберите раздел **Задачи**.

   Откроется список задач, созданных для этого устройства.

5. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

6. На первом шаге мастера выберите название приложения Kaspersky Endpoint Security и тип задачи.

   Перейдите к следующему шагу мастера.

7. Введите название новой задачи и настройте доступные параметры задачи, следуя указаниям мастера.

8. Завершите работу мастера.

   В списке задач отобразится новая задача.

Как запустить, остановить, приостановить или возобновить задачу в Консоли администрирования

1. В Консоли администрирования выполните одно из следующих действий:

   - Если вы хотите запустить или остановить задачу, которая выполняется на устройствах, входящих в определенную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите вкладку **Задачи**.

     Откроется список задач, созданных для выбранной группы администрирования.

   - Если вы хотите запустить или остановить задачу, которая выполняется на одном или нескольких устройствах (задачу для набора устройств), в дереве консоли выберите папку **Задачи**.

     Откроется список всех задач, созданных на Сервере администрирования.

2. В списке задач выберите нужную задачу, откройте контекстное меню задачи и выберите действие, которое вы хотите выполнить.

   > Задачу *Обновление* невозможно приостановить и возобновить, ее можно только запустить или остановить.

В списке задач вы можете следить за выполнением задачи: просматривать статус задачи и статистику выполнения задачи на устройствах. Также вы можете создать выборку событий для контроля за выполнением задач. Дополнительная информация о выборке событий приведена в справке Kaspersky Security Center.

Результаты выполнения задач также сохраняются локально на устройстве и в отчетах Kaspersky Security Center.

Особенности управления и выполнения задач

- Задача для наборов устройств выполняется только на устройствах, указанных в задаче. Если в набор устройств, для которого сформирована задача, добавить новые устройства, то для них эта задача не будет выполняется. В этом случае вам нужно создать новую задачу или изменить уже существующую задачу.

- Задачи выполняются, только если на устройствах запущено приложение Kaspersky Endpoint Security.

- Если устройство находится под управлением политики, просмотр и управление задачами, созданными в Kaspersky Security Center, могут быть недоступны через командную строку или графический интерфейс приложения.

- Для приложения Kaspersky Endpoint Security в Kaspersky Security Center вы можете создавать задачи всех типов. Применение и выполнение задач на защищаемом устройстве определяется режимом использования приложения на этом устройстве. Например, задачи *Добавление ключа*, *Обновление* и *Откат обновления баз* не применяются на устройстве, если приложение используется в режиме Легкого агента.

Вход и выход из Web Console и Cloud Console

Kaspersky Security Center Web Console

Для входа в Web Console вам нужно знать веб-адрес Сервера администрирования и номер порта, указанные во время установки Web Console (по умолчанию используется порт 8080). Также требуется включить JavaScript в браузере.

Вы можете войти в Kaspersky Security Center Web Console следующими способами:

- С помощью доменной аутентификации (единый вход).

- Указав имя пользователя и пароль доменного пользователя.

- Указав имя пользователя и пароль внутреннего пользователя

Подробнее о входе и выходе из Kaspersky Security Center Web Console см. в справке Kaspersky Security Center.

Чтобы войти в Web Console, указав имя учетной записи и пароль:

1. В браузере перейдите по адресу:

   ```
   https://<Kaspersky Security Center Web Console address>:<port number>
   ```

   Откроется страница выбора Сервера администрирования..

2. Если вы добавили несколько доверенных серверов администрирования, в списке выберите Сервер администрирования, к которому вы хотите подключиться.

   Если вы добавили только один Сервер администрирования, список Серверов администрирования не отображается.

   Браузер перенаправляется на `https://< адрес Сервера администрирования>: 4444`.

3. Введите имя пользователя и пароль вашей учетной записи.

   Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев.

4. Нажмите на кнопку **Войти**.

   Если Сервер администрирования не отвечает или вы указали неверные учетные данные, отобразится сообщение об ошибке.

5. Введите одноразовый код безопасности, сгенерированный в приложении для аутентификации на мобильном устройстве.

   При первом входе настройте двухэтапную аутентификацию для своей учетной записи.

После входа отобразится панель мониторинга (dashboard) с последними использованными языком и темой.

Подробнее об интерфейсе Web Console см. в справке Kaspersky Security Center.

Чтобы выйти из Web Console:

в левом нижнем углу экрана выберите **<Имя учетной записи>** → **Выход**.

Web Console закроется и отобразится страница входа.

Kaspersky Security Center Cloud Console

Для Kaspersky Security Center Cloud Console используйте веб-токен для входа в учетную запись на портале Cloud Console.

Подробная информация о Kaspersky Security Center Cloud Console приведена в документации Kaspersky Security Center Cloud Console.

Управление через командную строку

С помощью командной строки вы можете устанавливать и удалять, запускать и останавливать приложение Kaspersky Endpoint Security на устройстве, а также локально управлять работой приложения.

Компоненты и задачи

Работу функциональных компонентов приложения обеспечивают *локальные задачи Kaspersky Endpoint Security*, которые выполняются в операционной системе. Чтобы включить или выключить функциональный компонент приложения на устройстве, вы запускаете или останавливаете соответствующую задачу Kaspersky Endpoint Security в командной строке.

Для однократной проверки устройства вы также запускаете соответствующую задачу Kaspersky Endpoint Security.

Чтобы задать параметры работы функционального компонента на устройстве или параметры проверки устройства, вы настраиваете параметры соответствующей задачи Kaspersky Endpoint Security.

Общие параметры

Помимо параметров отдельных задач Kaspersky Endpoint Security предусмотрены общие параметры:

- Общие параметры проверки контейнеров. Используются при проверке контейнеров и пространств имен в режиме реального времени (Мониторинг контейнеров).
- Параметры проверки сетевого трафика. Используются в работе компонентов Защита от веб-угроз, Защита от сетевых угроз, Защита от почтовых угроз и Веб-Контроль.
- Общие параметры приложения. Определяют работу приложения в целом и работу отдельных функций.

Команды управления

Управление задачами и параметрами приложения Kaspersky Endpoint Security в командной строке выполняется с помощью *утилиты kesl-control*.

Создавать и удалять можно только пользовательские задачи. Предустановленные задачи недоступны для создания и удаления.

В зависимости от режима использования приложения можно создавать пользовательские задачи следующих типов:

- стандартный режим: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* и *InventoryScan*;
- режим Легкого агента: *ODS*, *ODFIM*, *ContainerScan* и *InventoryScan*.

Можно запускать и останавливать все предустановленные и пользовательские задачи, кроме задачи типа *License*.

Можно приостановить и возобновить только задачи типов *ODS*, *ODFIM* и *InventoryScan*.

Локальные задачи Kaspersky Endpoint Security

Для управления приложением Kaspersky Endpoint Security с помощью командной строки предусмотрены задачи, перечисленные в таблице ниже.

Каждая задача приложения имеет имя, используемое в командной строке, идентификатор и тип.

Идентификаторы уникальны для всех задач, включая удаленные. Приложение не использует повторно идентификаторы удаленных задач. Идентификатор новой задачи представляет собой номер, следующий по порядку за идентификатором последней созданной задачи.

Имена задач не чувствительны к регистру.

Во время установки приложения создаются *предустановленные задачи*. Эти задачи недоступны для удаления. Для каждой предустановленной задачи зарезервированы имя и идентификатор.

Задачи, которые вы создаете во время работы с приложением, называются *пользовательские задачи*. Имена этих задач вы задаете при создании задачи. Идентификаторы пользовательских задач приложение задает и присваивает задаче при ее создании. Идентификаторы пользовательских задач начинаются со 100.

Во время работы приложение создает *временные задачи проверки*. Имена и идентификаторы временных задач задаются приложением. Временные задачи автоматически удаляются после завершения.

Задачи приложения

Задача	Описание задачи	Имя задачи в командной строке	ID задачи	Тип задачи
Защита от файловых угроз	Эта задача позволяет включать и выключать защиту от файловых угроз в реальном времени и определяет параметры компонента Защита от файловых угроз. Если включена Защита от файловых угроз, задача запускается автоматически при старте приложения	File_Threat_Protection	1	OAS
Поиск вредоносного ПО	Эта задача позволяет выполнять проверку объектов файловой системы на наличие вредоносного ПО по требованию и определяет параметры проверки. Вы можете использовать эту задачу для полной или выборочной проверки устройства.	Scan_My_Computer	2	ODS
Поиск вредоносного ПО (пользовательская)		задается пользователем	от 100	ODS
Выборочная проверка файлов	Эта задача предназначена для настройки и хранения параметров, которые используются во время проверки указанных файлов и директорий по команде `kesl-control --scan-file`. В результате выполнения команды приложение создает и запускает временную задачу проверки файлов.	Scan_File	3	ODS
Проверка важных областей	Эта задача позволяет выполнять проверку важных областей операционной системы по требованию и определяет параметры проверки.	Critical_Areas_Scan	4	ODS
Обновление	С помощью этой задачи вы можете выполнять обновление баз и модулей приложения по расписанию и по требованию и настраивать параметры обновления.	Update	6	Update
Обновление (пользовательская)		задается пользователем	от 100	Update
Откат обновления баз	С помощью этой задачи вы можете выполнять откат последнего обновления баз и модулей приложения.	Rollback	7	Rollback
Откат обновления баз (пользовательская)		задается пользователем	от 100	Rollback
Лицензирование	Эта задача обеспечивает возможность активировать приложение, установленное на устройстве. Задача запускается автоматически при запуске приложения и постоянно находится в оперативной памяти устройства. Задача не имеет параметров, управление лицензионными ключами реализовано с помощью специальных команд управления. Задача недоступна для запуска, остановки и удаления.	License	9	License
Проверка целостности системы	Эта задача позволяет проверять наличие изменений в файлах и директориях, которые вы включили в область мониторинга, путем сравнения текущего состояния контролируемого объекта с ранее зафиксированным состоянием.	System_Integrity_Monitoring	11	OAFIM
Проверка целостности системы (пользовательская)		задается пользователем	от 100	ODFIM
Управление сетевым экраном	Эта задача позволяет включать и выключать управление сетевым экраном и определяет параметры контроля сетевых соединений на устройстве.	Firewall_Management	12	Firewall

Задача	Описание задачи	Имя задачи в командной строке	ID задачи	Тип задачи
Защита от шифрования	Эта задача позволяет включать и выключать защиту файлов от удаленного вредоносного шифрования и определяет параметры компонента Защита от шифрования.	Anti_Cryptor	13	AntiCryptor
Защита от веб-угроз	Эта задача позволяет включать и выключать защиту от веб-угроз и определяет параметры работы компонента Защита от веб-угроз. Если включена Защита от веб-угроз, задача запускается автоматически при старте приложения.	Web_Threat_Protection	14	WTP
Контроль устройств	Эта задача позволяет включать и выключать Контроль устройств и определяет параметры компонента Контроль устройств. Если включен Контроль устройств, задача запускается автоматически при старте приложения.	Device_Control	15	DeviceControl
Проверка съемных дисков	Эта задача позволяет в реальном времени контролировать подключение съемных дисков к устройству и определяет параметры проверки съемных дисков и их загрузочных секторов на наличие вредоносного ПО.	Removable_Drives_Scan	16	RDS
Защита от сетевых угроз	Эта задача позволяет включать и выключать защиту от сетевых угроз и определяет параметры работы компонента Защита от сетевых угроз.	Network_Threat_Protection	17	NTP
Проверка контейнеров	Эта задача позволяет выполнять проверку контейнеров и образов по требованию и определяет параметры проверки.	Container_Scan	18	ContainerScan
Проверка контейнеров (пользовательская)		задается пользователем	от 100	ContainerScan
Выборочная проверка контейнеров	Эта задача предназначена для настройки и хранения параметров, которые используются во время проверки указанных контейнеров и образов по команде `kesl-control [-T] --scan-container`. В результате выполнения команды приложение создает и запускает временную задачу проверки контейнеров.	Custom_Container_Scan	19	ContainerScan
Анализ поведения	Эта задача позволяет контролировать вредоносную активность приложений в операционной системе. Если включен Анализ поведения, задача запускается автоматически при старте приложения.	Behavior_Detection	20	BehaviorDetection
Контроль приложений	Эта задача позволяет включать и выключать Контроль приложений и определяет параметры компонента Контроль приложений.	Application_Control	21	AppControl
Инвентаризация	Эта задача позволяет получать информацию обо всех исполняемых файлах приложений, хранящихся на устройстве, а также управлять категорией приложений "Золотой образ" (Golden Image).	Inventory_Scan	22	InventoryScan
Инвентаризация (пользовательская)		задается пользователем	от 100	InventoryScan
Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)	Эта задача позволяет включать и выключать интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises) или с Kaspersky Endpoint Detection and Response (KATA) и определяет параметры интеграции.	KATAEDR	24	KATAEDR

Задача	Описание задачи	Имя задачи в командной строке	ID задачи	Тип задачи
Веб-Контроль	Эта задача позволяет включать и выключать Веб-Контроль и определяет параметры компонента Веб-Контроль.	Web_Control	26	WebControl
Интеграция с Sandbox	Эта задача позволяет включать и выключать интеграцию с Sandbox и определяет параметры интеграции.	Standalone_Sandbox	29	StandaloneSandbox
Запрет запуска объектов (EDR Expert (on-premises))	Эта задача позволяет включать и выключать использование правил запрета запуска объектов компонента Endpoint Detection and Response Expert (on-premises) и просматривать список этих правил.	KATAEDR_Prevention	30	KATAEDRPrevention
Интеграция с Kaspersky Network Detection and Response (KATA)	Эта задача позволяет включать и выключать интеграцию с Kaspersky Network Detection and Response (KATA) и определяет параметры интеграции.	KATANDR	31	KATANDR
Запрет запуска объектов (EDR Optimum)	Эта задача позволяет включать и выключать использование правил запрета запуска объектов компонента Endpoint Detection and Response Optimum и просматривать список этих правил.	EDRO_Prevention	32	Prevention
Интеграция с KUMA	Эта задача позволяет включать и выключать интеграцию с Kaspersky Unified Monitoring and Analysis Platform и определяет параметры интеграции.	KUMA	33	KUMA
Защита от почтовых угроз	Эта задача позволяет проверять вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других приложений, представляющих угрозу. Если включена Защита от почтовых угроз, задача запускается автоматически при старте приложения.	Mail_Monitoring	35	MailMonitoring
Защита от атак BadUSB	Эта задача позволяет предотвратить подключение к устройству зараженных USB-устройств, имитирующих клавиатуру.	Bad_USB	37	BadUSB
Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud)	Эта задача позволяет включать и выключать интеграцию с Kaspersky Endpoint Detection and Response Expert (cloud) и определяет параметры интеграции.	EDRExpertCloud	39	EDRExpertCloud

Изменение параметров задач

Можно изменять параметры всех пользовательских задач и всех предустановленных задач, кроме задач типов *Rollback* и *License* (эти задачи не имеют параметров). Если приложение используется в режиме Легкого агента, параметры предустановленной задачи типа *Update* также недоступны для изменения.

Для задач типа *OAS*, *ODS*, *OAFIM*, *ODFIM* и *AntiCryptor* можно добавлять и удалять области проверки и области исключения.

Вы можете изменять параметры задач следующими способами:

- Используя конфигурационный файл. Этот способ позволяет изменять сразу все параметры задачи. Конфигурационный файл вы можете получить с помощью команды вывода параметров задачи.

- Используя ключи командной строки в формате <имя параметра>=<значение параметра>. Этот способ позволяет изменять отдельные параметры задачи. Текущие значения параметров задачи вы можете посмотреть с помощью команды вывода параметров задачи.

Для некоторых задач также предусмотрены отдельные команды управления, которые позволяют изменять параметры задач.

Как вывести текущие значения параметров задачи

Вы можете выводить текущие значения параметров задачи в консоль или в конфигурационный файл. Этот файл затем можно использовать для изменения параметров задачи.

```
Вывести в консоль текущие значения параметров задачи

kesl-control --get-settings <task ID|name>
```

Где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

```
Вывести в конфигурационный файл текущие значения параметров задачи

kesl-control --get-settings <task ID/name> --file <path to configuration file> [--json]
```

Где:

- `--file <path to configuration file>` – путь к конфигурационному файлу, в который будут выведены параметры задачи. Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанной директории не существует, конфигурационный файл не будет создан.

- `--json` – выводить параметры в файл формата JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Как изменить параметры задачи с помощью конфигурационного файла

1. Выведите параметры задачи в конфигурационный файл с помощью команды:

   ```
   kesl-control --get-settings --file <path to configuration file> [--json]
   ```

   где:

   - `--file <path to configuration file>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры задачи.

   - `--json` – укажите этот ключ, если вы хотите вывести параметры в конфигурационный файл формата JSON. Если вы не укажете ключ `--json`, приложение выведет параметры в файла формата INI.

2. Откройте конфигурационный файл, измените значения нужных параметров и сохраните изменения.

   Для задач типа *OAS*, *ODS*, *OAFIM*, *ODFIM* и *AntiCryptor* вы можете добавлять или удалять области проверки и области исключения.

Если вы хотите добавить область проверки, добавьте в файл секцию `[ScanScope.item_#]` со следующими параметрами:

- `AreaDesc` – описание области проверки, содержащее дополнительную информацию об этой области.
- `UseScanArea` – включить проверку указанной области.
- `Path` – путь к директории с проверяемыми объектами. Вы можете указывать путь к локальной директории или включать проверку удаленных директорий, смонтированных на клиентском устройстве.
- `AreaMask.item_#` – ограничение области проверки. Вы можете указать маску имени файлов, которые нужно проверять. По умолчанию проверка включена для всех объектов области проверки. Вы можете указать несколько элементов `AreaMask.item_#`.

Если вы хотите добавить область исключения, добавьте в файл секцию `[ExcludedFromScanScope.item_#]` со следующими параметрами:

- `AreaDesc` – описание области исключения, содержащее дополнительную информацию об области исключения.
- `UseScanArea` – включить исключение указанной области.
- `Path` – путь к директории с исключаемыми объектами. Вы можете указывать путь к локальной директории или исключать удаленные директории, смонтированные на клиентском устройстве. Возможные значения параметра зависят от типа задачи.
- `AreaMask.item_#` – ограничение области исключения. Вы можете указать маску имени файлов, которые вы хотите исключить из области проверки. По умолчанию исключаются все объекты области.

Пример

```
[ExcludedFromScanScope.item_0000]
AreaDesc=
UseScanArea=Yes
Path=/tmp/notchecked
AreaMask.item_0000=*
```

Вы можете указать несколько секций `[ScanScope.item_#]` и `[ExcludedFromScanScope.item_#]`. Приложение будет обрабатывать области по индексу в порядке возрастания.

3. Выполните команду:

```
kesl-control --set-settings <task ID/name> --file <path to configuration file> [--json]
```

где:

- `<task ID/name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--file <path to configuration file>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры задачи.
- `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Все значения параметров задачи, заданные в файле, будут импортированы в приложение.

Если в параметрах задачи Контроль приложений вы меняете разрешающий список или запрещаете запуск всех приложений и/или приложений, влияющих на работу приложения Kaspersky Endpoint Security, требуется запускать команду `--set-settings` с ключом `--accept`.

Как изменить отдельные параметры задачи с помощью ключей командной строки

Выполните команду:

```
kesl-control --set-settings <task ID|name> <setting name >=<setting value> [<setting name >=<setting value>]
```

Где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `<setting name >=<setting value>` – имя и значение одного из параметров задачи. Текущие значения параметров задачи вы можете получить с помощью команды вывода параметров задачи.

Значения указанных параметров задачи будут изменены.

Если в параметрах задачи Контроль приложений вы меняете разрешающий список или запрещаете запуск всех приложений и/или приложений, влияющих на работу приложения Kaspersky Endpoint Security, требуется запускать команду `--set-settings` с ключом `--accept`.

Как добавить или удалить область проверки с помощью ключей командной строки

```
Добавить область проверки с помощью ключей командной строки
kesl-control --set-settings <task ID|name> --add-path <path>
```

Где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `<path>` – путь к директории с проверяемыми объектами.

В результате выполнения команды в параметры задачи будет добавлена новая секция `[ScanScope.item_#]`. Приложение будет проверять объекты в директории, указанной параметром `Path`. Остальные параметры области проверки принимают значения по умолчанию.

Если в параметрах задачи уже есть секция `[ScanScope.item_#]` с указанным значением параметра `Path`, дублирующая секция не добавляется.

Если для параметра `UseScanArea` установлено значение `No`, после выполнения этой команды значение изменится на `Yes` и будет выполняться проверка объектов, расположенных в этой директории.

```
Пример добавления директории /home в область проверки для задачи с ID=100
kesl-control --set-settings 100 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/home
```

В задачу будут добавлены следующие параметры области проверки:

```
[ScanScope.item_0001]
AreaDesc=
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

Удалить область проверки с помощью ключей командной строки

```
kesl-control --set-settings <task ID|name> --del-path <path>
```

В результате выполнения команды из параметров задачи будет удалена секция `[ScanScope.item_#]`, содержащая указанный путь. Приложение не будет проверять объекты в указанной директории.

Как добавить или удалить область исключения с помощью ключей командной строки

Добавить область исключения с помощью ключей командной строки

```
kesl-control --set-settings <task ID|name> --add-exclusion <path>
```

Где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `<path>` – путь к директории с исключаемыми объектами.

В результате выполнения команды в параметры задачи будет добавлена новая секция `[ExcludedFromScanScope.item_#]`. Приложение будет исключать из проверки объекты в директории, указанной параметром `Path`. Остальные параметры области исключения принимают значения по умолчанию.

Если в параметрах задачи уже есть секция `[ExcludedFromScanScope.item_#]` с указанным значением параметра `Path`, дублирующая секция не добавляется.

Если для параметра `UseScanArea` установлено значение `No`, после выполнения этой команды значение изменится на `Yes` и объекты, расположенные в этой директории, будут исключаться из проверки.

Удалить область исключения с помощью ключей командной строки

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

В результате выполнения команды из параметров задачи будет удалена секция `[ExcludedFromScanScope.item_#]`, содержащая указанный путь. Приложение не будет исключать из проверки объекты в указанной директории.

Как восстановить заданные по умолчанию параметры задачи

Выполните команду:

```
kesl-control --set-settings <task ID|name> --set-to-default
```

Где `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Приложение изменит значения параметров на заданные по умолчанию.

Настройка расписания запуска задач

В зависимости от режима использования приложения можно настраивать расписание запуска задач следующих типов:

- стандартный режим: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* и *InventoryScan*;
- режим Легкого агента: *ODS*, *ODFIM*, *ContainerScan* и *InventoryScan*.

Вы можете настраивать расписание запуска задач следующими способами:

- Используя конфигурационный файл. Этот способ позволяет изменять сразу все параметры расписания запуска задачи. Конфигурационный файл вы можете получить с помощью команды вывода параметров расписания.
- Используя ключи командной строки в формате <имя параметра>=<значение параметра>. Этот способ позволяет изменять отдельные параметры расписания запуска задачи. Текущие значения параметров задачи вы можете посмотреть с помощью команды вывода параметров расписания.

Как вывести текущие параметры расписания

Вы можете выводить текущие значения параметров расписания запуска задачи в консоль или в конфигурационный файл. Этот файл затем можно использовать для изменения параметров расписания.

Вывести в консоль текущие параметры расписания запуска задачи

```
kesl-control --get-schedule <task ID|name> [--json]
```

Где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ --json, параметры будут выведены в формате INI.

Вывести в конфигурационный файл текущие параметры расписания запуска задачи

```
kesl-control --get-schedule <task ID|name> --file <path to configuration file> [--json]
```

Где `--file <path to configuration file>` – путь к конфигурационному файлу, в который будут выведены параметры расписания задачи. Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанной директории не существует, конфигурационный файл не будет создан.

Пример вывода параметров расписания задачи обновления в файл с именем update_schedule.ini и сохранения созданного файла в текущей директории

```
kesl-control --get-schedule 6 --file update_schedule.ini
```

Пример вывода в консоль расписания задачи обновления

```
kesl-control --get-schedule 6
```

Как настроить расписание запуска задачи с помощью конфигурационного файла

```
kesl-control --set-schedule <task ID|name> --file <path to configuration file> [--json]
```

Где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--file <path to configuration file>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры расписания задачи.
- `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Пример импорта в задачу с ID=2 параметров расписания из конфигурационного файла /home/test/on_demand_schedule.ini

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

Как изменить параметры расписания запуска задачи с помощью ключей командной строки

```
kesl-control --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

Где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `<setting name>=<setting value>` – имя и значение одного из параметров расписания задач.

Пример настройки запуска задачи каждые 10 часов

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2021/May/30 23:05:00;10
RandomInterval=0
```

Пример настройки запуска задачи каждые 10 минут

```
RuleType=Minutely
RunMissedStartRules=No
StartTime=23:10:00;10
RandomInterval=0
```

Пример настройки запуска задачи 15-го числа каждого месяца

```
RuleType=Monthly
RunMissedStartRules=No
StartTime=23:25:00;15
RandomInterval=0
```

Пример настройки запуска задачи каждый вторник

```
RuleType=Weekly
StartTime=18:01:30;Tue
```

```
RandomInterval=99
RunMissedStartRules=No
```

Пример настройки запуска задачи через каждые 11 дней

```
RuleType=Daily
RunMissedStartRules=No
StartTime=23:15:00;11
RandomInterval=0
```

Управление общими параметрами приложения

Общие параметры приложения определяют работу приложения в целом и работу отдельных функций. С помощью общих параметров вы можете:

- Настраивать использование Kaspersky Security Network и облегченной версии баз вредоносного ПО в работе приложения.
- Настраивать использование прокси-сервера в работе приложения.
- Выбирать режим перехвата файловых операций (блокировать / не блокировать файлы во время проверки).
- Настраивать исключения из проверки точек монтирования (глобальные исключения).
- Настраивать исключения из проверки памяти процессов.
- Включать и выключать мониторинг контейнеров в реальном времени.
- Включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.
- Включать и выключать интеграцию с Kaspersky Managed Detection and Response.
- Настраивать использование журналов событий.
- Настраивать ограничение на использование ресурсов процессора для задач проверки (типа ODS).
- Ограничивать количество задач выборочной проверки, которые может одновременно запустить непривилегированный пользователь.

Вы можете изменять общие параметры приложения с помощью специальных команд управления следующими способами:

- Используя конфигурационный файл. Этот способ позволяет изменять сразу все общие параметры. Конфигурационный файл вы можете получить с помощью команды вывода общих параметров.
- Используя ключи командной строки в формате <имя параметра>=<значение параметра>. Этот способ позволяет изменять отдельные параметры. Текущие значения параметров вы можете посмотреть с помощью команды вывода общих параметров.

Как вывести текущие значения общих параметров приложения

Вы можете выводить текущие значения общих параметров приложения в консоль или в конфигурационный файл. Этот файл можно использовать для изменения параметров приложения.

Вывести в консоль текущие значения общих параметров приложения

```
kesl-control --get-app-settings [--json]
```

Где `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Вывести в конфигурационный файл текущие значения общих параметров приложения

```
kesl-control --get-app-settings --file <path to configuration file> [--json]
```

Где `--file <path to configuration file>` – путь к конфигурационному файлу, в который будут выведены общие параметры приложения. Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанной директории не существует, конфигурационный файл не будет создан.

Пример вывода общих параметров приложения в файл kesl_config.ini с сохранением созданного файла в текущей директории

```
kesl-control --get-app-settings --file kesl_config.ini
```

Как изменить общие параметры с помощью конфигурационного файла

1. Выведите общие параметры приложения в конфигурационный файл с помощью команды `kesl-control --get-app-settings`.

2. Откройте конфигурационный файл, измените значения нужных параметров и сохраните изменения.

3. Выполните команду:

   ```
   kesl-control --set-app-settings --file <path to configuration file> [--json]
   ```

   где:

   - `--file <path to configuration file>` – полный путь к конфигурационному файлу с общими параметрами приложения. Если вы удалите какой-либо параметр в конфигурационном файле, после выполнения команды для этого параметра будет указано значение по умолчанию.

   - `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

   Все значения общих параметров, заданные в файле, будут импортированы в приложение.

Пример импорта в приложение общих параметров из конфигурационного файла /home/test/kesl_config.ini

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

Как изменить общие параметры с помощью ключей командной строки

Изменить общие параметры с помощью ключей командной строки

```
kesl-control --set-app-settings <setting name>=<setting value> [<setting name >=<setting value>]
```

Где `<setting name>=<setting value>` – имя и значение одного из общих параметров приложения.

Значения указанных общих параметров будут изменены.

Пример установки низкого уровня детализации файла трассировки

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

Пример добавления исключения точки монтирования из перехвата файловых операций

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

Использование фильтра для ограничения результатов запросов

Фильтр позволяет ограничивать результаты запроса при выполнении команд управления приложением. Условия фильтра задаются с помощью одного или нескольких *логических выражений*, скомбинированных с помощью логического оператора `and`. Условия фильтра требуется заключать в кавычки.

Вы можете использовать фильтр для решения следующих задач:

Вывести информацию об определенных текущих событиях приложения

```
kesl-control -W --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Вывести информацию об определенных событиях приложения в журнале событий

```
kesl-control -E --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Вывести информацию об определенных объектах в резервном хранилище

```
kesl-control -B --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Удалить определенные объекты из резервного хранилища

```
kesl-control -B --mass-remove --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator>
'<value>']"
```

Где:

- `<field>` – название поля базы данных.
- `<comparison operator>` – одна из следующих операций сравнения:
  - `>` – больше.
  - `<` – меньше.
  - `like` – соответствует указанному значению. При указании значения можно использовать маски %, например: логическое выражение `"FileName like '%etc%'"` задает ограничение "содержит текст "etc" в поле FileName".

    > Операция сравнения `like` работает только с полями, которые хранятся в базе данных как текст. Операция `like` не подходит для полей с датами, временем, числами или другими типами данных, отличными от текста.

- `==` – равно.
- `!=` – не равно.
- `>=` – больше или равно.
- `<=` – меньше или равно.

- `<value>` – значение поля. Значение требуется указывать в одинарных кавычках (').

  Значение даты вы можете указывать в системе отметок времени UNIX™ (количество секунд, прошедших с 00:00:00 (UTC), 1 января 1970 года) или в формате YYYY-MM-DD hh:mm:ss. Значение даты и времени указывается пользователем и отображается приложением по локальному времени пользователя.

Пример вывода информации о событиях, которые содержат текст "etc" в поле FileName

```
kesl-control -E --query "FileName like '%etc%'"
```

Пример вывода информации о событиях с типом ThreatDetected (обнаружена угроза)

```
kesl-control -E --query "EventType == 'ThreatDetected'"
```

Пример вывода информации о событиях с типом ThreatDetected, сформированных задачами типа ODS

```
kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
```

Пример вывода информации о событиях, сформированных после даты, указанной в системе отметок времени UNIX (количество секунд, прошедших с 00:00:00 (UTC), 1 января 1970 года)

```
kesl-control -E --query "Date > '1583425000'"
```

Пример вывода информации о событиях, сформированных после даты, указанной в формате YYYY-MM-DD hh:mm:ss

```
kesl-control -E --query "Date > '2022-12-22 18:52:45'"
```

Пример вывода информации о файлах в резервном хранилище, имеющих высокий (High) уровень важности

```
kesl-control -B --query "DangerLevel == 'High'"
```

Экспорт и импорт параметров приложения

Kaspersky Endpoint Security позволяет импортировать и экспортировать все параметры приложения для диагностики сбоев, проверки параметров или для упрощения настройки приложения на устройствах пользователей.

Предоставляйте доступ к конфигурационному файлу только доверенным пользователям. Перед импортом параметров в приложение проверяйте пути к каталогам, файлам настроек, исполняемым файлам, карантину. Не импортируйте конфигурационный файл из недоверенных источников. Компрометация конфигурационного файла может оказать влияние на безопасность, целостность или работоспособность инфраструктуры вашей организации, а также пользовательских данных.

Экспорт параметров

При экспорте параметров все параметры приложения (включая общие параметры проверки контейнеров, параметры проверки сетевого трафика, общие параметры приложения и параметры задач) сохраняются в конфигурационном файле. Вы можете использовать этот конфигурационный файл, чтобы затем импортировать параметры в приложение.

Экспортировать параметры приложения

```
kesl-control --export-settings --file <configuration file path> [--json]
```

Где:

- `--file <configuration file path>` – полный путь к конфигурационному файлу, в который будут сохранены параметры приложения.
- `--json` – экспортировать параметры в конфигурационный файл формата JSON. Если вы не укажете ключ `--json`, экспорт будет выполнен в файл формата INI.

Импорт параметров

1. Выполните команду:

   ```
   kesl-control --import-settings --file <configuration file path> [--json]
   ```

   Где:

   - `--file <configuration file path>` – полный путь к конфигурационному файлу, параметры из которого будут импортированы в приложение.
   - `--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

2. Перезапустите приложение.

Особенности и ограничения экспорта и импорта параметров

- Во время импорта или экспорта параметров приложение должно быть запущено.
- Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, для экспорта и импорта недоступны параметры предустановленной задачи типа `Update`.
- Если изменение параметров запрещено политикой, то импорт параметров недоступен.

- Если вы импортируете в более новую версию приложения параметры, экспортированные из более старой версии приложения, то для параметров, которые отсутствовали в старой версии, устанавливаются значения по умолчанию.
- Импортировать параметры в более старую версию приложения невозможно.
- Импортировать некоторые параметры политики и задач из веб-плагина приложения версий 12.3 и 12.4 в приложение версии 12.5 невозможно. Ограничение распространяется на следующие параметры политик и задач:
  - область защиты и область исключений Защиты от файловых угроз, Защиты от шифрования;
  - исключение из проверки процессов для Анализа поведения;
  - доверенные устройства для Контроля устройств;
  - область проверки и область исключений Контроля целостности системы;
  - правила Веб-Контроля;
  - параметры прокси-сервера;
  - исключение из проверки памяти процессов;
  - глобальные исключения (исключенные из проверки точки монтирования);
  - область проверки задач типов *ODS, ContainerScan*, *InventoryScan*, *ODFIM*.
- После импорта параметров выключается использование Kaspersky Security Network (`UseKSN=No`), использование облачного режима (`CloudMode=No`) и интеграция с MDR (`UseMDR=No`). Настройте параметры, если вы хотите использовать эту функциональность.
- После импорта параметров приложения внутренние идентификаторы задач могут измениться. Для управления задачами рекомендуется использовать имена задач.
- При интеграции с Kaspersky Endpoint Detection and Response Expert (cloud) при экспорте параметров экспортируются все параметры, в том числе полученные от Kaspersky Endpoint Detection and Response Expert (cloud):
  - адрес и порт сервера телеметрии;
  - адрес и порт сервера реагирования;
  - время ожидания соединения с серверов реагирования;
  - время ожидания ответа от сервера реагирования;
  - время ожидания соединения с серверов телеметрии;
  - время ожидания ответа от сервера телеметрии;
  - клиентский сертификат сервера телеметрии;
  - серверный сертификат сервера телеметрии;

- клиентский сертификат сервера реагирования;
- серверный сертификат сервера реагирования.

При импорте перечисленные выше параметры не импортируются на устройстве.

Управление через графический интерфейс

Для управления приложением через графический интерфейс вам потребуются права пользователя с ролью Администратор (admin).

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, графический интерфейс не поддерживается.

В **стандартном режиме** приложения с помощью графического интерфейса вы можете:

- Просматривать информацию о состоянии защиты устройства.
- Настраивать компоненты приложения.

  Компоненты приложения

  - Защита от файловых угроз.
  - Управление сетевым экраном.
  - Защита от шифрования.
  - Проверка съемных дисков.
  - Защита от веб-угроз.
  - Защита от почтовых угроз.
  - Контроль устройств.
  - Защита от сетевых угроз.
  - Защита от атак BadUSB.
  - Анализ поведения.
  - Защита от эксплойтов.
  - Контроль приложений.
  - Веб-Контроль.
  - Контроль целостности системы.
- Выполнять проверку файлов и директорий, в том числе отправлять файлы на проверку в Sandbox.

- Запускать обновление и откат обновления баз.
- Включать и выключать использование Kaspersky Security Network в работе приложения.
- Запрашивать и получать временный доступ к заблокированному устройству у администратора локальной сети организации.
- Управлять лицензионными ключами приложения и просматривать информацию об используемых лицензиях и ключах.
- Просматривать информацию об объектах, помещенных в резервное хранилище.
- Просматривать отчеты о работе приложения.
- Создавать файлы трассировки приложения.

Значок приложения в области уведомлений

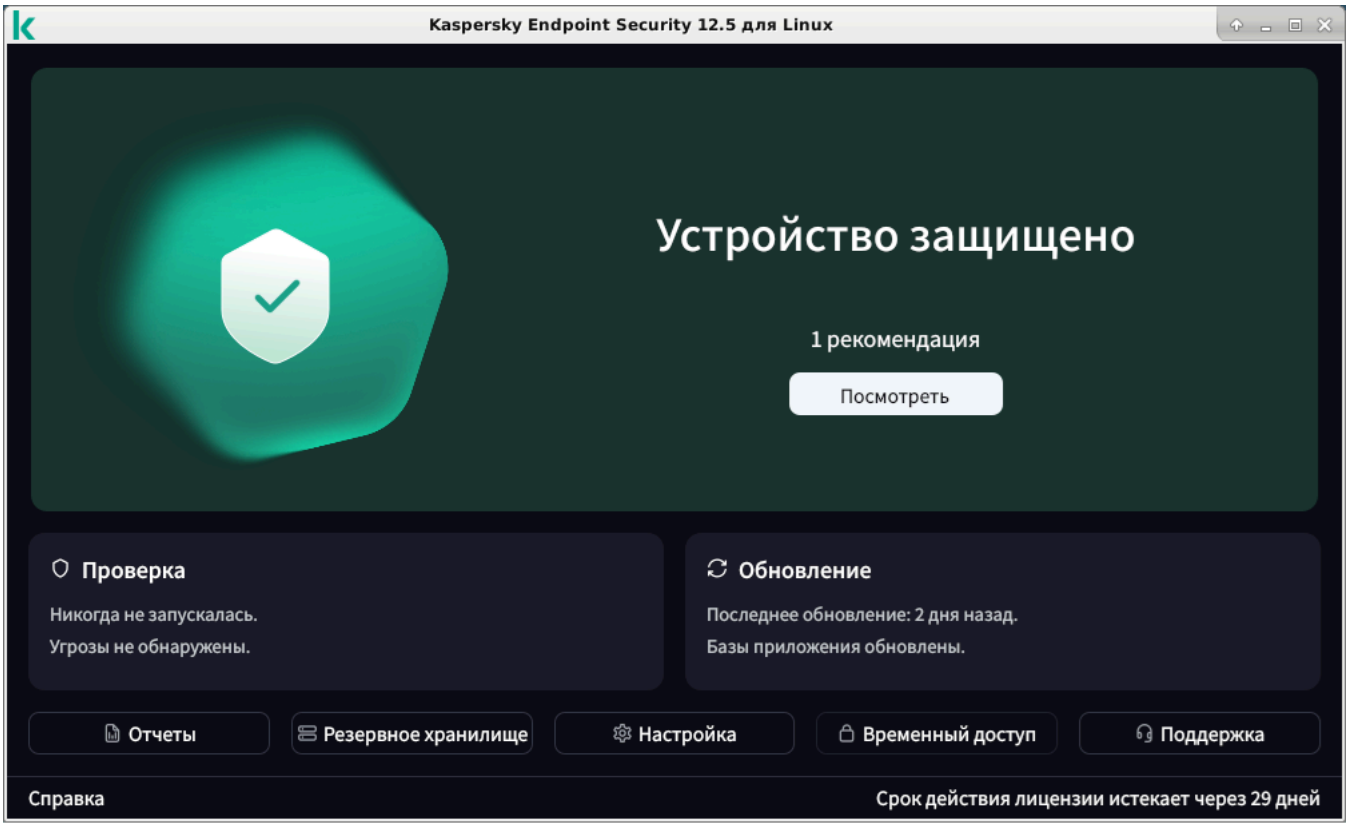
Значок приложения Kaspersky Endpoint Security в области уведомлений панели задач обеспечивает доступ к контекстному меню и главному окну графического интерфейса приложения.

> На некоторых операционных системах значок приложения по умолчанию может отсутствовать после установки пакета графического интерфейса приложения.

Контекстное меню значка приложения содержит следующие пункты:

- **Kaspersky Endpoint Security 12.5 для Linux**. Открывает главное окно графического интерфейса приложения.
- **Выход**. Выполняет выход из графического интерфейса приложения.

Главное окно графического интерфейса приложения



Главное окно приложения

Статус защиты	Информация о состоянии защиты устройства. Отображается в верхней части главного окна. Вы можете нажать на кнопку **Посмотреть**, чтобы открыть окно **Центр защиты**. В этом окне можно посмотреть рекомендации о действиях, которые нужно выполнить для устранения проблем в защите (при их наличии).
Проверка	Информация о состоянии задачи Поиск вредоносного ПО и количестве обнаруженных угроз. Вы можете нажать на этот блок, чтобы открыть окно **Проверка**. В этом окне можно запускать и останавливать задачи *Поиск вредоносного ПО*, *Проверка важных областей* и *Проверка контейнеров* и просматривать отчеты для этих задач.
Обновление	Информация о состоянии задачи обновления баз. Вы можете нажать на этот блок, чтобы открыть окно **Обновление**. В этом окне можно запускать задачи *Обновление* и *Откат обновления баз* и просматривать отчеты для этих задач.
Отчеты	Просмотр отчетов, а также статистики работы компонентов и задач.
Резервное хранилище	Просмотр информации об объектах в резервном хранилище. Что делать, если кнопка неактивна
Настройка	Включение или выключение компонентов приложения, а также настройка использования Kaspersky Security Network. Что делать, если кнопка неактивна
Временный доступ	Запрос и получение временого доступа к заблокированному устройству.
Поддержка	Информация о приложении: текущая версия Kaspersky Endpoint Security, дата выпуска баз, ключ и другая информация. Также вы можете перейти на информационные ресурсы "Лаборатории Касперского", чтобы ознакомиться с полезной информацией или обратиться в Службу технической поддержки.
Срок действия лицензии	Оставшийся срок действия лицензии Вы можете нажать на эту область, чтобы открыть окно **Лицензии**. В этом окне можно посмотреть подробную информацию о вашей лицензии, а также перейти на сайт "Лаборатории Касперского" и приобрести новую лицензию.

Мониторинг состояния защиты

Состояние защиты клиентских устройств Kaspersky Security Center

Вы можете получать информацию о состоянии защиты устройства в Kaspersky Security Center с помощью статусов клиентских устройств. Клиентским устройством для Kaspersky Security Center является устройство, на котором установлен Агент администрирования Kaspersky Security Center.

Статус клиентского устройства может изменяться на *Критический* или *Предупреждение* в соответствии с правилами, определенными в Kaspersky Security Center. Например, статус может измениться, если на устройстве не установлено приложение защиты, давно не выполнялся поиск вирусов, устарели базы приложения, истек срок действия лицензии или если Kaspersky Security Center получил такой статус устройства от управляемого приложения.

Подробнее о причинах изменения статусов и настройке условий присвоения статусов см. в справке Kaspersky Security Center.

Как посмотреть состояние защиты устройства в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Чтобы выбрать вложенную группу, нажмите на кнопку **Показать иерархию** в верхней части окна.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. Нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства на вкладке **Общие** выберите раздел **Защита**.

В разделе **Защита** отображается следующая информация об устройстве:

- **Видимо в сети** – видимость выбранного устройства в сети: *Да* или *Нет*.
- **Статус устройства** – статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на выбранном устройстве и активности устройства в сети: *OK*, *Критический* или *Предупреждение*.
- **Описание статуса** – причины смены статуса устройства на *Критический* или *Предупреждение*.
- **Состояние защиты** – текущий статус защиты от файловых угроз на выбранном устройстве, например: *Выполняется*, *Остановлена*, *Приостановлена*.
- **Последняя полная проверка** – дата и время выполнения последней полной проверки на выбранном устройстве.

- **Обнаружен вирус** – общее количество вредоносных объектов, обнаруженных на выбранном устройстве (счетчик обнаруженных угроз) с момента установки приложения Kaspersky Endpoint Security.

- **Объекты, которые не удалось вылечить** – количество зараженных объектов, которые приложению Kaspersky Endpoint Security не удалось вылечить.

Как посмотреть состояние защиты устройства в Консоли администрирования

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.

2. В рабочей области выберите вкладку **Устройства**.

3. В списке управляемых устройств выберите нужное вам устройство и откройте окно **Свойства: <Имя устройства>** двойным щелчком мыши.

4. В открывшемся окне свойств управляемого устройства выберите раздел **Защита**.

В разделе **Защита** отображается следующая информация об устройстве:

- **Статус устройства** – статус клиентского устройства, формируемый на основании установленных администратором критериев состояния защиты на выбранном устройстве и активности устройства в сети.

- **Все проблемы** – полный список проблем, обнаруженных управляемыми приложениями, установленными на выбранном устройстве. Каждая проблема имеет статус, который приложение предлагает вам назначить устройству.

- **Статус постоянной защиты** – текущий статус защиты от файловых угроз на выбранном устройстве, например, *Выполняется* или *Остановлена*. При изменении статуса защиты новый статус отображается в окне свойств устройства только после синхронизации устройства с Сервером администрирования.

- **Последняя проверка по требованию** – дата и время выполнения последнего поиска вредоносного ПО на выбранном устройстве.

- **Всего обнаружено угроз** – общее количество угроз, обнаруженных на выбранном устройстве с момента установки приложения (первой проверки устройства) или с момента последнего обнуления счетчика угроз.

  Чтобы обнулить счетчик, нажмите на кнопку **Обнулить**.

- **Активные угрозы** – количество необработанных файлов на выбранном устройстве.

Подробнее о статусах клиентского устройства см. в справке Kaspersky Security Center.

Общая информация о работе приложения на устройстве

Как посмотреть общую информацию о работе приложения в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Чтобы выбрать вложенную группу, нажмите на кнопку **Показать иерархию** в верхней части окна.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. Нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

5. В списке приложений, установленных на устройстве, нажмите на название приложения Kaspersky Endpoint Security.

   Откроется окно свойств приложения.

6. Посмотрите общую информацию о приложении на вкладке **Общие** в разделе **Информация**:

   - **Имя** – название приложения.
   - **Версия** – номер версии приложения.
   - **Установлено** – дата и время установки приложения на устройстве.
   - **Последнее обновление ПО** – дата и время последнего обновления модулей приложения Kaspersky Endpoint Security.
   - **Последняя синхронизация** – дата и время последнего соединения устройства с Сервером администрирования Kaspersky Security Center.
   - **Текущий статус** – состояние работы приложения на устройстве, например: *Выполняется* или *Остановлено*.
   - Блок **Устанавливаемые обновления** содержит информацию об установленных версиях обновлений для приложения.
   - Блок **Базы приложения** содержит информацию о дате и времени выпуска обновления баз приложения и дате и времени последнего обновления.

7. Посмотрите информацию о работе функциональных компонентов приложения на вкладке **Общие** в разделе **Компоненты**. Для каждого компонента отображается его статус (например, *Остановлен, Приостановлен, Не установлен*) и версия.

8. Посмотрите список событий приложения на устройстве на вкладке **События**.

Как посмотреть общую информацию о работе приложения в Консоли администрирования

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.

2. В рабочей области выберите вкладку **Устройства**.

3. В списке управляемых устройств выберите нужное вам устройство и откройте окно **Свойства: <Имя устройства>** двойным щелчком мыши.

4. В открывшемся окне свойств управляемого устройства выберите раздел **Программы**.

   В правой части окна отобразится список приложений "Лаборатории Касперского", установленных на устройстве.

5. Выберите приложение Kaspersky Endpoint Security и откройте окно свойств приложения двойным щелчком мыши или с помощью кнопки **Свойства** в нижней части окна.

   Откроется окно свойств приложения.

6. Посмотрите общую информацию о приложении в разделе **Общие**:

   - **Номер версии** – номер версии приложения.
   - **Установлено** – дата и время установки приложения на устройстве.
   - **Текущее состояние** – статус работы приложения (служба kesl). Приложение может иметь статус, например: *Выполняется* или *Приостановлена*.
   - **Последнее обновление ПО** – дата и время последнего обновления модулей приложения Kaspersky Endpoint Security.
   - **Установленные обновления** – информация об установленных версиях обновлений для приложения.
   - **Базы приложения** – дата и время выпуска обновления баз приложения.

7. Посмотрите информацию о работе функциональных компонентов приложения в разделе **Компоненты**. Для каждого компонента отображается его статус (например, *Остановлен, Приостановлен, Не установлен*) и версия.

Как посмотреть общую информацию о работе приложения в командной строке

Выполните команду

```
kesl-control --app-info [--json] [--check-permissions]
```

Где:

`--json` – выводить данные в формате JSON.

`--check-permissions` – выводить пути к директориям приложения с неверно настроенными правами.

В результате выполнения команды в консоль будет выведена следующая информация:

- **Название**. Название приложения.
- **Версия**. Текущая версия приложения.
- **Политика**. Информация о том, применяется ли на устройстве политика Kaspersky Security Center.
- Расширенная информация о политике, применяемой на устройстве:
  - Название политики.
  - Дата и время последнего применения или обновления политики на устройстве.
  - Группа администрирования Kaspersky Security Center, в которую входит устройство.
  - Список профилей политики, применяемых на устройстве (если есть).

Расширенная информация о политике отображается, если в параметрах Агента администрирования, установленного на устройстве, включено получение расширенных данных о политике Kaspersky Endpoint Security (параметр **Приложение может получать расширенные данные политики на устройстве**). По умолчанию параметр выключен. Подробнее о параметрах Агента администрирования см. в справке Kaspersky Security Center.

- Информация о лицензии, по которой используется приложение:
  - **Информация о лицензии приложения**. Информация о лицензии приложения или статус лицензионного ключа приложения.
  - **Дата окончания срока действия лицензии Kaspersky Endpoint Security**. Дата и время (UTC) окончания срока действия лицензии приложения.
- Информация о лицензии для активации компонента Endpoint Detection and Response Optimum и компонентов для интеграции с решениями "Лаборатории Касперского". Поля отображаются, если на защищенном устройстве активированы эти компоненты:
  - **Информация о лицензии EDR Optimum**. Информация о лицензии, по которой активирован компонент Endpoint Detection and Response Optimum, или статус лицензионного ключа EDR Optimum.
  - **Дата окончания срока действия лицензии EDR Optimum**. Дата и время (UTC) окончания срока действия лицензии.
  - **Информация о лицензии KUMA**. Информация о лицензии, по которой используется функциональность Kaspersky Unified Monitoring and Analysis Platform, или статус лицензионного ключа KUMA.
  - **Дата окончания срока действия лицензии KUMA**. Дата и время (UTC) окончания срока действия лицензии.
  - **Информация о лицензии MDR**. Информация о лицензии, по которой активирован компонент Managed Detection and Response, или статус лицензионного ключа MDR.
  - **Дата окончания срока действия лицензии MDR**. Дата и время (UTC) окончания срока действия лицензии.
  - **Информация о лицензии EDR Expert (on-premises)**. Информация о лицензии, по которой активирован компонент Endpoint Detection and Response Expert (on-premises), или статус лицензионного ключа EDR Expert (on-premises).
  - **Дата окончания срока действия лицензии EDR Expert (on-premises)**. Дата и время (UTC) окончания срока действия лицензии.
  - **Информация о лицензии EDR Expert (cloud)**. Информация о лицензии, по которой активирован компонент Endpoint Detection and Response Expert (cloud), или статус лицензионного ключа EDR Expert (cloud).
  - **Дата окончания срока действия лицензии EDR Expert (cloud)**. Дата и время (UTC) окончания срока действия лицензии.
- **Статус подписки**. Статус подписки. Это поле отображается, если приложение используется по подписке.
- **Статус файла MDR BLOB**. Статус файла MDR BLOB, который используется для интеграции с Kaspersky Managed Detection and Response.

- **Дата окончания срока действия лицензии из файла MDR BLOB**. Дата и время (UTC) окончания срока действия лицензии на использование Kaspersky Managed Detection and Response. Это поле отображается, если загружен конфигурационный файл BLOB для интеграции с Kaspersky Managed Detection and Response.

- **Состояние резервного хранилища**. Информация о состоянии резервного хранилища.

- **Использование резервного хранилища**. Размер резервного хранилища.

- **Дата последнего запуска задачи Scan_My_Computer**. Время последнего запуска задачи Поиск вредоносного ПО.

- **Дата последнего выпуска баз приложения**. Время последнего выпуска баз приложения.

- **Базы приложения загружены**. Информация о том, загружены ли базы приложения.

- **Состояние обновляемого модуля ядра**. Информация о состоянии обновляемого модуля ядра.

- **Использование Kaspersky Security Network**. Информация об использовании Kaspersky Security Network: `Расширенный режим KSN`, `Стандартный режим KSN` или `Выключен`.

- **Режим Легкого агента**. Информация о том, что приложение используется в режиме Легкого агента. Если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response, эта строка не отображается.

- **Режим Агента Endpoint Detection and Response**. Информация о том, что приложение используется в режиме EDR-Агента. Если приложение используется в стандартном режиме или в режиме Легкого агента, эта строка не отображается.

- **Инфраструктура Kaspersky Security Network**. Информация об инфраструктурном решении, которое используется для работы с репутационными базами "Лаборатории Касперского": `Kaspersky Security Network` или `Kaspersky Private Security Network`.

- **Интеграция с Kaspersky Managed Detection and Response**. Статус интеграции с Kaspersky Managed Detection and Response.

- **Интеграция с Kaspersky Endpoint Detection and Response Optimum**. Статус интеграции с Kaspersky Endpoint Detection and Response Optimum.

- **Защита от файловых угроз**. Статус защиты от файловых угроз в реальном времени.

- **Мониторинг контейнеров**. Статус проверки контейнеров в реальном времени.

- **Контроль целостности системы**. Статус компонента Контроль целостности системы.

- **Управление сетевым экраном**. Статус компонента Управление сетевым экраном.

- **Защита от шифрования**. Статус компонента Защита от шифрования.

- **Защита от веб-угроз**. Статус компонента Защита от веб-угроз.

- **Контроль устройств**. Статус компонента Контроль устройств.

- **Проверка съемных дисков**. Статус компонента Проверка съемных дисков.

- **Защита от атак BadUSB**. Статус компонента Защита от атак BadUSB.

- **Защита от сетевых угроз**. Статус компонента Защита от сетевых угроз.
- **Анализ поведения**. Статус компонента Анализ поведения.
- **Контроль приложений**. Статус компонента Контроль приложений.
- **Веб-Контроль**. Статус компонента Веб-Контроль.
- **Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)**. Статус интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) или с Kaspersky Endpoint Detection and Response (KATA).
- **Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud)**. Статус интеграции с Kaspersky Endpoint Detection and Response Expert (cloud).
- **Интеграция с Sandbox**. Статус интеграции с Sandbox.
- **Интеграция с Kaspersky Unified Monitoring and Analysis Platform**. Статус интеграции с Kaspersky Unified Monitoring and Analysis Platform.
- **Интеграция с Kaspersky Network Detection and Response (KATA)**. Статус интеграции с Kaspersky Network Detection and Response (KATA).
- **Защита от почтовых угроз**. Статус компонента Защита от почтовых угроз.
- **Действия после обновления**. Действия по обновлению приложения и действия, которые требуется выполнить пользователю.
- **Приложение работает нестабильно**. Информация о записи дампов при сбое в работе приложения. Это поле отображается, если в директории для хранения дампов обнаружены файлы.
- **Статус приложения**. Информация о состоянии подключения к Агенту администрирования и прав на системные директории:
  - *OK*. Агент администрирования подключен, права на системные директории настроены корректно.
  - *Критический. Нет подключения к Агенту администрирования.*
  - *Критический. Неверно настроены права на системные директории.*
  - *Критический. Нет подключения к Агенту администрирования. Неверно настроены права на системные директории.*

Как посмотреть общую информацию о работе приложения в графическом интерфейсе

1. Откройте главное окно графического интерфейса приложения.
2. В нижней части главного окна нажмите на кнопку **Поддержка**.

   Откроется окно **Поддержка**.

3. Посмотрите общую информацию об устройстве и установленном приложении:

   - Версия приложения.
   - **Лицензионный ключ** – активный основной лицензионный ключ, добавленный в приложение, или информация об отсутствии ключа. По ссылке в этом поле вы можете открыть окно **Лицензии**, в котором отображается подробная информация о лицензии.
   - **Статус ключа** – информация о статусе активного основного лицензионного ключа или информация об отсутствии ключа.
   - **Дата выпуска баз** – состояние и дата выпуска баз приложения.
   - **Операционная система** – сведения об операционной системе устройства.
   - **Управление приложением** – информация о том, находится ли устройство под управлением политики.

   Если в политике Агента администрирования включен параметр **Приложение может получать расширенные данные политики на устройстве**, в окне также отображается следующая информация о политике, которая применяется на устройстве с установленным приложением.

   - **Название политики** – название политики, под управлением которой работает устройство с установленным приложением.
   - **Дата применения политики** – дата и время последнего применения или обновления политики на устройстве. с установленным приложением.
   - **Группа администрирования** – название группы администрирования, в состав которой входит устройство с установленным приложением, работающее под управлением политики.
   - **Активные профили политики** – список активных профилей политики, применяемых на устройстве (если есть).

Статистика работы приложения

Вы можете просматривать статистику о наиболее часто проверяемых файлах и запускаемых процессах.

Параметры подсчета и вывода статистики приложением можно настроить в конфигурационном файле kesl.ini в секции `[ScannerImpactStats]`.

Как посмотреть статистику проверок в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Чтобы выбрать вложенную группу, нажмите на кнопку **Показать иерархию** в верхней части окна.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. Нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

5. В списке приложений, установленных на устройстве, нажмите на название приложения Kaspersky Endpoint Security.

6. В открывшемся окне свойств приложения на вкладке **Параметры приложения** выберите раздел **Статистика** → **Статистика проверки**.

7. Посмотрите статистику работы приложения в окне **Статистика проверки**:

   - В блоке **Наиболее часто проверяемые файлы (Защита от файловых угроз)** отображаются пути к файлам, которые компонент Защита от файловых угроз проверяет наиболее часто, и количество обращений компонента к этим файлам. Файлы отображаются в порядке убывания количества обращений к ним.

   - В блоке **Наиболее часто запускаемые процессы** отображаются пути к процессам, запуск которых приложение Kaspersky Endpoint Security обнаруживает наиболее часто, и количество этих запусков. Пути к процессам отображаются в порядке убывания количества запусков процессов.

   По кнопкам **Экспортировать**, расположенным в верхней части каждого блока, вы можете экспортировать статистику в файл текстового формата.

Как посмотреть статистику проверок в Консоли администрирования

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.

2. В рабочей области выберите вкладку **Устройства**.

3. В списке управляемых устройств выберите нужное вам устройство и откройте окно **Свойства: <Имя устройства>** двойным щелчком мыши.

4. В открывшемся окне свойств управляемого устройства выберите раздел **Программы**.

   В правой части окна отобразится список приложений "Лаборатории Касперского", установленных на устройстве.

5. Выберите приложение Kaspersky Endpoint Security и откройте окно свойств приложения двойным щелчком мыши или с помощью кнопки **Свойства** в нижней части окна.

6. В открывшемся окне выберите раздел **Статистика** → **Статистика проверки**.

7. Посмотрите статистику работы приложения:

   - В блоке **Наиболее часто проверяемые файлы (Защита от файловых угроз)** отображаются пути к файлам, которые компонент Защита от файловых угроз проверяет наиболее часто, и количество обращений компонента к этим файлам. Файлы отображаются в порядке убывания количества обращений к ним.

   - В блоке **Наиболее часто запускаемые процессы** отображаются пути к процессам, запуск которых приложение Kaspersky Endpoint Security обнаруживает наиболее часто, и количество этих запусков. Пути к процессам отображаются в порядке убывания количества запусков процессов.

   По кнопкам **Экспортировать**, расположенным под каждым блоком, вы можете экспортировать статистику в файл текстового формата.

Как посмотреть статистику проверок в командной строке

Выполните команду

```
kesl-control [-S] --get-statistic [--files] [--processes]
```

Где:

- `--files` – статистика о файлах, которые наиболее часто проверяет компонент Защита от файловых угроз, и количество обращений компонента к этим файлам;
- `--processes` – статистика о процессах, запуск которых приложение Kaspersky Endpoint Security обнаруживает наиболее часто, и количество этих запусков;

  Исключение процессов из проверки компонентом Анализ поведения не удаляет их из статистики, но увеличивает производительность приложения Kaspersky Endpoint Security.

Если вы не укажете ключи, приложение выведет три списка: статистику о наиболее часто проверяемых файлах, статистику о наиболее часто запускаемых процессах и список обнаруженных на устройстве точек монтирования.

На операционных системах CentOS 5.2, 5.4, 6.4 и 6.6 статистика часто проверяемых файлов не собирается.

Обнаруженные точки монтирования

Вы можете просматривать список обнаруженных на устройстве точек монтирования. В списке отображается информация о том, добавлена ли точка монтирования в исключения из проверки.

Как посмотреть список точек монтирования в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Чтобы выбрать вложенную группу, нажмите на кнопку **Показать иерархию** в верхней части окна.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. Нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

5. В списке приложений, установленных на устройстве, нажмите на название приложения Kaspersky Endpoint Security.

6. В открывшемся окне свойств приложения на вкладке **Параметры приложения** выберите раздел **Статистика** → **Точки монтирования**.

   Откроется окно **Точки монтирования**.

7. Посмотрите информацию о точках монтирования в таблице:

   - **Путь к точке монтирования** – путь к обнаруженной на устройстве точке монтирования.
   - **Пространство имен** – информация о том, обнаружена ли точка монтирования в пространстве имен.
   - **Исключена** – информация о том, добавлена ли точка монтирования в исключения из проверки.

   Пути к точкам монтирования отсортированы следующим образом:

   - статичные, системные, служебные и другие точки монтирования;
   - смонтированные пакеты snap и точки монтирования внутри их пространств имен;
   - точки монтирования, созданные системой управления контейнерами Docker.

   По кнопке **Экспортировать**, расположенной в верхней части окна над списком, вы можете экспортировать список точек монтирования в файл текстового формата. Файл содержит список путей к точкам монтирования, а также метки **[Пространство имен]** и **[Исключена]**.

Как посмотреть список точек монтирования в Консоли администрирования

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.
2. В рабочей области выберите вкладку **Устройства**.
3. В списке управляемых устройств выберите нужное вам устройство и откройте окно **Свойства: <Имя устройства>** двойным щелчком мыши.
4. В открывшемся окне свойств управляемого устройства выберите раздел **Программы**.

   В правой части окна отобразится список приложений "Лаборатории Касперского", установленных на устройстве.
5. Выберите приложение Kaspersky Endpoint Security и откройте окно свойств приложения двойным щелчком мыши или с помощью кнопки **Свойства** в нижней части окна.
6. В окне свойств приложения выберите раздел **Статистика** → **Точки монтирования**.
7. Посмотрите информацию о точках монтирования в таблице **Список точек монтирования**:

   - **Путь к точке монтирования** – путь к обнаруженной на устройстве точке монтирования.
   - **Пространство имен** – информация о том, обнаружена ли точка монтирования в пространстве имен.
   - **Исключена** – информация о том, добавлена ли точка монтирования в исключения из проверки.

   Пути к точкам монтирования отсортированы следующим образом:

   - статичные, системные, служебные и другие точки монтирования;
   - смонтированные пакеты snap и точки монтирования внутри их пространств имен;
   - точки монтирования, созданные системой управления контейнерами Docker.

По кнопке **Экспортировать**, расположенной под списком, вы можете экспортировать список точек монтирования в файл текстового формата. Файл содержит список путей к точкам монтирования, а также метки `[Пространство имен]` и `[Исключена]`.

Как посмотреть список точек монтирования в командной строке

Выполните команду

```
kesl-control [-S] --get-statistic --mountpoints
```

В выводе отображается следующая информация:

- `[excluded]` – информация о том, добавлена ли точка монтирования в исключения из проверки;
- `[namespace]` – информация о том, обнаружена ли точка монтирования в пространстве имен;
- путь к обнаруженной на устройстве точке монтирования.

Пути к точкам монтирования отсортированы следующим образом:

- статичные, системные, служебные и другие точки монтирования;
- смонтированные пакеты snap и точки монтирования внутри их пространств имен;
- точки монтирования, созданные системой управления контейнерами Docker.

Список функций и технологий

В командной строке вы можете посмотреть список функций приложения, информацию об их статусах (используется или не используется) и технологиях Linux, с помощью которых реализованы эти функции приложения.

Посмотреть список функций и технологий

```
kesl-control --supported-tech-info
```

В результате выполнения команды в консоль будет выведена следующая информация:

Перехват файловых операций:

Статус: используется/не используется.

Технологии: fanotify, модуль ядра для защиты от файловых угроз, обновляемый модуль ядра.

Перехват запуска процессов:

Статус: используется/не используется.

Технологии: eBPF, kprobe, netlink, не определено, обновляемый модуль ядра.

Перехват сетевого трафика:

Статус: используется/не используется.

Технологии: eBPF, iptables, не определено.

Утилита iptables:

Статус: используется/не используется.

Технологии: ipv6, не определено, ограничение времени ожидания, поддержка нескольких меток в правилах.

Сетевая изоляция:

Статус: используется/не используется.

Технологии: eBPF, iptables, не определено.

Защита от эксплойтов:

Статус: используется/не используется.

Технологии: не определено, обновляемый модуль ядра.

Статусы постоянной защиты

Статус постоянной защиты компьютера определяет статус компонента Защита от файловых угроз. Защита от файловых угроз обеспечивает минимальный уровень безопасности компьютера. Компонент запускается вместе с Kaspersky Endpoint Security и проверяет файлы в режиме реального времени.

Статусы постоянной защиты

Статус в Kaspersky Security Center	Статус в командной строке	Описание
Выполняется	Запущена	Задача Защита от файловых угроз запущена и работает.
Запускается	Запускается или Возобновляется	Попытка запуска задачи Защита от файловых угроз. Дождитесь запуска задачи.
Остановлена	Остановлена или Останавливается	Задача Защита от файловых угроз остановлена вручную. Запустите задачу в Kaspersky Security Center или на компьютере локально. Если приложение установлено в режиме Легкого агента, этот статус устройство получает при отсутствии связи с SVM.
Приостановлен	Приостанавливается или Приостановлена	Задача Защита от файловых угроз приостановлена вручную. Запустите задачу в Kaspersky Security Center или на компьютере локально.
Не установлен		Приложение установлено в режиме EDR-агента. Компонент Защита от файловых угроз работает в режиме информирования.
Нет данных		Неизвестная ошибка.

Как узнать статус постоянной защиты

Вы можете узнать статус постоянной защиты компьютера в консоли Kaspersky Security Center в списке управляемых устройств или локально на компьютере.

Как узнать статус постоянной защиты в Web Console

В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

В списке устройств в графе **Статус постоянной защиты** отображается текущий статус защиты. Если графа **Статус постоянной защиты** отсутствует, настройте параметры столбцов (⚙).

Как узнать статус постоянной защиты в командной строке

Выполните команду

```
kesl-control --get-task-state 1
```

В результате Kaspersky Endpoint Security покажет информацию о работе Защиты от файловых угроз в следующем виде:

Имя: File_Threat_Protection	
Идентификатор	: 1
Тип	: OAS
Состояние	: <protection status>

Что делать, если статус постоянной защиты отличается от Выполняется

1. Убедитесь, что Защита от файловых угроз включена в свойствах политики.
2. Проверьте, что приложение активировано.
3. Попробуйте запустить задачу Защита от файловых угроз:

   Как запустить задачу Защита от файловых угроз в Web Console

   1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

      Откроется список управляемых устройств.
   2. Найдите нужное устройство в списке и нажмите на его имя.
   3. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Задачи**.

      Откроется список всех задач на устройстве.
   4. Выберите задачу **Защита от файловых угроз** и нажмите на кнопку **Запустить**.

Как запустить задачу Защита от файловых угроз в командной строке

Выполните команду

```
kesl-control --start-task 1
```

События и отчеты

В процессе работы приложения возникают различного рода *события*. Они могут иметь информационный характер или нести важную информацию. Например, с помощью события приложение может сообщать об успешно выполненном обновлении баз приложения или об ошибке в работе компонента, которую требуется устранить.

Kaspersky Endpoint Security позволяет вносить информацию о событиях, возникающих в работе приложения, в следующие журналы:

- Журнал событий приложения. По умолчанию приложение сохраняет информацию о событиях в файлах базы данных журнала событий в директории /var/opt/kaspersky/kesl/private/storage. Вы можете настраивать параметры журнала событий приложения в командной строке.
- Журнал операционной системы (syslog). По умолчанию журнал операционной системы не используется. Вы можете включить запись событий в этот журнал.

Для доступа к журналу событий приложения и к журналу операционной системы требуются root-права.

Если управление приложением Kaspersky Endpoint Security осуществляется с помощью Kaspersky Security Center, данные о событиях могут передаваться на Сервер администрирования Kaspersky Security Center. Для некоторых событий действуют правила агрегирования. В случае, если за короткий промежуток времени в процессе работы приложения создается много событий одного типа, приложение переключается в режим агрегирования событий и отправляет в Kaspersky Security Center одно агрегированное событие с описанием параметров этих событий. Для разных событий могут использоваться разные правила агрегирования. Подробнее о событиях см. в справке Kaspersky Security Center.

Вы можете получать информацию о событиях приложения следующими способами:

- В Консоли администрирования и в Web Console.
- В командной строке.
- При использовании графического пользовательского интерфейса приложения – во всплывающих уведомлениях, если отображение уведомлений разрешено в свойствах политики или в общих параметрах приложения.

На основе событий, происходящих во время работы приложения, можно формировать различные *отчеты*. В отчеты записываются информация о работе каждого компонента приложения Kaspersky Endpoint Security и результаты выполнения каждой задачи и работы всего приложения в целом.

Вы можете просматривать отчеты следующими способами:

- В Консоли администрирования и в Web Console доступны отчеты Kaspersky Security Center. С их помощью вы можете, например, получить сведения о зараженных файлах, использовании ключей и баз приложения. Подробную информацию о работе с отчетами Kaspersky Security Center см. в справке Kaspersky Security Center.

- В графическом пользовательском интерфейсе Kaspersky Endpoint Security доступны отчеты о работе приложения, его компонентов и задач.

Содержимое отчетов и событий

В событиях и отчетах могут содержаться следующие персональные данные:

- имена и идентификаторы пользователей в операционной системе;

- пути к файлам пользователя;

- IP-адреса удаленных устройств, проверяемых компонентом Защита от шифрования;

- IP-адреса отправителей и получателей сетевых пакетов, проверяемых компонентом Управление сетевым экраном;

- веб-адреса источников обновлений;

- значения общих параметров приложения;

- имена и параметры задач командной строки;

- обнаруженные вредоносные, фишинговые, рекламные веб-адреса и веб-адреса, содержащие легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным;

- названия контейнеров и образов;

- пути к контейнерам и образам;

- названия и идентификаторы устройств;

- названия категорий приложений;

- веб-адреса репозиториев;

- имена файлов, пути к файлам и хеш-суммы исполняемых файлов приложений.

Правила экранирования символов в путях к файлам

Некоторые события могут содержать пути к файлам. При выводе путь к файлу рассматривается как строка в кодировке UTF-8. В случае если какой-то из байт в пути не соответствует правилам кодирования UTF-8, то он заменяется на символ ?. Также на символ ? заменяется последовательность из четырех байт, кодирующая код символов, выходящих за пределы диапазона Unicode (больше 0x10FFFF). Специальные символы экранируются (заменяются) определенным образом.

Правила экранирования символов в путях к файлам в событиях при выводе по команде `kesl-control -E --query`:

- символы '\a', '\b', '\t', '\n', '\v', '\f', '\r' заменяются двумя символами следующим образом:

  '\a' -> "\\a"

  '\b' -> "\\b"

  '\t' -> "\\t"

  '\n' -> "\\n"

  '\v' -> "\\v"

  '\f' -> "\\f"

  '\r' -> "\\r"

- все прочие специальные символы выводятся без изменений.

Правила экранирования символов в путях к файлам в событиях при выводе по команде `kesl-control -E --query --json`:

- символы '\b', '\f', '\n', '\r', '\t', '"', '\\' экранируются, в соответствии с форматом JSON, следующим образом:

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\"

  '\\' -> "\\\\"

- все прочие специальные символы экранируются в соответствии с общими правилами экранирования специальных символов для формата JSON ('\a' -> '\u0007').

Правила экранирования символов в путях к файлам в событиях при передаче в syslog:

- символы '\b', '\f', '\n', '\r', '\t', '"', '\\' экранируются, в соответствии с форматом JSON, следующим образом:

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\"

  '\\' -> "\\\\"

- все прочие специальные символы экранируются в соответствии с общими правилами экранирования специальных символов для формата JSON ('\a' -> '\u0007').

Первый обратный слеш в последовательности при описании правил – это символ экранирования.

Примеры:
`'\a'` – это один символ (управляющий);

`'\\a'` – это два символа (обратный слеш + символ a);

`'\\'` – это один символ (обратный слеш), `'\\\\'` – это два символа (обратный слеш + обратный слеш).

Настройка записи событий в журнал операционной системы

События, возникающие в работе приложения Kaspersky Endpoint Security, могут записываться в журнал операционной системы (syslog). Вы можете включать и выключать запись событий в этот журнал с помощью Web Console, Консоли администрирования или командной строки.

По умолчанию запись событий в журнал операционной системы выключена.

Если Kaspersky Endpoint Security используется в стандартном режиме или в режиме EDR-агента, а также находится под управлением политики в Kaspersky Security Center, по умолчанию в журнал операционной системы записывается информация о добавлении и удалении лицензионных ключей и об истечении срока действия лицензии. Вы можете выбрать события, которые будут записываться в журнал операционной системы, в свойствах политики, под управлением которой работает приложение.

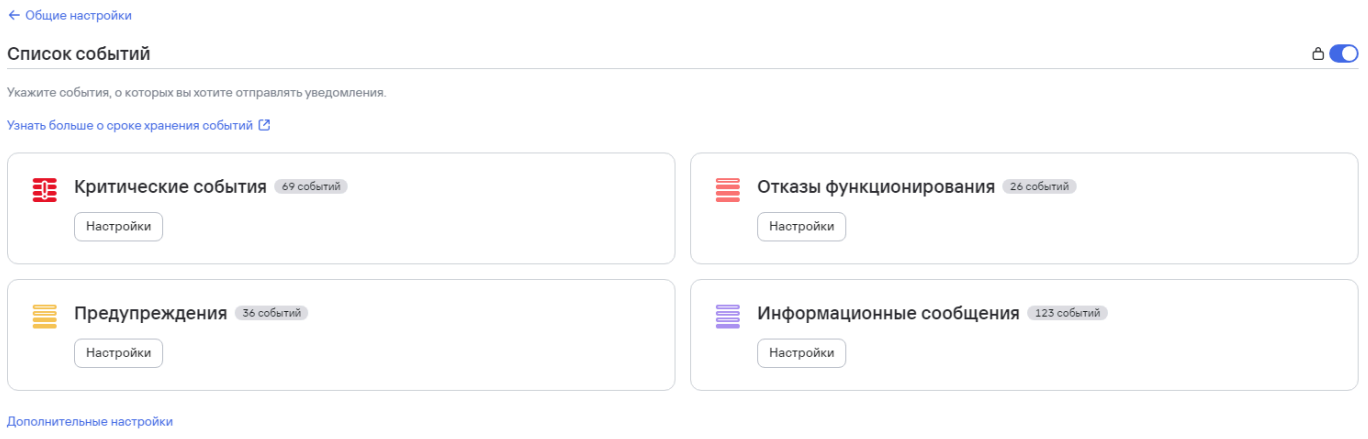
Как настроить запись событий в syslog в Web Console

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

   Откроется окно свойств политики.
3. Перейдите на вкладку **Параметры приложения**.
4. Выберите **Общие настройки** → **Настройки уведомлений**.

   Отобразятся блоки типов событий по уровню важности.
5. Нажмите на кнопку **Настройки** в блоке с названием уровня важности, соответствующего событию, для которого хотите настроить запись в журнал операционной системы.

   Откроется окно со списком всех событий выбранного уровня важности. Вы можете включать и выключать запись в журнал операционной системы для каждого события отдельно.
6. В столбце **События** нажмите на название события, для которого вы хотите настроить запись в журнал операционной системы.
7. Перейдите на вкладку **Уведомления**.
8. Установите или снимите флажок **Сохранять в журнале событий операционной системы**.



Настройки уведомлений о событиях

Как настроить запись событий в syslog в Консоли администрирования

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.

2. В рабочей области выберите вкладку **Политики**.

3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

4. Перейдите в раздел **Общие параметры** → **Интерфейс**.

5. В блоке **Уведомления** нажмите на кнопку **Настроить**.

   Откроется окно **Параметры уведомлений**.

6. С помощью флажков выберите события, которые приложение будет записывать в журнал операционной системы.

   Вы также можете выбрать все события определенного уровня важности:

   - *Критические события* – события, представляющие серьезную угрозу безопасности устройства (обнаружение вредоносных объектов, уязвимостей, проблем в работе приложения). Критические события требуют вашего немедленного внимания. Рекомендуется не выключать уведомления о возникновении критических событий.

   - *Отказы функционирования* – события, возникающие при сбое в работе приложения (ошибка обработки, ошибка в настройках задачи). Такие события не представляют прямую угрозу безопасности устройства, однако требуют ваших действий для корректной работы приложения.

   - *Предупреждения* – события, которые не требуют ваших немедленных действий, но в дальнейшем могут представлять угрозу для безопасности устройства.

   - *Информационные сообщения* – события, носящие информационный характер.

Как настроить запись событий в syslog в командной строке

В командной строке вы можете включать и выключать запись событий в журнал операционной системы с помощью параметра `UseSyslog` из общих параметров приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Включение/выключение записи событий в syslog

```
kesl-control --set-app-settings UseSyslog=<Yes|No>
```

Где:

- `Yes` – включить запись всех событий в syslog.
- `No` (значение по умолчанию) – выключить запись событий в syslog.

Настройка параметров журнала событий приложения

По умолчанию информация о событиях сохраняется в журнале событий приложения, расположенном на устройстве.

База данных журнала событий содержит следующие файлы:

- Несколько файлов с событиями. Количество файлов зависит от текущего количества событий в журнале событий и от максимального количества событий, которое будет хранить приложение (задается в параметре `MaxEventsNumber`).

  Название файла с событиями содержит в названии порядковый номер его создания (например, events.db.0001). Файлы создаются по мере их наполнения. Если во всех файлах событий за исключением самого раннего файла количество событий достигает заданного значения параметра `MaxEventsNumber`, самый ранний файл удаляется. Таким образом, приложение может хранить больше событий, чем указано в параметре.

- Основной файл базы данных для управления файлами с событиями, в котором хранится информация о файлах журнала событий. Этот файл не удаляется.

В командной строке вы можете настраивать следующие параметры журнала событий приложения с помощью общих параметров приложения:

- Изменять путь к основному файлу базы данных журнала событий с помощью параметра `EventsStoragePath`. Значение по умолчанию: /var/opt/kaspersky/kesl/private/storage/events.db.
- Задавать максимальное количество событий, которые будет хранить приложение, с помощью параметра `MaxEventsNumber`. Значение по умолчанию: 500000.

Вы можете смотреть текущие значения параметров в общих параметрах приложения в командной строке или в конфигурационном файле.

Вывести в консоль текущие значения общих параметров приложения

```
kesl-control --get-app-settings [--json]
```

Где `--json` – выводить параметры в формате JSON.

```
Вывести в конфигурационный файл текущие значения общих параметров приложения

kesl-control --get-app-settings --file <path to configuration file> [--json]
```

Где `--file <path to configuration file>` – путь к конфигурационному файлу, в который будут выведены общие параметры приложения. Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанной директории не существует, конфигурационный файл не будет создан.

Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

```
Изменить параметры событий с помощью ключей командной строки

kesl-control --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Где <setting name>=<setting value> – имя и значение одного из параметров.

```
Изменить параметры событий при помощи конфигурационного файла

kesl-control --set-app-settings --file <path to configuration file> [--json]
```

Где:

- `--file <path to configuration file>` – полный путь к конфигурационному файлу с общими параметрами приложения. Если вы удалите какой-либо параметр в конфигурационном файле, после выполнения команды для этого параметра будет указано значение по умолчанию.

- `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ --json, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Все значения общих параметров, заданные в файле, будут импортированы в приложение.

Просмотр событий приложения

Просмотр всех событий приложения Kaspersky Endpoint Security в Kaspersky Security Center

События, возникающие в работе приложения Kaspersky Endpoint Security, по уровню важности делятся на следующие типы:

- *Критические события* – события, представляющие серьезную угрозу безопасности устройства (обнаружение вредоносных объектов, уязвимостей, проблем в работе приложения). Критические события требуют вашего немедленного внимания. Рекомендуется не выключать уведомления о возникновении критических событий.

- *Отказы функционирования* – события, возникающие при сбое в работе приложения (ошибка обработки, ошибка в настройках задачи). Такие события не представляют прямую угрозу безопасности устройства, однако требуют ваших действий для корректной работы приложения.

- *Предупреждения* – события, которые не требуют ваших немедленных действий, но в дальнейшем могут представлять угрозу для безопасности устройства.
- *Информационные сообщения* – события, носящие информационный характер.

Список всех событий в работе приложения Kaspersky Endpoint Security отображается в Web Console и в Консоли администрирования.

Как посмотреть список всех событий в Web Console

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

   Откроется окно свойств политики.
3. Перейдите на вкладку **Настройка событий**.

   Отобразится список всех событий, отфильтрованный по уровню важности.
4. Используйте меню слева, чтобы посмотреть все события других уровней важности.

Как посмотреть список всех событий в Консоли администрирования

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.
2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.
4. Перейдите в раздел **Общие параметры** → **Параметры уведомлений**.
5. В блоке **Уведомления** нажмите на кнопку **Настроить.**

   Откроется окно **Параметры уведомлений**.

Вы можете настроить уведомления о событиях. С помощью уведомлений вы можете своевременно получать информацию о событиях в работе приложения. Вы можете настроить выполнение скрипта при получении события из приложения или получение уведомлений о событиях по электронной почте. Подробнее о работе с событиями в Kaspersky Security Center см. в справке Kaspersky Security Center.

Просмотр событий в графическом интерфейсе приложения

В графическом интерфейсе приложения информация о событиях по умолчанию отображается во всплывающих уведомлениях.

Как настроить всплывающие уведомления в Web Console

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

   Откроется окно свойств политики.
3. Перейдите на вкладку **Параметры приложения**.

4. Выберите **Общие настройки** → **Настройки уведомлений**.

5. Нажмите на ссылку **Дополнительные настройки**.

   Откроется окно **Дополнительные настройки**.

6. Установите или снимите флажок **Показывать всплывающие уведомления в графическом пользовательском интерфейсе**. По умолчанию флажок установлен.

7. Сохраните изменения.

Как настроить всплывающие уведомления в Консоли администрирования

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.

2. В рабочей области выберите вкладку **Политики**.

3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

4. Перейдите в раздел **Общие параметры** → **Параметры уведомлений**.

5. Установите или снимите флажок **Показывать всплывающие уведомления в графическом пользовательском интерфейсе**. По умолчанию флажок установлен.

Как настроить всплывающие уведомления в командной строке

В командной строке вы можете включать и выключать отображение всплывающих уведомлений в графическом интерфейсе с помощью параметра `ShowPopUpNotifications` из общих параметров приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

```
Включение/выключение отображения всплывающих уведомлений в графическом интерфейсе

kesl-control --set-app-settings ShowPopUpNotifications=<Yes|No>
```

Где:

- `Yes` (значение по умолчанию) – показывать всплывающие уведомления в графическом пользовательском интерфейсе.

- `No` – не показывать всплывающие уведомления в графическом пользовательском интерфейсе.

Просмотр текущих событий приложения Kaspersky Endpoint Security в командной строке

С помощью командной строки вы можете выводить в консоль информацию обо всех текущих событиях приложения или о событиях, связанных с указанной задачей. С помощью фильтра вы также можете выводить определенные текущие события, например, события указанного типа.

```
Вывести в консоль информацию обо всех текущих событиях приложения

kesl-control -W
```

Команда возвращает название события и дополнительную информацию о событии.

```
Запустить задачу и выводить в консоль информацию о связанных с ней текущих событиях
kesl-control --start-task <task ID|name> -W
```

где `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда запускает задачу с указанным идентификатором или названием и включает вывод связанных с ней текущих событий. Вывод событий осуществляется по мере их генерации этой задачей.

```
Пример запуска задачи с ID=1 с включением вывода ее событий
kesl-control --start-task 1 -W
```

```
Вывести в консоль информацию о текущих событиях, соответствующих условиям фильтра
kesl-control -W --query "<filter conditions>"
```

где `<filter conditions>` – одно или несколько логических выражений в формате `<field> <comparison operation> '<value>'`, скомбинированных с помощью логического оператора `and`.

```
Пример вывода событий TaskStateChanged
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

```
Пример вывода событий TaskSettingsChanged, инициированных пользователем User
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

Вывод событий из журнала событий приложения

Вы можете выводить в консоль или в файл информацию о событиях из журнала событий приложения с помощью командной строки. Для вывода определенных событий используйте фильтр.

```
Вывести в консоль информацию обо всех событиях в журнале событий приложения
kesl-control -E --query [--db <database file>]
```

где `<database file>` – полный путь к файлу базы данных журнала событий, из которого вы хотите вывести события.

По умолчанию приложение сохраняет информацию о событиях в базе данных `/var/opt/kaspersky/kesl/private/storage/events.db`. Расположение базы данных определяется общим параметром приложения `EventsStoragePath`.

Если журнал событий расположен в базе данных по умолчанию, для вывода событий в консоль используйте команду:

```
kesl-control -E
```

Вы можете использовать утилиту `less`, чтобы перемещаться по списку отображаемых событий. По умолчанию в приложении хранится до 500 000 событий. Максимальное количество событий, которые хранит приложение, определяется общим параметром приложения `MaxEventsNumber`.

Вывести в консоль информацию о событиях в журнале событий приложения, соответствующих определенным условиям

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--json] [--reverse]
```

где:

- `<filter conditions>` – одно или несколько логических выражений в формате `<field> <comparison operator> '<value>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.
- `<number>` – количество последних событий из выборки (то есть количество записей от конца выборки), которые нужно вывести.
- `--json` – выводить события в формате JSON.
- `--reverse` – выводить события в обратном порядке (от самого нового события наверху к более старым внизу).

Вывести в файл информацию обо всех событиях в журнале событий приложения

```
kesl-control -E --query "<>" [--db <database file>] [-n <number>] --file <path to file> [--json]
```

где `--file <path to file>` – полный путь к файлу, в который вы хотите вывести события.

Полезные статьи

Что делать при ложных срабатываниях

Просмотр отчетов

Просмотр отчетов доступен только в графическом интерфейсе приложения.

Информация о работе каждого компонента Kaspersky Endpoint Security, о выполнении каждой задачи проверки, задачи обновления и задачи проверки целостности, а также о работе приложения в целом сохраняется в *отчетах*.

В отчетах предусмотрены следующие уровни важности событий:

- *Критический* – события критической важности, на которые нужно обратить внимание, поскольку они указывают на проблемы в работе приложения или на уязвимости в защите устройства.
- *Высокий.*
- *Средний.*

- *Низкий.*
- *Информационный.*
- *Ошибка.*

В приложении доступны следующие отчеты:

- **Статистика**. Статистические данные о работе компонента Защита от файловых угроз и о задачах проверки. Вы можете обновить отображаемый отчет, нажав на кнопку **Обновить**.
- **Системный аудит**. Информация о событиях, которые произошли во время работы приложения и во время взаимодействия пользователя с приложением.
- **Защита от угроз**. Информация о событиях, зарегистрированных в журнале во время работы следующих компонентов приложения:
  - Защита от файловых угроз.
  - Проверка съемных дисков.
  - Защита от шифрования.
  - Защита от веб-угроз.
  - Защита от почтовых угроз.
  - Защита от сетевых угроз.
  - Защита от атак BadUSB.
  - Управление сетевым экраном.
  - Контроль приложений.
  - Контроль устройств.
  - Анализ поведения.
  - Защита от эксплойтов.
  - Контроль целостности системы.
  - Веб-Контроль.
- **Задачи по требованию**. Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время выполнения задач проверки, задач обновления и задач проверки целостности системы.
- **Запрет запуска объектов**. Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время работы запрета запуска объектов компонентов EDR Expert (on-premises) и EDR Optimum.

Как посмотреть отчет в интерфейсе приложения

1. Откройте главное окно графического интерфейса приложения.

2. В нижней части главного окна приложения нажмите на кнопку **Отчеты**.

   Откроется окно **Отчеты**.

3. В левой части окна **Отчеты** выберите нужный тип отчета.

   В правой части окна отобразится отчет. Данные в отчетах представлены в виде таблицы, которая содержит список событий. Каждая строка в таблице содержит информацию об отдельном событии. Атрибуты события отображаются в столбцах таблицы. События, зарегистрированные в работе разных компонентов и задач, имеют разный набор атрибутов.

   По умолчанию события в отчете отсортированы по возрастанию значений столбца **Дата и время**. Для удобства работы с отчетами вы можете изменять представление данных на экране следующими способами:

   - фильтровать список событий по времени возникновения;
   - использовать функцию поиска определенного события.

4. Если вы хотите посмотреть подробную информацию о событии, выберите это событие в отчете.

   В нижней части окна отобразится блок, который содержит атрибуты этого события.

Сбор метрик о состоянии системы

Приложение Kaspersky Endpoint Security во время своей работы оказывает влияние на операционную систему. Для анализа происходящего предусмотрена возможность сбора метрик, связанных с производительностью приложения.

Анализировать метрики вы можете в системах визуализации данных, например Grafana. Экспортированные метрики можно публиковать в основные системы мониторинга, например Prometheus и Zabbix.

Настроить сбор метрик о ресурсах операционной системы, используемых приложением

```
kesl-control [-J] --export-metrics [--period <interval in seconds between outputs>|--interactive]
```

Где:

`--period` – периодический вывод результатов в командную строку (с указанием интервала вывода в секундах);

`--interactive` – интерактивный вывод (по нажатию клавиши **Enter**).

В результате выполнения команды в консоль будет выведен список метрик.

Список метрик

Внутреннее название метрики, метка и тип метрики	Описание и рекомендуемое пороговое значение
lfs_system_descriptor_opened_count Gauge	Количество дескрипторов, открытых в данный момент процессом kesl. Если рост количества дескрипторов превышает 250 за час, рекомендуется обратиться в Службу технической поддержки.
lfs_system_uptime_milliseconds Counter	Количество миллисекунд, прошедшее от запуска операционной системы до настоящего момента.

Внутреннее название метрики, метка и тип метрики	Описание и рекомендуемое пороговое значение
lfs_system_memory_usage_bytes метка type=virtual Gauge	Количество виртуальной памяти, используемой в данный момент процессом kesl. Рекомендуется выставить пороговое значение самостоятельно на основе данных системы. Получить данные можно самостоятельно или с помощью скрипта для сбора информации. За примером скрипта вы можете обратиться в Службу технической поддержки.
lfs_system_memory_usage_bytes метка type=resident Gauge	Количество резидентной памяти, используемой в данный момент процессом kesl. Рекомендуется выставить пороговое значение самостоятельно на основе данных системы. Получить данные можно самостоятельно или с помощью скрипта для сбора информации. За примером скрипта вы можете обратиться в Службу технической поддержки.
lfs_system_memory_usage_bytes метка type=swap Gauge	Количество памяти из области подкачки, используемой в данный момент процессом kesl. Рекомендуется выставить пороговое значение самостоятельно на основе данных системы. Получить данные можно самостоятельно или с помощью скрипта для сбора информации. За примером скрипта вы можете обратиться в Службу технической поддержки.
lfs_system_memory_wd_limits_bytes метка type=virtual Gauge	Ограничение на использование виртуальной памяти процессом kesl.
lfs_system_memory_wd_limits_bytes метка type=resident Gauge	Ограничение на использование резидентной памяти процессом kesl.
lfs_system_memory_wd_limits_bytes метка type=swap Gauge	Ограничение на использование памяти из файла подкачки процессом kesl.
lfs_system_cpu_usage_milliseconds метка type=user Counter	Количество миллисекунд процессорного времени, потребленное процессом kesl в пользовательском пространстве, от начала запуска процесса kesl и до настоящего момента. Рекомендуется выставить пороговое значение самостоятельно на основе данных системы. Получить данные можно самостоятельно или с помощью скрипта для сбора информации. За примером скрипта вы можете обратиться в Службу технической поддержки.
lfs_system_cpu_usage_milliseconds метка type=kernel Counter	Количество миллисекунд процессорного времени, потребленное процессом kesl в пространстве ядра, от начала запуска процесса kesl и до настоящего момента. Рекомендуется выставить пороговое значение самостоятельно на основе данных системы. Получить данные можно самостоятельно или с помощью скрипта для сбора информации. За примером скрипта вы можете обратиться в Службу технической поддержки.
lfs_system_cpu_usage_milliseconds метка type=total Counter	Количество миллисекунд процессорного времени, потребленное процессом kesl в пользовательском пространстве и в пространстве ядра, от начала работы процесса kesl и до настоящего момента. Если процессорное время процесса kesl превышает всю остальную нагрузку, рекомендуется обратиться в Службу технической поддержки.
lfs_tcpSynInterceptor_connection_hanging_count Counter	Общее количество зависших сетевых соединений на этапе установления соединения в сети TCP между сервером и клиентом от начала работы процесса kesl до настоящего момента (зависшими считаются сетевые соединения, ожидающие решение удаленного сервера по разрешению подключения от 1 секунды до 2 минут в зависимости от системного параметра /proc/sys/net/ipv4/tcp_syn_retries). Рост может быть обусловлен тем, что удаленный сервер недоступен или отсутствует. Если прирост количества зависших сетевых соединений больше 10 в минуту, рекомендуется обратиться в Службу технической поддержки.
lfs_tcpSynInterceptor_connection_count Gauge	Количество сетевых соединений, в данный момент ожидающих подключения к удаленному серверу.

Внутреннее название метрики, метка и тип метрики	Описание и рекомендуемое пороговое значение
lfs_tcpSynInterceptor_verdict_count метка verdict=allow Counter	Общее количество перехваченных соединений, которые удалось установить, от начала работы процесса kesl до настоящего момента.
lfs_tcpSynInterceptor_verdict_count метка verdict=drop Counter	Общее количество перехваченных соединений, для которых не удалось установить соединение, от начала работы процесса kesl до настоящего момента.
lfs_tcpSynInterceptor_verdict_count метка verdict=unknown Counter	Общее количество сетевых соединений от начала работы процесса kesl до настоящего момента с необрабатываемым решением удаленного сервера по разрешению подключения.
lfs_tcpSynInterceptor_verdict_latency_milliseconds Histogram	Гистограмма по времени принятия решения удаленного сервера по разрешению подключения от момента перехвата SYN-пакета до принятия решения для него.
lfs_tproxy_connection_count метка direction=inbound Gauge	Текущее количество входящих перехваченных сетевых соединений в данный момент.
lfs_tproxy_connection_count метка direction=outbound Gauge	Текущее количество исходящих перехваченных сетевых соединений в данный момент.
lfs_tproxy_connection_processed_count метка direction=inbound Counter	Общее количество входящих перехваченных сетевых соединений.
lfs_tproxy_connection_processed_count метка direction=outbound Counter	Общее количество исходящих перехваченных сетевых соединений.
lfs_tproxy_connection_orphaned_count Counter	Общее количество соединений (от начала работы компонентов Защита от веб-угроз, Защита от сетевых угроз и Веб-Контроль), перехваченных приложением Kaspersky Endpoint Security, хотя их перехват не планировался (например, из-за несовместимой конфигурации iptables или по причине того, что приложение не успело обработать новую конфигурацию перехвата). Такие соединения будут отклонены. Если общее количество таких соединений превышает 10, это может свидетельствовать о некорректной работе приложения или системы, рекомендуется обратиться в Службу технической поддержки.
lfs_tproxy_threadPool_task_count Counter	Общее количество задач (новое соединение, новая порция данных, данные отправлены и так далее), поступивших в пул потоков от начала работы компонентов Защита от веб-угроз, Защита от сетевых угроз и Веб-Контроль. Если разница между общим количеством задач и количеством выполненных задач неснижаемо растет, требуется добавить ресурсов, настроить исключения или обратиться в Службу технической поддержки.
lfs_tproxy_threadPool_thread_count Gauge	Количество потоков, обслуживающих MITM-механизм сетевого перехватчика. Потоки выделяются менеджером потоков для обработки соединений. Все потоки выполняют один и тот же код, в рамках которого они ожидают сетевых событий: новых соединений, новых пакетов в рамках зарегистрированных соединений.
lfs_tproxy_threadPool_thread_waiting Gauge	Количество свободных потоков из числа lfs_tproxy_threadPool_thread_count. Потоки, ждущие на poll в MITM-механизме сетевого перехватчика.
lfs_tproxy_threadPool_task_duration_milliseconds Histogram	Гистограмма по времени выполнения задач обработки перехваченных соединений. Если время выполнения 95% задач превышает 1 секунду, требуется добавить ресурсов, настроить исключения или обратиться в Службу технической поддержки.

Внутреннее название метрики, метка и тип метрики	Описание и рекомендуемое пороговое значение
lfs_tproxy_socket_count Gauge	Текущее количество сокетов (слушающие сокеты и сокеты соединений). Перехваченное соединение имеет 2 сокета соединений.
lfs_trafficScanning_object_hanging_count Gauge	Текущее количество зависших проверок объектов в перехваченном трафике (зависшими считаются проверки, длительность которых превышает 1 минуту). Если общее количество зависших проверок объектов больше 35, имеется проблема с базами приложения, рекомендуется обратиться в Службу технической поддержки.
lfs_trafficScanning_object_duration_milliseconds Histogram	Гистограмма по времени проверок объектов в перехваченном трафике. Если время проверок 95% объектов превышает 1 секунду, требуется добавить ресурсов, обновить базы приложения или обратиться в Службу технической поддержки. Если скорость прироста проверок пакетов в перехваченном трафике равна 0 и значение метрики lfs_tproxy_threadPool_task_count не равно 0, требуется обновить базы приложения или обратиться в Службу технической поддержки.
lfs_fileMonitor_cache_size Gauge	Текущий размер кеша File Monitor (кеш ревизий файлов), который отслеживает изменения файлов. Если текущий размер кеша File Monitor больше 50000, рекомендуется обратиться в Службу технической поддержки.
lfs_fileMonitor_cache_hit_count Counter	Число попаданий в кеш File Monitor (кеш ревизий файлов), который отслеживает изменения файлов.
lfs_fileMonitor_cache_miss_count Counter	Число кеш-промахов File Monitor (кеш ревизий файлов), который отслеживает изменения файлов.
lfs_faCache_file_count Gauge	Текущий размер кеша файлов перехватчика fanotify, не нуждающихся в проверке. Если текущий размер кеша файлов больше 100000, рекомендуется обратиться в Службу технической поддержки.
lfs_faCache_file_hit_count Counter	Число попаданий в кеш файлов перехватчика fanotify, не нуждающихся в проверке.
lfs_faCache_file_miss_count Counter	Число кеш-промахов файлов перехватчика fanotify, не нуждающихся в проверке.
lfs_faCache_volume_count Gauge	Текущий размер кеша точек монтирования перехватчика fanotify.
lfs_oas_cache_file_count Gauge	Текущий размер кеша файлов Защиты от файловых угроз, не нуждающихся в проверке. Если текущий размер кеша файлов больше 100000, рекомендуется обратиться в Службу технической поддержки.
lfs_oas_cache_file_hit_count Counter	Число попаданий в кеш файлов Защиты от файловых угроз, не нуждающихся в проверке.
lfs_oas_cache_file_miss_count Counter	Число кеш-промахов файлов Защиты от файловых угроз, не нуждающихся в проверке.
lfs_oas_cache_volume_count Gauge	Текущий размер кеша точек монтирования Защиты от файловых угроз.
lfs_processManager_cache_size Gauge	Текущее количество активных процессов в системе, находящихся в кеше.
lfs_processManager_cache_hit_count Counter	Число попаданий в кеш процессов в системе.
lfs_processManager_cache_miss_count Counter	Число кеш-промахов процессов в системе.

Внутреннее название метрики, метка и тип метрики	Описание и рекомендуемое пороговое значение
lfs_blockingProcessInterceptor_cache_size Gauge	Текущий размер кеша интерпретаторов, с помощью которых могут быть запущены процессы. Количество зависит от интенсивности запуска интерпретаторов на конкретном устройстве. Если текущий размер кеша файлов больше 10000, рекомендуется обратиться в Службу технической поддержки.
lfs_blockingProcessInterceptor_cache_hit_count Counter	Число попаданий в кеш интерпретаторов.
lfs_blockingProcessInterceptor_cache_miss_count Counter	Число кеш-промахов интерпретаторов.
lfs_doc_prevention_cache_file_count Gauge	Текущий размер кеша файлов задачи *Запрет запуска объектов* для объектов, не нуждающихся в проверке (при открытии документов).
lfs_script_prevention_cache_file_count Gauge	Текущий размер кеша файлов задачи *Запрет запуска объектов* для объектов, не нуждающихся в проверке (при запуске скриптов).
lfs_doc_prevention_cache_file_hit_count Counter	Число попаданий в кеш файлов задачи *Запрет запуска объектов* для объектов, не нуждающихся в проверке (при открытии документов).
lfs_script_prevention_cache_file_hit_count Counter	Число попаданий в кеш файлов задачи *Запрет запуска объектов* для объектов, не нуждающихся в проверке (при запуске скриптов).
lfs_doc_prevention_cache_file_miss_count Counter	Число кеш-промахов файлов задачи *Запрет запуска объектов* для объектов, не нуждающихся в проверке (при открытии документов).
lfs_script_prevention_cache_file_miss_count Counter	Число кеш-промахов файлов задачи *Запрет запуска объектов* для объектов, не нуждающихся в проверке (при запуске скриптов).
lfs_doc_prevention_cache_volume_count Gauge	Текущий размер кеша точек монтирования задачи Запрет запуска объектов для документов.
lfs_script_prevention_cache_volume_count Gauge	Текущий размер кеша точек монтирования задачи Запрет запуска объектов для скриптов.
eka_telemetry_metrics_registry_callbacks_exec_duration_milliseconds Gauge	Период времени, который заняло текущее обновление метрик всеми зарегистрированными в реестре клиентами (в миллисекундах).
eka_telemetry_metrics_registry_registered_callbacks Gauge	Текущее количество вызовов функций обновления метрик, которые выполнили MetricsRegistry для всех зарегистрированных клиентов.
eka_telemetry_metrics_registry_scrape_duration_milliseconds Gauge	Период времени, который занял сбор значений всех метрик реестра (в миллисекундах). Если 99% значений этой метрики больше 1 секунды в течение 10 минут, рекомендуется обратиться в Службу технической поддержки.

Мониторинг стабильности работы приложения

Мониторинг стабильности работы приложения Kaspersky Endpoint Security позволяет отслеживать количество нештатных остановок приложения и уведомлять администратора о нестабильной работе.

Как настроить мониторинг стабильности работы приложения в Web Console

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

   Откроется окно свойств политики.
3. Перейдите на вкладку **Параметры приложения**.

4. Выберите **Общие настройки** → **Производительность**.

5. Установите или снимите флажок **Включить мониторинг стабильности работы приложения**. По умолчанию флажок снят.

Как настроить мониторинг стабильности работы приложения в Консоли администрирования

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.

2. В рабочей области выберите вкладку **Политики**.

3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

4. Перейдите в раздел **Общие параметры** → **Параметры приложения**.

5. Установите или снимите флажок **Включить мониторинг стабильности работы приложения**. По умолчанию флажок снят.

Для применения параметра требуется перезапустить приложение и Агент администрирования.

Если приложение работает нестабильно, в свойствах устройства с установленным приложением отображается сообщение: *<Количество> нештатных остановок приложения начиная с <дата и время>*.

Как настроить мониторинг стабильности работы приложения в командной строке

В командной строке вы можете настраивать мониторинг стабильности работы приложения Kaspersky Endpoint Security с помощью параметров `TrackProductCrashes`, `ProductHealthLogFile`, `WarnThreshold`, `WarnAfter_#_crash` и `WarnRemovingThreshold` в конфигурационном файле kesl.ini.

Параметр `TrackProductCrashes` позволяет включить отправку статуса устройства от приложения Kaspersky Endpoint Security в Kaspersky Security Center при нестабильной работе приложения. Параметр может принимать следующие значения:

- `Yes/true` – включить отправку статуса устройства от приложения Kaspersky Endpoint Security в Kaspersky Security Center.

- `No/false` – выключить отправку статуса устройства от приложения Kaspersky Endpoint Security в Kaspersky Security Center.

Параметр `ProductHealthLogFile` позволяет задать путь к файлу, с помощью которого осуществляется мониторинг стабильности приложения. Значение по умолчанию: /var/opt/kaspersky/kesl/private/kesl_health.log.

Параметр `WarnThreshold` позволяет задать интервал времени (в секундах), за который приложение должно посчитать количество нештатных остановок, прежде чем вывести уведомление о нестабильной работе. Значение по умолчанию: 3600 секунд.

Параметр `WarnRemovingThreshold` позволяет задать интервал времени (в секундах), по истечении которого статус о нестабильной работе приложения будет снят. Значение по умолчанию: 86400 секунд.

Параметр `WarnAfter_#_crash` позволяет задать количество нештатных остановок приложения, по достижении которого отображается уведомление о нестабильной работе приложения. Параметр может принимать значения от 0 до 10. Значение по умолчанию: 10. Если указано значение 0, уведомление о нестабильной работе приложения не отображается.

После внесения изменений в файл перезапустите Kaspersky Endpoint Security.

Проверка целостности компонентов приложения

Приложение Kaspersky Endpoint Security содержит множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленники могут заменить один или несколько исполняемых модулей или файлов приложения другими файлами, содержащими вредоносный код. Чтобы предотвратить такую замену модулей и файлов, в приложении Kaspersky Endpoint Security предусмотрена проверка целостности компонентов приложения. Приложение проверяет модули и файлы на наличие неавторизованных изменений и повреждений. Если модуль или файл приложения имеет некорректную контрольную сумму, то он считается поврежденным.

Проверка целостности выполняется для следующих компонентов приложения, если они установлены на устройстве:

- пакет приложения;
- пакет графического пользовательского интерфейса;
- пакет Агента администрирования Kaspersky Security Center;
- веб-плагин управления Kaspersky Endpoint Security;
- MMC-плагин управления Kaspersky Endpoint Security.

Проверка целостности компонентов приложения выполняется с помощью утилиты проверки целостности. Утилита проверяет целостность файлов, перечисленных в специальных списках, которые называются *файлы манифеста*. Для каждого компонента приложения существует свой файл манифеста, содержащий список файлов приложения, целостность которых важна для корректной работы этого компонента приложения. Файлы манифеста подписаны цифровой подписью, их целостность также проверяется.

Для запуска утилиты проверки целостности на устройствах с операционными системами Linux требуется учетная запись с root-правами.

Утилита проверки целостности устанавливается вместе с приложением и расположена по следующим путям:

- В составе пакета приложения (integrity_checker): /opt/kaspersky/kesl/bin/integrity_checker.
- В составе MMC-плагина управления Kaspersky Endpoint Security (integrity_checker.exe):
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<номер версии>.plg\integrity_checker.exe – для 32-битных операционных систем;
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<номер версии>.plg\integrity_checker.exe – для 64-битных операционных систем.

Файлы манифеста расположены по следующим путям:

- Для проверки целостности пакета приложения: /opt/kaspersky/kesl/bin/integrity_check.xml.
- Для проверки целостности пакета графического пользовательского интерфейса: /opt/kaspersky/kesl/bin/gui_integrity_check.xml.
- Для проверки Агента администрирования:
  - /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml – для 32-битных операционных систем;
  - /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml – для 64-битных операционных систем.
- Для проверки MMC-плагина управления Kaspersky Endpoint Security
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<версия плагина>.plg\integrity_check.xml – для 32-битных операционных систем;
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<версия плагина>.plg\integrity_check.xml – для 64-битных операционных систем.

Чтобы проверить целостность компонента решения, вам нужно запустить утилиту из папки расположения утилиты для этого компонента.

Проверить целостность пакета приложения

```
integrity_checker [<path to manifest file>] --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
```

Проверить целостность пакета графического пользовательского интерфейса

```
integrity_checker <path to manifest file> --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
```

Проверить целостность MMC-плагина управления Kaspersky Endpoint Security

```
integrity_checker.exe [<path to manifest file>]
```

Проверить целостность Агента администрирования

```
integrity_checker <path to manifest file>
```

По умолчанию используется путь к файлу манифеста, расположенному в той же директории, в которой расположена утилита проверки целостности.

Вы можете запустить утилиту со следующими необязательными параметрами:

- `--crl <directory>` – путь к директории, содержащей список отозванных сертификатов (Certificate Revocation List).
- `--verbose` – детализировать вывод информации о выполненных действиях и результатах. Если вы не укажете этот параметр, будут отображаться только ошибки, объекты, не прошедшие проверку, и общая статистика проверки.
- `--trace <file name>` – записывать в указанный файл события, произошедшие во время проверки, с уровнем детализации DEBUG.
- `--signature-type kds` – тип проверяемой сигнатуры (этот параметр является обязательным для проверки веб-плагина управления Kaspersky Endpoint Security).
- `--signature-type kds-with-filename` – тип проверяемой сигнатуры (этот параметр является обязательным для проверки пакета приложения и пакета графического интерфейса).
- `--single_file <file name>` – проверить только указанный файл, входящий в состав манифеста, остальные объекты манифеста игнорировать.
- `--version` – отобразить версию утилиты и не выполнять проверку целостности.

Посмотреть все доступные параметры утилиты проверки целостности

```
integrity_checker --help
```

Результат проверки файла манифеста отображается в следующем виде:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата 0).
- `FAILED` – целостность файлов не подтверждена (код возврата отличен от 0).

Если при запуске приложения обнаружено нарушение целостности приложения или Агента администрирования, приложение Kaspersky Endpoint Security формирует событие об этом в журнале событий и в Kaspersky Security Center.

Управление доступом к приложению

Управление доступом к Kaspersky Endpoint Security построено на политике Role Based Access Control (RBAC). Чтобы предоставить пользователю определенные права или доступ к ресурсу, нужно назначить ему соответствующие роли. *Роль* – это набор прав и разрешений на управление приложением.

Применение ролей пользователей облегчает и сокращает рутинные действия по настройке прав доступа пользователей к приложению. Права доступа в роли настраивают в соответствии с типовыми задачами и служебными обязанностями пользователей.

Для обеспечения защиты устройств приложению необходимы повышенные привилегии в операционной системе. Приложение выполняет основные защитные функции в том числе и с привилегиями пользователя root.

В рамках ролевой модели приложения существует роль Администратор (admin). При этом действия пользователей, обладающих ролью Администратор, в отдельных случаях могут приводить к выполнению операций с использованием привилегий пользователя root операционной системы.

Роль Администратор должна предоставляться только доверенным пользователям. Компрометация или недобросовестное использование роли Администратор ведет к компрометации всего устройства и может оказать влияние на безопасность, целостность или работоспособность инфраструктуры вашей организации, а также пользовательских данных.

Назначение роли Администратор является ответственностью владельца системы и должно осуществляться в соответствии с принятыми в вашей организации правилами разграничения доступа и уровнем доверия к пользователям.

Предустановленные роли

Доступ к функциям приложения Kaspersky Endpoint Security через командную строку предоставляется пользователю в соответствии с его ролью. *Роль* – это набор прав и разрешений на управление приложением.

В операционной системе создаются четыре группы пользователей системы:

- kesladmin;
- kesluser;
- keslaudit;
- nokesl.

Когда роль в приложении назначается пользователю системы, этот пользователь добавляется в соответствующую группу (см. таблицу ниже). При отзыве роли у пользователя пользователь удаляется из соответствующей группы.

После назначения или отзыва роли необходимо перезапустить приложение (процесс kesl) и его графический интерфейс (процесс kesl-gui).

Роли и группы пользователей

Название роли	Роль в приложении	Группа пользователей ОС	Права
Администратор	admin	kesladmin	Управление параметрами приложения и параметрами задач через графический интерфейс и командную строку приложения без использования команды `sudo`. Управление лицензированием приложения. Назначение ролей пользователям. Отзыв ролей у пользователей (администратор не имеет права отозвать роль admin у себя самого). Просмотр и управление хранилищами пользователей.
Пользователь	user	kesluser	Управление только задачами выборочной проверки файлов. Запуск и остановка задач обновления. Отправка файлов на проверку в Sandbox. Просмотр отчетов для созданных пользователем задач. Просмотр особых событий, общих для всех пользователей приложения.

Название роли	Роль в приложении	Группа пользователей ОС	Права
Аудитор	audit	keslaudit	Просмотр параметров приложения. Просмотр статуса приложения. Просмотр всех задач, их параметров и расписания запуска. Просмотр всех событий. Просмотр всех объектов в резервном хранилище.
–	–	nokesl	Роль в приложении не назначена, права отсутствуют.

Как назначить или отозвать роль пользователя

Роли определяют набор прав и доступных действий пользователя в системе. Управлять ролями могут только пользователи с ролью Администратор (kesladmin). На защищаемом устройстве рекомендуется определить как минимум одного пользователя с ролью Администратор, чтобы предотвратить управление приложением пользователями, обладающими привилегиями root.

Просмотр списка пользователей и ролей

```
kesl-control --get-user-list
```

Назначить роль пользователю

```
kesl-control --grant-role <admin|user|audit> <user name>
```

Пример назначения роли audit пользователю test15

```
kesl-control --grant-role audit test15
```

Отозвать роль у пользователя

```
kesl-control --revoke-role <role> <user name>
```

Пример отзыва роли audit у пользователя test15

```
kesl-control --revoke-role audit test15
```

Функциональные области RBAC в Kaspersky Security Center

По умолчанию пользователи с ролью "Администратор Kaspersky Endpoint Security" в системе администрирования Kaspersky Security Center имеют доступ ко всем функциям Kaspersky Endpoint Security.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Endpoint Security один из следующих предустановленных уровней доступа к функциям Kaspersky Endpoint Security:

- **Чтение** – возможность просматривать общие параметры работы Kaspersky Endpoint Security и параметры работы компонентов Kaspersky Endpoint Security.
- **Изменение** – возможность просматривать и изменять общие параметры работы Kaspersky Endpoint Security и параметры работы компонентов Kaspersky Endpoint Security.

- **Выполнение** – возможность запускать и останавливать задачи Kaspersky Endpoint Security.
- **Выполнение операций с выборками устройств** – возможность запускать и останавливать задачи Kaspersky Endpoint Security для выборки устройств.

Также вы можете выполнять расширенную настройку прав доступа: разрешать или запрещать доступ к функциям Kaspersky Endpoint Security.

Как настроить права доступа к функциям приложения в Web Console

1. В главном окне Web Console выберите **Пользователи и роли** → **Роль**.
2. Выберите роль, функциональные области которой вы хотите настроить.

   Если требуется, вы можете добавить новую роль. Подробнее см. в справке Kaspersky Security Center.
3. Настройте права доступа к приложению Kaspersky Endpoint Security.
4. Нажмите на кнопку **Сохранить**.

Права доступа к функциям Kaspersky Endpoint Security

Функциональная область	Функции Kaspersky Endpoint Security
Базовая функциональность	Обновление баз и модулей приложения Откат обновления баз Инвентаризация Защита от атак badUSB Контроль целостности системы Проверка целостности системы Настройки обнаружения Kaspersky Security Network Взаимодействие с пользователем Производительность Настройки сети Проверка контейнеров Служба технической поддержки Отчеты и хранилище Интеграция с KSC Источник телеметрии и режим работы auditd (Настройки взаимодействия с ОС) Настройки уведомлений Режим Легкого агента Добавление ключа
Контроль приложений	Контроль приложений
Контроль устройств	Контроль устройств
Шифрование данных	Предоставление временного доступа к устройству (Контроль устройств)
Доверенная зона	Доверенная зона: • доверенные веб-адреса; • доверенные IP-адреса; • контролируемые порты; • доверенные корневые сертификаты; • доверенные домены; • доверенные точки монтирования; • исключения из перехвата трафика • доверенные приложения; • исключения из Поиска вредоносного ПО; • доверенные устройства.

Функциональная область	Функции Kaspersky Endpoint Security
Detection and Response	Встроенные агенты: • Managed Detection and Response; • Endpoint Detection and Response; • Endpoint Detection and Response Expert (on-premises); • Endpoint Detection and Response Expert (cloud); • Network Detection and Response (KATA); • Sandbox; • Интеграция с KUMA. Действия по реагированию: • Завершение процесса; • Запуск процесса; • Поиск IOC; • Получение файла с устройства; • Помещение файла на карантин; • Удаление файла с устройства; • Сетевая изоляция; • Запрет запуска объектов; • Настройки телеметрии.
Предотвращение вторжений	Анализ поведения Защита от эксплойтов Защита от шифрования Защита от сетевых угроз Управление сетевым экраном
Компоненты защиты	Поиск вредоносного ПО Проверка важных областей Защита от файловых угроз Защита от почтовых угроз Проверка съемных дисков Защита от веб-угроз
Веб-Контроль	Веб-Контроль

Рекомендации для типовых ролей защищаемых устройств

Рабочая станция

Если вы устанавливаете приложение на рабочую станцию, рекомендуется также установить графический интерфейс приложения.

После установки приложения:

- Включите Защиту от веб-угроз.
- Если устройство не имеет прямого выхода в интернет, выберите локальный способ проверки сертификатов в параметрах проверки сетевого трафика одним из следующих способов:
  - В Web Console в блоке **Проверка защищенных соединений** нажмите на кнопку **Настройки**, а затем установите для параметра **Политика проверки сертификатов** значение **Локальная проверка**.
  - В Консоли администрирования в блоке **Параметры зашифрованных соединений** установите для параметра **Политика проверки сертификатов** значение **Локальная проверка**.

- Локально на устройстве с помощью командной строки:

```
kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
```

Приложение не будет использовать интернет для проверки сертификатов.

- Настройте исключение из перехвата файловых операций (глобальное исключение) для всех удаленных директорий, смонтированных на устройстве с помощью протоколов Samba и NFS.

Файловый сервер

После установки приложения:

1. Убедитесь, что в параметрах Защиты от файловых угроз выключена проверка архивов. Это значение установлено по умолчанию.

2. Создайте задачу *Поиск вредоносного ПО* со следующими параметрами:

   - проверка архивов – включена;

   - расписание запуска задачи – в часы минимальной нагрузки на устройство.

Веб-сервер

Приложение Kaspersky Endpoint Security не предназначено для защиты веб-серверов. Для защиты веб-серверов рекомендуется использовать Kaspersky NGFW и Kaspersky Web Traffic Security.

Если вы используете Kaspersky Endpoint Security на веб-сервере, при работе по протоколу HTTPS и высокой клиентской нагрузке на сервер Защита от веб-угроз может значительно увеличивать потребление системных ресурсов. Это происходит из-за того, что приложение расшифровывает и проверяет HTTPS-трафик.

Проанализируйте, как изменяется нагрузка на веб-сервер во время работы Защиты от веб-угроз. Вы можете настроить исключения, чтобы подобрать оптимальные настройки и устранить проблемы совместимости.

Прокси-сервер

После установки приложения выключите компоненты Защита от веб-угроз и Защита от сетевых угроз на устройстве, выполняющем функции прокси-сервера или балансировщика нагрузки.

Сервер с контейнеризацией

После установки приложения выключите компоненты Защита от веб-угроз, Защита от сетевых угроз и Управление сетевым экраном на серверах, которые используются для сервисов контейнеризации. Для защиты контейнерных сред вы можете использовать приложение Kaspersky Container Security.

Сервер СУБД

Настройте глобальные исключения для рабочих директорий СУБД.

Список рабочих директорий в вашей инфраструктуре уточните у администратора СУБД.

Ниже приведены примеры директорий для операционной системы Ubuntu. В других операционных системах директории могут отличаться.

Рекомендации для популярных СУБД

PostgreSQL. Критически важно полностью исключить задержки в файловых операциях с файлами данных и журналами предзаписи (WAL-файлами). Рекомендуем дополнительно исключить из проверки файловые операции процессов PostgreSQL и табличные пространства (см. пример ниже). При типовой установке PostgreSQL эти файлы находятся в следующих директориях:

- статистика и параллельные запросы: `/dev/shm`
- данные: `/var/lib/postgresql/<PostgreSQL version>/main`
- WAL-файлы: `/var/lib/postgresql/<PostgreSQL version>/main/pg_wal`
- исполняемые файлы: `/usr/lib/postgresql/<PostgreSQL version>/bin/`

Postgres Pro. Выполните рекомендации, указанные для PostgreSQL. Дополнительно добавьте в исключения директорию `/var/lib/pgpro/<Postgres Pro version>/data`.

Oracle Database. Список рабочих директорий всех баз данных можно получить из конфигурационного файла `/etc/oratab`.

ScyllaDB. При работе компонентов Защита от веб-угроз и Защита от сетевых угроз используйте для перехвата трафика режим eBPF. Для управления режимом работы кеша событий решений Detection and Response используйте значение по умолчанию для параметра `UseIncreasedXdrEventsCache=yes` в конфигурационном файле kesl.ini.

Пример настройки глобальных исключений для рабочих директорий PostgreSQL

Если для перехвата системных событий вы используете механизм на основе *технологии fanotify*, необходимо чтобы директории файлов СУБД являлись точками монтирования. Если для перехвата системных событий вы используете механизм на основе *обновляемого модуля ядра*, создавать точки монтирования не нужно.

Чтобы создать точки монтирования:

1. Проверьте, являются ли директории файлов СУБД точками монтирования:

```
mount
```

Если директорий нет в выводе команды mount:

a. Создайте точку монтирования:

```
mount --bind /var/lib/postgresql/<PostgreSQL version>/main/ /var/lib/postgresql/<PostgreSQL version>/main
```

Создавать отдельную точку монтирования для директории с WAL-файлами не нужно, она вложена в директорию данных.

b. Добавьте следующую строку в файл /etc/fstab, чтобы созданная точка монтирования осталась в системе после перезагрузки:

```
/var/lib/postgresql/<PostgreSQL version>/main /var/lib/postgresql/<PostgreSQL version>/main none
defaults,bind 0 0
```

2. Перезапустите службу PostgreSQL:

```
systemctl restart postgresql
```

Чтобы настроить глобальные исключения для рабочих директорий:

1. Добавьте директории в глобальные исключения:

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=/var/lib/postgresql/<PostgreSQL version>/main
kesl-control --set-app-settings ExcludedMountPoint.item_0001=/var/lib/postgresql/<PostgreSQL
version>/main/pg_wal
kesl-control --set-app-settings ExcludedMountPoint.item_0002=/usr/lib/postgresql/<PostgreSQL version>/bin/
kesl-control --set-app-settings ExcludedMountPoint.item_0003=/usr/lib/postgresql/<PostgreSQL version>
```

2. Если вы используете табличные пространства, также добавьте их в исключения:

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=<tablespace directory>
```

3. Перезапустите приложение, чтобы применить глобальные исключения:

```
systemctl restart kesl
```

Обновление баз и модулей приложения

Обновление баз и модулей приложения Kaspersky Endpoint Security обеспечивает актуальность защиты устройства. Каждый день в мире появляются новые вирусы и другие приложения, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули приложения.

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

Если развертывание приложения прошло успешно и вы выбрали обновление баз на этапе первоначальной настройки, то после установки приложения базы обновлены и актуальны. Вы можете получить информацию о состоянии баз при просмотре состояния защиты устройства в Kaspersky Security Center с помощью статусов клиентских устройств и в командной строке с помощью команды `kesl-control --app-info`. Если базы не актуальны, вам нужно настроить и запустить обновление баз.

Настройка обновления баз и модулей

1. **Выбор схемы распространения обновлений и источника обновлений**

   Источник обновлений – это ресурс, содержащий обновления баз и модулей приложения Kaspersky Endpoint Security. Источником обновлений могут быть серверы обновлений "Лаборатории Касперского", хранилище Сервера администрирования Kaspersky Security Center, FTP-, HTTP- или HTTPS-серверы, локальная или сетевая директория, смонтированная пользователем по протоколу Samba или NFS.

   > Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, обновление баз на защищенных виртуальных машинах выполняется из директории на SVM.

2. **Настройка задачи обновления баз**

   Загрузка пакета обновлений и установка обновлений баз и модулей приложения на устройстве выполняются с помощью задачи *Обновление*.

> Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) может быть недоступна в приложении на территории США.

В процессе обновления на ваше устройство загружаются и устанавливаются следующие объекты:

- Базы Kaspersky Endpoint Security. Базы приложения включают в себя правила обнаружения вредоносных программ, описание сетевых атак, базы вредоносных и фишинговых веб-адресов, базы баннеров, спам-базы и другие данные.
- Модули приложения. Обновления модулей предназначены для устранения уязвимостей в приложении и улучшения методов защиты устройства. Обновления модулей могут менять поведение компонентов приложения и добавлять новые возможности.

Также вы можете получать автоматически устанавливаемые обновления приложения (автопатчи). Автопатчи содержат исправления и улучшения в работе приложения.

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

> Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт). Объем занимаемого дискового пространства может достигать 3 ГБ.

Полезные статьи

Решение проблем с обновлением баз и модулей приложения

Что делать со статусом "Установка обновления версии приложения или модуля cryptossl завершена. Перезапустите приложение"

Как выбрать источник и схему распространения обновлений

Выбор источника обновлений Kaspersky Endpoint Security

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

Источником обновлений могут быть серверы обновлений "Лаборатории Касперского", хранилище Сервера администрирования Kaspersky Security Center, локальная или сетевая директория (SMB/NFS), смонтированная пользователем, FTP-, HTTP- или HTTPS-серверы. При выборе собственного HTTPS-сервера в качестве источника обновления вам нужно убедиться, что он имеет корректную цепочку сертификатов. Использование самоподписанного сертификата возможно только в качестве корневого в цепочке сертификатов. В этом случае его требуется добавить в список доверенных сертификатов на устройстве.

> Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, обновление баз на защищенных виртуальных машинах выполняется из директории на SVM.

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 из первого доступного источника обновлений. Вы можете настраивать время ожидания ответа от выбранного источника обновлений при попытке соединения с ним. Если в течение указанного времени от источника обновлений не приходит ответ, приложение обращается к другому указанному источнику обновлений.

Выбор схемы распространения обновлений

Приложение Kaspersky Endpoint Security поддерживает следующие схемы распространения обновлений баз и модулей приложения:

Централизованное обновление

Если вы используете Kaspersky Security Center для централизованного управления защитой устройств в вашей организации, мы рекомендуем настроить централизованное обновление баз. 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.

   В качестве хранилища вы можете использовать хранилище Сервера администрирования Kaspersky Security Center. Загрузку пакета обновлений в хранилище Сервера администрирования обеспечивает задача Сервера администрирования *Загрузка обновлений в хранилище Сервера администрирования*.

2. Распространение пакета обновлений на клиентские устройства.

   Распространение пакета обновлений на клиентские устройства обеспечивает задача приложения Kaspersky Endpoint Security *Обновление*. В параметрах задачи вам нужно выбрать Kaspersky Security Center в качестве источника обновлений.

Обновление с серверов обновлений "Лаборатории Касперского"

Серверы обновлений "Лаборатории Касперского" расположены в разных странах по всему миру, что обеспечивает высокую надежность обновления. Если обновление не может быть выполнено с одного сервера, приложение переключается к следующему серверу. Обновления загружаются по протоколу HTTPS. Подробнее о серверах обновлений "Лаборатории Касперского" см. в базе знаний Службы технической поддержки.

Обновление из локальной или сетевой директории (SMB/NFS), смонтированной пользователем, или с FTP-, HTTP- или HTTPS-сервера

Пользовательский источник обновлений должен содержать предварительно скачанные пакеты обновлений (например, с помощью Kaspersky Update Utility). При выборе собственного HTTPS-сервера в качестве источника обновления вам нужно убедиться, что он имеет корректную цепочку сертификатов. Использование самоподписанного сертификата возможно только в качестве корневого в цепочке сертификатов. В этом случае его требуется добавить в список доверенных сертификатов на устройстве. Вы можете указать пользовательский источник обновлений в параметрах задачи *Обновление*. Подробнее о создании пользовательских источников обновлений см. в справке Kaspersky Security Center.

Загрузка обновлений с серверов обновлений "Лаборатории Касперского" или с других FTP-, HTTP- или HTTPS-серверов осуществляется по стандартным сетевым протоколам. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, укажите настройки прокси-сервера.

Как настроить задачу обновления баз

Загрузка пакета обновлений и установка обновлений баз и модулей приложения на устройстве выполняются с помощью задачи *Обновление*.

Обновление баз в Kaspersky Security Center

В Kaspersky Security Center задача *Обновление* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Обновление* во время работы мастера требуется установить плагин управления Kaspersky Endpoint Security.

Вы можете использовать автоматически созданную групповую задачу *Обновление*, а также создавать и запускать пользовательские групповые и локальные задачи обновления с помощью Web Console или Консоли администрирования.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, обновление баз на защищенных виртуальных машинах выполняется с помощью специальной локальной задачи *Обновление*, в которой в качестве источника обновлений указана директория на SVM. Задача обновления запускается автоматически. Вы не можете удалять эту задачу и изменять ее параметры. Обновление баз и модулей приложения с помощью задач, созданных в Kaspersky Security Center, не поддерживается.

Как настроить и запустить задачу обновления в Web Console

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

   Откроется список задач.

2. В списке задач выберите задачу обновления Kaspersky Endpoint Security и нажмите на название задачи.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. В разделе **Источники обновлений** выберите в таблице источник, из которого приложение будет получать обновления баз и модулей, в зависимости от используемой схемы обновления.

   Список источников обновлений содержит два источника: серверы обновлений "Лаборатории Касперского" и Kaspersky Security Center. В столбце **Статус** отображается, использует ли приложение этот источник обновлений при выполнении задачи. Вы можете добавить в список другие источники обновлений, нажав на кнопку **Добавить**. В качестве источников обновлений вы можете указывать FTP-, HTTP- или HTTPS-серверы или директории на любом смонтированном устройстве защищаемого клиентского устройства, включая директории на удаленных устройствах, смонтированные по протоколам Samba или NFS. Если обновление не может быть выполнено из одного источника обновлений, приложение Kaspersky Endpoint Security переключается к следующему источнику. Приложение обращается к источникам обновлений в том порядке, в котором они указаны в таблице.

5. В окне свойств задачи выберите вкладку **Расписание** и настройте расписание запуска задачи обновления. По умолчанию выбран запуск задачи в ручном режиме.

   Если в качестве источника обновлений вы выбрали **Kaspersky Security Center**, в раскрывающемся списке **Запуск задачи** выберите **При загрузке обновлений в хранилище**. Подробнее о расписании задач см. в справке Kaspersky Security Center.

6. Сохраните внесенные изменения.

Задача будет запускаться в соответствии с настроенным расписанием. Вы также можете запускать задачу вручную.

Как настроить и запустить задачу обновления в Консоли администрирования

1. В Консоли администрирования выполните одно из следующих действий:

   - Если вы хотите изменить параметры задачи, которая выполняется на устройствах, входящих в определенную группу администрирования, в дереве консоли выберите эту группу администрирования, затем в рабочей области выберите вкладку **Задачи**.

   - Если вы хотите изменить параметры задачи, которая выполняется на одном или нескольких устройствах (задачи для набора устройств), в дереве консоли выберите папку **Задачи**.

2. В списке задач выберите нужную задачу обновления и откройте окно свойств задачи двойным щелчком мыши.

3. В окне свойств задачи в списке слева выберите раздел **Источники обновлений.**

4. Выберите в таблице источник обновлений, из которого приложение будет получать обновление баз и модулей, в зависимости от используемой схемы обновления.

   Список источников обновлений содержит два источника: серверы обновлений "Лаборатории Касперского" и Kaspersky Security Center. В столбце **Статус** отображается, использует ли приложение этот источник обновлений при выполнении задачи. Вы можете добавить в список другие источники обновлений, нажав на кнопку **Добавить**. В качестве источников обновлений вы можете указывать FTP-, HTTP- или HTTPS-серверы. Если обновление не может быть выполнено из одного источника обновлений, приложение Kaspersky Endpoint Security переключается к следующему источнику. Приложение обращается к источникам обновлений в том порядке, в котором они указаны в таблице.

5. Выберите раздел **Параметры** и настройте другие параметры обновления.

6. Выберите вкладку **Расписание** и настройте расписание запуска задачи обновления. По умолчанию выбран запуск задачи в ручном режиме.

   Если в качестве источника обновлений вы выбрали **Kaspersky Security Center**, в раскрывающемся списке **Запуск по расписанию** выберите **При загрузке обновлений в хранилище**. Подробнее о расписании задач см. в справке Kaspersky Security Center.

7. Нажмите на кнопку **Применить** или на кнопку **OK** в окне **Свойства: <Название задачи>**, чтобы сохранить внесенные изменения.

Задача будет запускаться в соответствии с настроенным расписанием. Вы также можете запускать задачу вручную.

Обновление баз в командной строке

В командной строке вы можете выполнять обновление баз и модулей приложения с помощью предустановленной задачи *Обновление* (`Update`), а также создавать пользовательские задачи обновления (задач типа `Update`).

Вы можете управлять задачами обновления вручную (запускать, останавливать, приостанавливать и возобновлять), настраивать расписание запуска задач и настраивать параметры обновления, изменяя параметры задач.

Как создать и настроить задачу обновления в командной строке

В командной строке вы можете создать и настроить пользовательскую задачу обновления двумя способами:

- создать задачу, указав все параметры для нее в конфигурационном файле;
- создать задачу с параметрами по умолчанию, а затем настроить ее параметры.

```
Создать и настроить задачу обновления с параметрами, указанными в конфигурационном файле

kesl-control --create-task <task name> --type <task type> --file <path to file> [--json]
```

Где:

- `<path to file>` – полный путь к конфигурационному файлу, параметры из которого будут использоваться при создании задачи;
- `--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

  Пример конфигурационного файла:

  ```
  ConnectionTimeout=10
  ApplicationUpdateMode=DownloadOnly
  [Sources.item_0000]
  Enabled=Yes
  SourceType=Custom
  URL=https://s00.upd.kaspersky.com
  ```

Чтобы создать и настроить задачу обновления с параметрами по умолчанию:

1. Создайте задачу, выполнив команду:

   ```
   kesl-control --create-task <update task name> --type Update
   ```

   Где `<update task name>` – имя, которое вы задаете для новой задачи обновления.

   В результате выполнения команды приложение создаст задачу обновления с параметрами по умолчанию.

2. При необходимости настройте параметры задачи обновления, выполнив команду:

   ```
   kesl-control --set-settings <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

3. При необходимости настройте параметры расписания запуска задачи, выполнив команду:

   ```
   kesl-control --set-schedule <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

4. Проверьте текущие значения параметров задачи, выполнив команду:

   ```
   kesl-control --get-settings <update task ID|name>
   ```

Обновление баз в графическом интерфейсе приложения

Как запустить или остановить задачу обновления в графическом интерфейсе

1. Откройте главное окно графического интерфейса приложения.
2. В главном окне приложения нажмите на кнопку **Обновление**.

   Откроется окно **Обновление**.

3. Выполните одно из следующих действий:

   - Если вы хотите запустить задачу, нажмите на кнопку **Запустить**, расположенную под той задачей, которую вы хотите запустить.

     Отобразится ход выполнения задачи обновления.

   - Если вы хотите остановить задачу, нажмите на кнопку **Остановить**, расположенную под той задачей, которую вы хотите остановить.

     Задача обновления остановится.

4. Если вы хотите просмотреть отчет по задаче, нажмите на кнопку **Показать отчет**.

Как выполнить обновление с помощью Kaspersky Update Utility

Для экономии интернет-трафика вы можете настроить обновление баз и модулей приложения на устройствах локальной сети организации из общей директории с помощью утилиты Kaspersky Update Utility. Для этого одно из устройств локальной сети организации должно получать пакеты обновлений с Сервера администрирования Kaspersky Security Center или с серверов обновлений "Лаборатории Касперского" и копировать полученные пакеты обновлений в общую директорию с помощью утилиты. Остальные устройства локальной сети организации смогут получать пакет обновлений из общей директории.

Чтобы настроить в Kaspersky Security Center обновление баз из общей директории с помощью утилиты Kaspersky Update Utility:

1. Установите Kaspersky Update Utility на одном из устройств локальной сети организации.

   Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта службы технической поддержки "Лаборатории Касперского".

2. Настройте копирование пакета обновлений в общую директорию в параметрах Kaspersky Update Utility.

   Выберите источник обновлений (например, хранилище Сервера администрирования) и общую директорию, в которую Kaspersky Update Utility будет копировать пакеты обновлений. Дополнительная информация о работе с Kaspersky Update Utility приведена в Базе знаний "Лаборатории Касперского".

3. Настройте обновление баз и модулей приложения из указанной общей директории на остальных устройствах локальной сети организации:

   a. Откройте свойства задачи **Обновление**, которая будет выполняться на нужном устройстве, с помощью Web Console или с помощью Консоли администрирования.

   b. В свойствах задачи перейдите в раздел **Источники обновлений**.

   c. В блоке **Источники обновлений** выберите вариант **Другие источники в локальной или глобальной сети**.

   d. В таблице источников обновлений нажмите на кнопку **Добавить** и укажите путь к общей директории.

   > Адрес источника обновлений должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.

   e. Установите флажок **Использовать этот источник** и нажмите на кнопку **OK**.

f. В таблице источников обновлений настройте порядок их использования с помощью кнопок **Вверх** и **Вниз**.

g. Сохраните изменения параметров задачи.

Чтобы настроить в командной строке обновление баз из общей директории с помощью утилиты Kaspersky Update Utility:

1. Установите Kaspersky Update Utility на одном из устройств локальной сети организации.

   Вы можете загрузить дистрибутив Kaspersky Update Utility с веб-сайта службы технической поддержки "Лаборатории Касперского".

2. Настройте копирование пакета обновлений в общую директорию в параметрах Kaspersky Update Utility.

   Выберите источник обновлений (например, хранилище Сервера администрирования) и общую директорию, в которую Kaspersky Update Utility будет копировать пакеты обновлений. Дополнительная информация о работе с Kaspersky Update Utility приведена в Базе знаний "Лаборатории Касперского".

3. Настройте обновление баз и модулей приложения из указанной общей директории на остальных устройствах локальной сети организации: в параметрах задачи `Update` задайте значение параметра `SourceType=Custom` и укажите путь к общей директории в секции `[Sources.item_#]`.

   Адрес источника обновлений должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.

Как откатить обновление баз и модулей приложения

После второго обновления баз и модулей приложения становится доступна функция отката к предыдущим базам и модулям приложения.

Каждый раз, когда пользователь запускает обновление, Kaspersky Endpoint Security создает резервную копию используемых баз и модулей приложения и только потом приступает к их обновлению. Это позволяет вернуться к использованию предыдущих баз и модулей приложения при необходимости. Возможность отката последнего обновления полезна, например, в случае, если новая версия баз вызывает ложное срабатывание, из-за которого Kaspersky Endpoint Security блокирует безопасное приложение.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, откат обновления баз с помощью задачи не поддерживается.

В Kaspersky Security Center вы можете создавать задачи отката обновления для групп администрирования или отдельных устройств с помощью Web Console или Консоли администрирования.

В командной строке вы можете откатить обновление баз следующими способами:

- Запустить предустановленную задачу *Откат обновления баз (Rollback)*.
- Создать и запустить пользовательскую задачу *Откат обновления баз (Rollback)*.

Задача *Откат обновления баз* не имеет параметров.

Как откатить обновление баз и модулей приложения в Web Console

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите название приложения.

   b. В раскрывающемся списке **Тип задачи** выберите **Откат обновления баз**.

   c. В поле **Название задачи** введите название новой задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите способ определения области действия задачи.

4. Выберите устройства в соответствии с выбранным способом определения области действия задачи.

5. Завершите работу мастера.

   В списке задач отобразится новая задача.

6. Установите флажок напротив задачи и нажмите на кнопку **Запустить**.

Как откатить обновление баз и модулей приложения в Консоли администрирования

1. В Консоли администрирования выполните одно из следующих действий:

   - Если вы хотите создать задачу, которая будет выполняться на устройствах, входящих в выбранную группу администрирования, в дереве консоли в папке **Управляемые устройства** выберите эту группу администрирования, затем в рабочей области выберите вкладку **Задачи** и нажмите на кнопку **Новая задача**.

     Запустится мастер создания задачи для устройств выбранной группы администрирования.

   - Если вы хотите создать задачу, которая будет выполняться на одном или нескольких устройствах (задачу для набора устройств), в дереве консоли выберите папку **Задачи** и нажмите на кнопку **Новая задача** в рабочей области.

     Запустится мастер создания задачи для набора устройств.

2. На первом шаге мастера выберите в списке название приложения Kaspersky Endpoint Security и тип задачи **Откат обновления баз** .

3. Если вы создаете задачу для набора устройств, мастер предложит выбрать устройства, которым будет назначена задача. Выберите способ определения области действия задачи.

4. Выберите устройства в соответствии с выбранным способом определения области действия задачи.

5. Настройте расписание задачи.

6. Введите название новой задачи.

7. Завершите работу мастера.

   В списке задач отобразится новая задача.

8. В списке задач выберите нужную задачу, откройте контекстное меню задачи и выберите **Запустить**.

Как откатить обновление баз и модулей приложения в командной строке

Выполните команду:

```
Откатить обновление баз и модулей

kesl-control --start-task 7
```

Как откатить обновление баз и модулей приложения в графическом интерфейсе

1. Откройте главное окно графического интерфейса приложения.

2. В главном окне приложения нажмите на кнопку **Обновление**.

   Откроется окно **Обновление**.

3. Запустите откат обновления баз по ссылке **Откатить обновление**.

Защита устройств от угроз

Защита от файловых угроз

Защита от файловых угроз обеспечивает минимальный уровень безопасности компьютера. Компонент запускается вместе с Kaspersky Endpoint Security и проверяет файлы в режиме реального времени.

Как работает Защита от файловых угроз

1. **Приложение перехватывает события файловых операций и блокирует действия до завершения проверки**

   Приложение использует механизм перехвата файловых операций и блокирует доступ при любом обращении к проверяемому файлу до завершения проверки.

2. **Приложение проверяет файл**

   Защита от файловых угроз проверяет файл с помощью следующих технологий:

   - Антивирусные базы
   - Облачные службы Kaspersky Security Network
   - Эвристический анализ – технология позволяет выявлять угрозы, которые еще не внесены в базы данных "Лаборатории Касперского".

3. **Завершение проверки**

   После проверки приложение или разрешает операцию, или запрещает ее и выполняет действие, предусмотренное при обнаружении угрозы.

Первоначальная настройка Защиты от файловых угроз

Первоначальная настройка включает шаги, необходимые для базовой защиты конечных устройств.

1. **Выберите механизм перехвата системных событий**

   Защита от файловых угроз перехватывает события файловых операций и блокирует действия до завершения проверки.

   При установке приложения вы выбрали механизм перехвата системных событий:

   - механизм перехвата на основе обновляемого модуля ядра
   - системный механизм перехвата на основе технологии fanotify
   - модуль ядра для защиты от файловых угроз на ОС без fanotify

   Выбор механизма перехвата системных событий зависит от конфигурации компьютера. Самой производительной технологией является механизм перехвата на основе обновляемого модуля ядра. Вы можете включить этот механизм в параметрах приложения.

2. **Настройте Защиту от файловых угроз**

   По умолчанию Защита от файловых угроз включена и использует параметры, рекомендованные специалистами "Лаборатории Касперского". Параметры по умолчанию обеспечивают рекомендуемый уровень защиты и оптимальное потребление ресурсов компьютера. Если у вас особые требования к безопасности инфраструктуры, вы можете изменить эти параметры.

3. **Настройте область защиты**

   По умолчанию приложение проверяет все файлы на защищаемом устройстве. Если вам нужно проверять только отдельную директорию (например, директорию, в которую автоматически загружаются файлы из внешнего источника), вы можете указать только эту директорию в качестве области защиты. В остальных случаях рекомендуем оставить область защиты по умолчанию и оптимизировать ее с помощью исключений.

4. **Исключите из проверки точки монтирования**

   Исключение из проверки точек монтирования позволяет не перехватывать файловые операции в определенной директории. Например, вы можете исключить из проверки общие сетевые ресурсы и для их защиты использовать Kaspersky Endpoint Security на том устройстве, где эти ресурсы хранятся физически. Также вы можете воспользоваться Рекомендациями для Защиты от файловых угроз и задач проверки.

5. **Добавьте исключения**

   Исключения позволяют поддерживать баланс между защищенностью и производительностью системы. Для стабильной работы стороннего ПО добавьте в исключения файлы и директории, которые указаны в документации к соответствующему программному обеспечению.

Рекомендуем исключить следующие объекты:

- Базы данных. Большие базы данных требуют большого количества ресурсов для проверки. Частое обращение к файлам базы данных приводит к частым проверкам.
- Файлы, с которыми работают ресурсоемкие процессы. Проверка таких файлов замедляет работу компьютера.
- Директории с файлами журналов. Операционная система записывает журнал постоянно. В результате Защита от файловых угроз проверяет журналы и тратит ресурсы компьютера.

Если объект исключен из проверки компонентом Защита от файловых угроз, рекомендуем проверять эти объекты с помощью задачи *Поиск вредоносного ПО*.

Дополнительная настройка для высоконагруженных серверов

Дополнительная настройка включает шаги для тонкой настройки Защиты от файловых угроз. Если после первоначальной настройки возникают задержки в работе устройства или если вы настраиваете высоконагруженные серверы, выполните следующие действия:

1. **Выключите блокировку доступа к файлам во время проверки**

   По умолчанию Защита от файловых угроз при любом обращении к проверяемому файлу блокирует к нему доступ до завершения проверки. Если вы выключите блокирующий режим, Защита от файловых угроз будет работать в режиме информирования. Такой режим перехвата файловых операций оказывает меньшее влияние на производительность системы во время работы, но есть риск, что угроза в файле не будет вылечена или удалена.

   Если блокирующий режим выключен, Контроль устройств, действие Запрет запуска объектов и задача Проверка съемных дисков также работают в режиме информирования.

2. **Соберите статистику проверки файлов**

   Контролируйте основные метрики работы компьютера: нагрузку на ЦПУ, быстродействие стороннего ПО и другие показатели. Это поможет вам определить, как снизить нагрузку на систему.

   Вы можете получить статистику проверки файлов с помощью инструментов анализа работы приложения. Также вы можете использовать собственные инструменты мониторинга.

3. **Оптимизируйте работу приложения**

   После анализа полученной информации оптимизируйте работу приложения:

   - добавьте глобальные исключения
   - добавьте исключения
   - оптимизируйте параметры приложения

4. **Включите блокировку доступа к файлам во время проверки**

   Включите блокировку доступа к файлам во время проверки. При обнаружении зараженного объекта приложение будет выполнять выбранное действие.

Особенности и ограничения

- Если у пользователя с root-правами отсутствует доступ к файлу в удаленной директории, смонтированной на устройстве по протоколу NFS4, приложение блокирует доступ к файлу для всех пользователей.
- Если включены Защита от файловых угроз и Мониторинг контейнеров, приложение также проверяет все пространства имен и контейнеры.

Как сформировать область защиты

Область защиты – список путей к объектам, которые Kaspersky Endpoint Security проверяет на наличие угроз. По умолчанию приложение проверяет все файлы на защищаемом устройстве. Если вам нужно проверять только отдельную директорию (например, директорию, в которую автоматически загружаются файлы из внешнего источника), вы можете указать эту директорию в качестве области защиты. В остальных случаях рекомендуем оставить область защиты по умолчанию и оптимизировать область с помощью исключений.

Kaspersky Endpoint Security проверяет объекты в том порядке, в котором эти объекты перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории настройки безопасности могли отличаться от родительской.

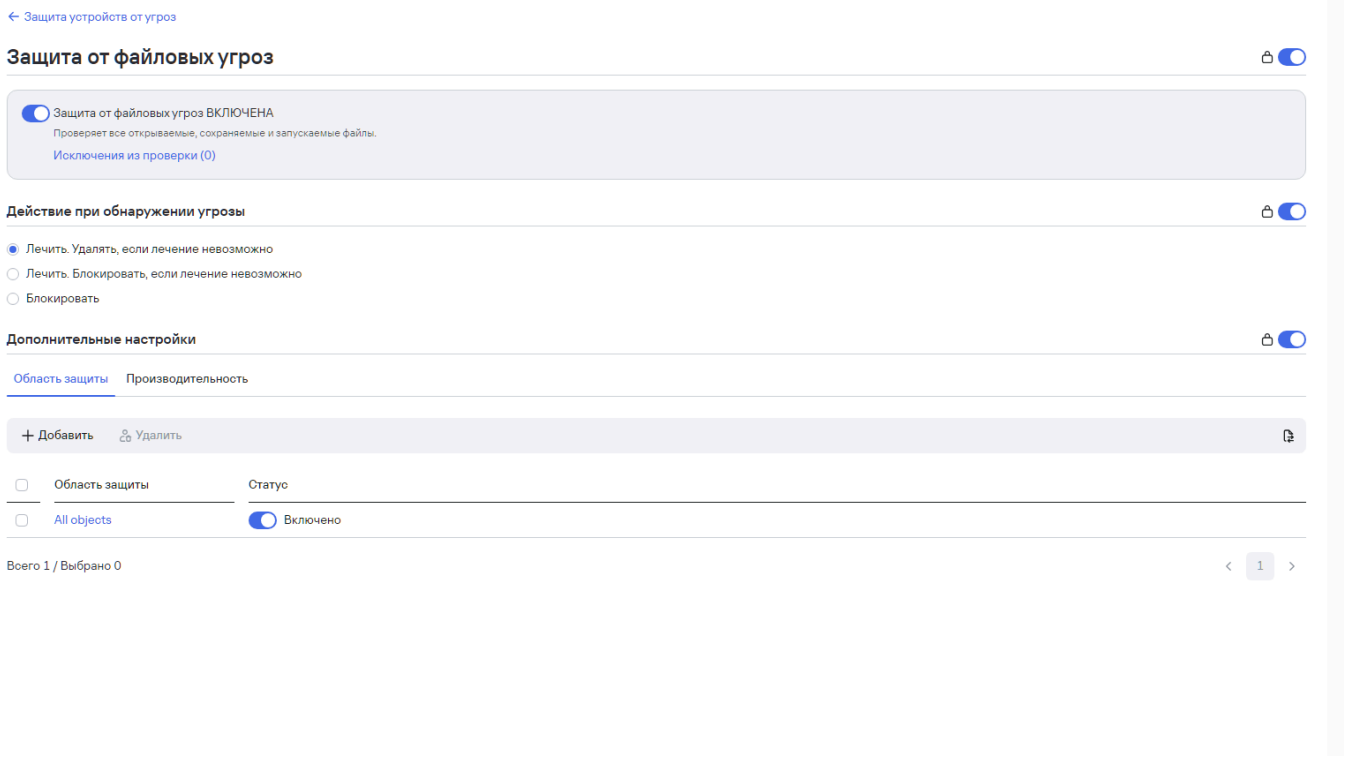
Как сформировать область защиты в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Защита от файловых угроз**.
5. В блоке **Область защиты** нажмите **Добавить**.
6. В открывшемся окне выберите тип файловой системы:
   - **Локальная**. Директории, расположенные на жестком диске и доступные без сетевого подключения.
   - **Смонтированная**. Смонтированные удаленные или локальные директории.
   - **Общая**. Директории компьютера, доступные по протоколу Samba (SMB) или NFS.
   - **Все удаленные смонтированные**. Все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
   - **Все общие**. Все директории компьютера, доступные по протоколам Samba и NFS.
7. Для локальной файловой системы укажите путь к директории (например, `/path/to/folder`). Если необходимо, установите флажок **Включить вложенные папки**.
8. Для смонтированной или для общей файловой системы укажите протокол доступа.

9. Укажите маски расширений объектов (например, `*.txt`). Разделяйте маски запятой.

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



Защита от файловых угроз

Как сформировать область защиты в командной строке

1. Выполните команду:

```
kesl-control --set-settings 1 --add-path <path>
```

В параметры задачи будет добавлена новая секция `[ScanScope.item_#]`. Приложение будет проверять объекты в директории, указанной параметром `Path`.

2. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 1
```

Пример

```
kesl-control --set-settings 1 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

В задачу будут добавлены следующие параметры области защиты:

```
[ScanScope.item_0001]
AreaDesc=All object
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

Как выбрать действие при обнаружении файловой угрозы

При обнаружении вредоносного ПО приложение Kaspersky Endpoint Security может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла. Вы можете выбрать действие, которое будет выполнять Kaspersky Endpoint Security при обнаружении угрозы, в параметрах Защиты от файловых угроз.

Как настроить действие при обнаружении угрозы в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Защита от файловых угроз**.
5. В блоке **Действие при обнаружении угрозы** выберите действие, которое выполнит приложение при обнаружении угрозы:
   - **Лечить. Удалять, если лечение невозможно** (по умолчанию). Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.
   - **Лечить. Блокировать, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение блокирует этот файл.
   - **Блокировать**. Если выбран этот вариант действия, то приложение автоматически блокирует зараженный файл без попытки вылечить и удалить.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как настроить действие при обнаружении угрозы в командной строке

1. Выполните команду:

   ```
   kesl-control --set-settings 1 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
   ```

2. Для проверки текущих значений параметров компонента выполните следующую команду:

   ```
   kesl-control --get-settings 1
   ```

Условные обозначения

Параметры команды

Параметр	Описание
`ActionOnThreat`	Действие при обнаружении угрозы: • `DisinfectDeleteIfNotPossible` (по умолчанию). Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл. • `DisinfectBlockIfNotPossible`. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение блокирует этот файл. • `Block`. Если выбран этот вариант действия, то приложение автоматически блокирует зараженный файл без попытки вылечить и удалить.

Что такое Интеллектуальный режим проверки файлов

Защита от файловых угроз проверяет все открываемые, сохраняемые и запускаемые файлы. По умолчанию Защита от файловых угроз проверяет файлы в интеллектуальном режиме. *Интеллектуальный режим* – режим работы приложения, в котором Защита от файловых угроз проверяет файл при попытке открытия. Далее, если процесс многократно обращается к файлу в течение некоторого времени и изменяет его, Защита от файловых угроз повторно проверят файл только при закрытии файла этим процессом. Благодаря этому приложение оказывает минимальную нагрузку на систему и обеспечивает высокий уровень защиты.

Для работы Интеллектуального режима работы приложения должен быть выбран и запущен обновляемый модуль ядра.

Изменить режим проверки файлов в Web Console невозможно.

Как выбрать режим проверки файлов в командной строке

1. Выполните команду:

```
kesl-control --set-settings 1 ScanByAccessType=<SmartCheck|OpenAndModify|Open>
```

2. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 1
```

Условные обозначения

Параметры команды

Параметр	Описание
`ScanByAccessType`	Режим проверки файлов: • `SmartCheck` (значение по умолчанию). Защита от файловых угроз проверяет файлы в интеллектуальном режиме. Kaspersky Endpoint Security проверяет файл при открытии и при закрытии, если файл был изменен. Если Интеллектуальный режим недоступен, приложение проверяет файлы при открытии и при каждом изменении файла (`OpenAndModify`). Интеллектуальный режим может быть недоступен, например, если остановлен обновляемый модуль ядра. • `OpenAndModify`. Kaspersky Endpoint Security проверяет файл при открытии и при каждом изменении файла, а не только при закрытии. • `Open`. Kaspersky Endpoint Security проверяет файл при попытке открытия как на чтение, так и на выполнение или изменение.

Как оптимизировать проверку файлов

Настройте проверку файлов, чтобы оптимизировать работу компонента Защита от файловых угроз. Это позволит снизить нагрузку на процессор защищаемого устройства. Вы можете ограничить проверку архивов, задать максимальный размер проверяемых объектов и максимальную длительность проверки объектов.

Как настроить проверку файлов в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз** → **Защита от файловых угроз**.

5. В блоке **Дополнительные настройки** перейдите на вкладку **Производительность** и настройте проверку файлов:

   - **Проверять архивы**. Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива). По умолчанию проверка выключена.

   - **Проверять дистрибутивы и самораспаковывающиеся архивы**. Проверка инсталляционных пакетов сторонних приложений и самораспаковывающихся архивов. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. По умолчанию проверка выключена.

   - **Проверять почтовые базы**. Проверка почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. По умолчанию проверка выключена.

   - **Проверять файлы почтовых форматов**. Проверка файлов сообщений электронной почты в текстовом формате. По умолчанию проверка выключена.

   - **Не проверять архивы размером более (МБ)**. Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.

   - **Пропускать файл, если его проверка длится более (сек.)**. Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра. По умолчанию приложение пытается проверить объект в течение минуты.

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

Как настроить проверку файлов в командной строке

1. Выполните команду:

```
kesl-control --set-settings 1 ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<Object size (MB)>
TimeLimit=<Scan time (sec)>
```

2. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 1
```

Условные обозначения

Параметры команды

Параметр	Описание
`ScanArchived`	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива). По умолчанию проверка выключена.
`ScanSfxArchived`	Проверка инсталляционных пакетов сторонних приложений и самораспаковывающихся архивов. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. По умолчанию проверка выключена.
`ScanMailBases`	Проверка почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. По умолчанию проверка выключена.
`ScanPlainMail`	Проверка файлов сообщений электронной почты в текстовом формате. По умолчанию проверка выключена.
`SkipPlainTextFiles`	Временное исключение из проверки файлов в текстовом формате. Приложение не будет проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. По умолчанию исключение из проверки выключено. Параметр предназначен для устройств, поддерживающих механизм перехвата системных событий на основе технологии fanotify. На устройствах с обновляемым модулем ядра приложение использует кеш результатов проверки для оптимизации нагрузки.
`SkipDatabaseJournals`	Временное исключение из проверки файла журналов баз данных. Приложение не будет проверять файл журнала баз данных, если файл журнала повторно используется тем же процессом в течение 10 минут после последней проверки. По умолчанию исключение из проверки выключено. Параметр предназначен для устройств, поддерживающих механизм перехвата системных событий на основе технологии fanotify. На устройствах с обновляемым модулем ядра приложение использует кеш результатов проверки для оптимизации нагрузки.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке. (Значение `0`).
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра. По умолчанию приложение пытается проверить объект в течение минуты. (Значение `60`).

Особенности проверки символических и жестких ссылок

Kaspersky Endpoint Security позволяет проверять символические и жесткие ссылки на файлы.

Символическая ссылка (англ. Soft link) – это файл, который указывает путь к другому файлу или директории. Символическая ссылка и файл, на который она указывает, могут находиться в разных файловых системах. Также такая ссылка может указывать на несуществующий файл. При удалении целевого файла ссылка не удаляется, но перестает работать.

Жесткая ссылка (англ. Hard link) – это альтернативное имя файла. Жесткая ссылка ссылается на индексный дескриптор (inode) файла, в котором содержится метаинформация о файле. Пока на файл есть хотя бы хотя бы одна жесткая ссылка, он продолжает существовать в файловой системе.

Проверка символических ссылок

Приложение проверяет символические ссылки только если файл, на который указывает символическая ссылка, входит в область защиты Защиты от файловых угроз.

Если файл находится вне области защиты, приложение не проверяет содержимое файла по символической ссылке. Если такой файл содержит вредоносный код, безопасность устройства окажется под угрозой.

Проверка жестких ссылок

При обнаружении вредоносного кода в файле, у которого больше одной жесткой ссылки, приложение лечит исходный файл. Если лечение невозможно, приложение удаляет обработанную жесткую ссылку и создает копию исходного файла с именем удаленной ссылки в резервном хранилище. Приложение удаляет только обрабатываемую жесткую ссылку, остальные жесткие ссылки остаются нетронутыми.

Когда вы восстанавливаете жесткую ссылку из резервного хранилища, приложение создает копию исходного файла с именем жесткой ссылки в исходном месте расположения. Связи с другими жесткими ссылками на исходный файл не восстановятся.

Резолвинг символических ссылок в исключениях по процессам

Если путь в параметре `ProgramPath` раздела `ExcludedForProgram` – символическая ссылка на бинарный исполняемый файл, то приложение применяет исключение к пути целевого файла. Правило действует для всех ссылок на этот файл, а не только для той, что указана явно. В этом параметре используется путь к образу программы, поэтому для ссылок на скрипты (например, `.sh`) резолвинг не выполняется.

Целевой файл определяется при запуске задачи и применении настроек. Если ссылка ведет на несуществующий файл, в исключения попадает путь к самой ссылке. При замене ссылки обычным исполняемым файлом с тем же именем исключение будет применяться к этому файлу.

Пример исключения по символической ссылке

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/md5sum
UseExcludedForProgram=Yes
Path=/root/s1
```

Ссылка `/usr/bin/md5sum` на момент запуска задачи ведет на `/bin/coreutils`, поэтому в исключения попадет `/bin/coreutils`. Если позже перенаправить ссылку на `/bin/false`, до перезапуска задачи исключение останется на `/bin/coreutils`, а к `/bin/false` исключение применяться не будет. После перезапуска исключение перейдет с `/bin/coreutils` на `/bin/false`.

Поиск вредоносного ПО

Проверка на наличие вредоносного ПО является важным фактором для обеспечения безопасности компьютера. Требуется регулярно выполнять поиск вредоносного ПО, чтобы исключить возможность распространения вредоносных приложений, которые не были обнаружены компонентами защиты, например, из-за установленного низкого уровня защиты или по другим причинам.

В Kaspersky Endpoint Security предустановлена стандартная задача *Поиск вредоносного ПО*. Вы можете использовать эту задачу для выполнения полной проверки устройства. При полной проверке приложение проверяет все объекты, расположенные на локальных дисках устройства, а также все смонтированные и общие объекты, доступ к которым предоставляется по протоколам Samba и NFS, с рекомендуемыми параметрами безопасности.

Мастер первоначальной настройки Сервера администрирования автоматически создает задачу *Поиск вредоносного ПО*. Для создания задачи *Поиск вредоносного ПО* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Linux. При необходимости вы можете создавать пользовательские задачи *Поиск вредоносного ПО*.

Настройка задачи Поиск вредоносного ПО

1. **Настройте расписание запуска задачи**

   Во время выполнения проверки Kaspersky Endpoint Security может потреблять больше ресурсов компьютера, чем обычно. Рекомендуется настроить расписание выполнения задач проверки в то время, когда компьютер наименее нагружен.

2. **Оптимизируйте нагрузку на систему во время выполнения проверки**

   Вы можете ограничить потребление ресурсов процессора при выполнении задачи Поиск вредоносного ПО. При этом время проверки компьютера может увеличиться.

   При работе ноутбука от аккумулятора приложение Kaspersky Endpoint Security позволяет отменить запуск задач, запланированных по расписанию.

3. **Настройте параметры задачи Поиск вредоносного ПО**

   По умолчанию задача Поиск вредоносного ПО использует параметры, рекомендованные специалистами "Лаборатории Касперского". Параметры по умолчанию обеспечивают рекомендуемый уровень защиты и оптимальное потребление ресурсов компьютера. Если у вас есть особые требования к безопасности инфраструктуры, вы можете изменить эти параметры.

   По умолчанию приложение проверяет архивы. Для этого приложение распаковывает архивы в директорию /tmp. Убедитесь, что на компьютере достаточно свободного места для распаковки архивов.

4 **Настройте область проверки**

По умолчанию приложение проверяет все файлы на защищаемом устройстве. Если вам нужно проверять только отдельную директорию (например, директорию, в которую автоматически загружаются файлы из внешнего источника), вы можете указать только эту директорию в качестве области проверки. В остальных случаях рекомендуем оставить область проверки по умолчанию и оптимизировать ее с помощью исключений.

> Для проверки серверов рекомендуется разделить область проверки на несколько подобластей и создать для каждой из них отдельную задачу Поиск вредоносного ПО. Чтобы распределить нагрузку, задайте в расписании разное время запуска для каждой задачи.

5 **Добавьте исключения из проверки**

Сформируйте область исключений:

- **Исключения из проверки**. Исключения позволяют поддерживать баланс между защищенностью и производительностью системы. Для стабильной работы стороннего ПО добавьте в исключения файлы и директории, которые указаны в документации к соответствующему программному обеспечению.

  Если вы уже сформировали область исключений для компонента Защита от файловых угроз, вы можете включить применение этих исключений и для задачи Поиск вредоносного ПО.

- **Глобальные исключения**. Исключение точек монтирования (глобальные исключения) позволяет не перехватывать файловые операции в определенных директориях. Исключите из области проверки общие сетевые ресурсы. Для защиты общих сетевых ресурсов используйте приложение Kaspersky Endpoint Security на том устройстве, где эти ресурсы хранятся физически.

6 **Запустите задачу Поиск вредоносного ПО**

Как запустить задачу Поиск вредоносного ПО в Web Console

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

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security *Поиск вредоносного ПО*.

   Откроется окно свойств задачи.

   Задача *Поиск вредоносного ПО* создается автоматически мастером первоначальной настройки Сервера администрирования. Для создания задачи *Поиск вредоносного ПО* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Linux.

   При необходимости вы можете создавать пользовательские задачи *Поиск вредоносного ПО*.

3. На вкладке **Параметры** настройте параметры задачи.

4. На вкладке **Параметры приложения** настройте параметры задачи (см. таблицу ниже).

5. На вкладке **Расписание** настройте режим запуска задачи.

   По умолчанию Kaspersky Endpoint Security настроен на ручной режим запуска задачи.

6. Сохраните внесенные изменения.

7. Запустите задачу.

Параметры задачи *Поиск вредоносного ПО*

Параметр	Описание
Область проверки	Таблица, содержащая области, проверяемые задачей. По умолчанию активна только одна область проверки, включающая все директории локальной файловой системы. Вы можете добавлять области проверки вручную.
Действие при обнаружении угрозы	• **Лечить. Удалять, если лечение невозможно** (значение по умолчанию). При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. • **Лечить. Информировать, если лечение невозможно**. При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), то приложение сохраняет в журнал информацию об этом. • **Информировать**. При выборе этого действия приложение сохраняет в журнале информацию о зараженном объекте.
Проверять архивы	Если функция включена, приложение проверяет архивы. Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Не проверять файлы размером более (МБ)**. По умолчанию функция включена.
Проверять дистрибутивы и самораспаковывающиеся архивы	Если функция включена, приложение проверяет самораспаковывающиеся архивы. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. По умолчанию функция включена.
Проверять файлы почтовых форматов	Если функция включена, приложение проверяет сообщения электронной почты в текстовом формате. По умолчанию функция выключена.
Проверять почтовые базы	Если функция включена, приложение проверяет почтовые базы приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. По умолчанию функция выключена.
Не проверять файлы размером более (МБ)	Вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 1–999999. По умолчанию ограничение выключено.
Пропускать файл, если его проверка длится более (сек.)	Вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 1–9999. По умолчанию ограничение выключено.
Не запускать несколько задач проверки одновременно	Отложенный запуск задач проверки, если проверка уже выполняется. Kaspersky Endpoint Security ставит новые задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, приложение запустило задачу полной проверки по расписанию. Если пользователь пытается запустить быструю проверку в интерфейсе приложения, Kaspersky Endpoint Security поставит задачу быстрой проверки в очередь и автоматически запустит ее после завершения полной проверки. По умолчанию функция выключена.
Использовать технологию iChecker	Если функция включена, приложение проверяет только новые и измененные с момента последней проверки файлы. Если функция выключена, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию функция включена.

Как запустить задачу Поиск вредоносного ПО в командной строке

1. В приложении по умолчанию есть задача *Поиск вредоносного ПО* (*Scan_My_Computer*). Если вы хотите создать новую задачу *Поиск вредоносного ПО*, выполните команду:

   ```
   kesl-control --create-task <task name> --type ODS
   ```

   где `<task name>` – имя, которое вы задаете для новой задачи.

   В результате выполнения команды приложение отобразит ID созданной задачи.

2. При необходимости измените параметры задачи (см. таблицу ниже) с помощью команды:

   ```
   kesl-control --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

   Пример изменения параметров задачи

   ```
   kesl-control --set-settings 101 ScanFiles=No
   ```

   Также вы можете настроить параметры задачи с помощью конфигурационного файла.

3. При необходимости настройте расписание запуска задачи. По умолчанию запуск задачи выполняется вручную.

4. Для проверки текущих значений параметров задачи выполните следующую команду:

   ```
   kesl-control --get-settings <task ID|name>
   ```

5. Для запуска задачи *Поиск вредоносного ПО* выполните следующую команду:

   ```
   kesl-control --start-task <task ID|name> [-W] [--progress]
   ```

   Пример команды

   ```
   kesl-control --start-task 2 -W
   ```

6. Для остановки задачи *Поиск вредоносного ПО* выполните следующую команду:

   ```
   kesl-control --stop-task <task ID|name> [-W]
   ```

Условные обозначения

Параметры задачи Поиск вредоносного ПО

Параметр	Описание	Значения
`ScanFiles`	Включение проверки файлов.	`Yes` (значение по умолчанию) – проверять файлы. `No` – не проверять файлы.
`ScanBootSectors`	Включение проверки загрузочных секторов.	`Yes` (значение по умолчанию) – проверять загрузочные секторы. `No` – не проверять загрузочные секторы.

Параметр	Описание	Значения
`ScanComputerMemory`	Включение проверки памяти процессов и памяти ядра.	`Yes` (значение по умолчанию) – проверять память процессов и память ядра. `No` – не проверять память процессов и память ядра.
`ScanStartupObjects`	Включение проверки объектов автозапуска.	`Yes` (значение по умолчанию) – проверять объекты автозапуска. `No` – не проверять объекты автозапуска.
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	`Yes` (значение по умолчанию) – проверять архивы. Если для параметра `ActionOnThreat` указано значение `DisinfectDeleteIfNotPossible` и лечение невозможно, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` (значение по умолчанию) – проверять самораспаковывающиеся архивы. `No` – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронной почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
`QueueScanTasks`	Отложенный запуск задач проверки, запланированных по расписанию, если запущенная ранее проверка по расписанию еще выполняется. Kaspersky Endpoint Security ставит запланированные задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, запланировано запускать задачу проверки в 18:00 и в 20:00. Задача проверки, которая должна запуститься в 20:00, будет отложена, если задача проверки, запущенная в 18:00, еще выполняется. Задача запустится после завершения задачи, запущенной в 18:00.	`Yes` – ставить в очередь задачи проверки, запланированные по расписанию, если текущая проверка еще выполняется. `No` (значение по умолчанию) – запускать запланированные задачи проверки по расписанию, даже если текущая проверка еще не завершена.

Параметр	Описание	Значения
`ActionOnThreat`	Выбор действия, которое приложение будет выполнять над зараженными объектами.	`DisinfectDeleteIfNotPossible` (лечить; удалять, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. `DisinfectInformIfNotPossible` (лечить; информировать, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение сохраняет в журнале информацию об этом. `Inform` (информировать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Включение исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.
	Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Включение исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats.item_#`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (значение по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.

Параметр	Описание	Значения
`UseOASExclusions`	Включение использования исключений Защиты от файловых угроз при проверке.	`Yes` (значение по умолчанию) – использовать исключения Защиты от файловых угроз. `No` – не использовать исключения Защиты от файловых угроз.
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию о незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию о проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию о необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (значение по умолчанию) – включить эвристический анализатор. `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка, минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) – рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.
`DeviceNameMasks.item_#`	Список имен устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску имени устройства.	`AllObjects` – проверять загрузочные секторы всех устройств. `<device name mask>` – проверять загрузочные секторы устройств, имена которых содержат указанную маску. Значение по умолчанию: `/**` – любой набор символов в имени устройства, включая символ `/`.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: `All objects`. Пример `AreaDesc="Mail bases scan"`
`UseScanArea`	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	`Yes` (значение по умолчанию) – проверять указанную область. `No` – не проверять указанную область.
`AreaMask.item_#`	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (проверять все объекты). Пример `AreaMask.item_0000=*doc`

Параметр	Описание	Значения
`Path`	Путь к директории с проверяемыми объектами.	`<path to local directory>` – проверять объекты в указанной директории. По умолчанию указан путь `/` – приложение проверяет все директории локальной файловой системы. `Shared:NFS` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. `Shared:SMB` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. `Mounted:NFS` – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `AllShared` – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. `<file system type>` – проверять все ресурсы указанной файловой системы устройства.
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры.		
`AreaDesc`	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из проверки.	`Yes` (значение по умолчанию) – исключать указанную область. `No` – не исключать указанную область.
`AreaMask.item_#`	Ограничение области исключения из проверки. В области исключения приложение исключает только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать все объекты).

Параметр	Описание	Значения
`Path`	Путь к директории с исключаемыми объектами.	`<path to local directory>` – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать маски. В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида `/.snapshots/*/snapshot/`. По умолчанию указан путь `/` – приложение исключает из проверки все директории локальной файловой системы. `Mounted:NFS` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `<file system type>` – исключать из проверки все ресурсы указанной файловой системы устройства. Удаленные директории исключаются из проверки приложением, только если они были смонтированы до запуска задачи. Удаленные директории, смонтированные после запуска задачи, из проверки не исключаются.

Как запустить задачу Поиск вредоносного ПО в графическом интерфейсе

1. Откройте главное окно графического интерфейса приложения.
2. Нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.
3. Если вы хотите запустить задачу проверки, нажмите на кнопку **Запустить**, расположенную под нужной задачей проверки.

   Отобразится ход выполнения задачи проверки.
4. Если вы хотите остановить задачу проверки, нажмите на кнопку **Остановить**, расположенную под нужной задачей проверки.

   Задача проверки остановится, отобразится информация о проверенных объектах и обнаруженных угрозах.
5. Если вы хотите просмотреть отчет по задаче проверки, нажмите на кнопку **Показать отчет**.

При обнаружении зараженного объекта или при завершении задачи проверки отображается соответствующее уведомление.

Также в окне **Проверка** отображается ход и результат выполнения временных задач проверки загрузочных секторов (*Scan_Boot_Sectors_{идентификатор}*) и временных задач выборочной проверки файлов (*Scan_File_{идентификатор}*).

7. **Соберите статистику проверки компьютера**

   Вы можете получить статистику проверки компьютера с помощью отчетов. Убедитесь, что продолжительность проверки находится в желаемых пределах. Проверьте обнаруженные объекты и, если объекты являются доверенными, добавьте эти объекты в исключения.

Особенности и ограничения

- Если у пользователя с root-правами отсутствует доступ к файлу на удаленной директории, смонтированной на устройстве по протоколу NFSv4, приложение пропустит этот файл во время проверки.
- Во время выполнения задач проверки Kaspersky Endpoint Security может лечить и удалять файлы, защищенные от изменения: файлы с атрибутами immutable и append-only и файлы в директориях с атрибутами immutable и append-only. В резервном хранилище сохраняются копии этих файлов, созданные до лечения или удаления. Вы можете восстанавливать файлы из резервных копий, если требуется. После выполнения задач проверки атрибуты immutable и append-only вылеченных файлов не сохраняются.
- Если во время поиска вредоносного ПО пользователь или служба watchdog перезапустили приложение, а также если во время поиска перезагрузился компьютер, поиск прерывается. При следующем запуске поиск вредоносного ПО начинается заново.

Полезные статьи

Что делать, если на устройстве заканчивается свободное дисковое пространство

Как сформировать область проверки

Область проверки – список путей к объектам, которые Kaspersky Endpoint Security проверяет на наличие угроз. По умолчанию приложение проверяет все файлы на защищаемом устройстве. Если вам нужно проверять только отдельную директорию (например, директорию, в которую автоматически загружаются файлы из внешнего источника), вы можете указать эту директорию в качестве области проверки.

Kaspersky Endpoint Security проверяет объекты в том порядке, в котором эти объекты перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории настройки безопасности могли отличаться от родительской.

> При работе на операционных системах, использующих специальную файловую систему parsecfs (Astra Linux Special Edition), рекомендуется добавить пути монтирования этой файловой системы в исключения из проверки.

Как сформировать область проверки в Web Console

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

   Откроется список задач.

2. Нажмите на задачу проверки.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. В разделе **Область проверки** нажмите на кнопку **Добавить**.

5. В раскрывающемся списке **Файловая система, протокол доступа и путь** выберите тип файловой системы:

   - **Локальная**. Директории, расположенные на жестком диске и доступные без сетевого подключения.
   - **Смонтированная**. Смонтированные удаленные или локальные директории.
   - **Общая**. Директории компьютера, доступные по протоколу Samba (SMB) или NFS.
   - **Все удаленные смонтированные**. Все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
   - **Все общие**. Все директории компьютера, доступные по протоколам Samba и NFS.

6. Для типов файловых систем **Смонтированная** и **Общая** выберите протокол доступа:

   - **NFS**. Удаленные директории, смонтированные на устройстве по протоколу NFS.
   - **Samba**. Удаленные директории, смонтированные на устройстве по протоколу Samba.
   - **Пользовательский**. Ресурсы файловой системы устройства с типом, отличным от NFS и Samba (например, `ext4` или `parsecfs`).

7. Укажите путь или маску пути к директории.

8. Если требуется, укажите маски имен объектов (например, `*.txt` или `report_*`). Разделяйте маски запятой.

9. Нажмите на кнопку **Добавить**.

   Новый объект будет добавлен в область проверки. Вы можете исключить объект из области проверки, не удаляя его из списка. Для этого выключите переключатель рядом с объектом.

10. Если требуется, включите или отключите предустановленные объекты в области проверки:

    - **Память ядра**. **Память запущенных процессов**.
    - **Запущенные процессы и объекты автозапуска**.
    - **Загрузочные секторы**.

- **Все жесткие диски**.
- **Все сетевые диски**.

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

Как сформировать область проверки в командной строке

1. Выполните команду:

```
kesl-control --set-settings 2 --add-path <path>
```

В параметры задачи будет добавлена новая секция `[ScanScope.item_#]`. Приложение будет проверять объекты в указанной директории.

Пример

```
kesl-control --set-settings 2 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

В задачу будут добавлены следующие параметры области проверки:

```
[ScanScope.item_0001]
AreaDesc=All objects
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

2. Если требуется включить в область проверки ресурсы смонтированной файловой системы определенного типа, отличного от NFS и Samba (например, `parsecfs`), укажите в параметре `Path` название типа файловой системы:

```
Path=<file system type>
```

Приложение будет проверять все ресурсы указанной файловой системы устройства.

Пример

```
kesl-control --set-settings 2 ScanScope.item_0002.UseScanArea=Yes ScanScope.item_0002.Path=parsecfs
```

В задачу будут добавлены следующие параметры области проверки:

```
[ScanScope.item_0002]
AreaDesc=All objects
UseScanArea=Yes
Path=parsecfs
AreaMask.item_0000=*
```

3. Для проверки текущих значений параметров задачи выполните следующую команду:

```
kesl-control --get-settings 2
```

Как настроить расписание проверки

Выполнение задачи *Поиск вредоносного ПО* может потребовать дополнительных затрат ресурсов компьютера. Чтобы минимизировать влияние Kaspersky Endpoint Security на производительность компьютеров пользователей во время их активного использования, вы можете настроить выполнение задачи в наиболее оптимальное время.

Например, если сотрудники вашей организации работают по фиксированному графику, вы можете настроить запуск проверки ночью или в выходные дни. Если по каким-либо причинам запуск проверки невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи проверки, как только это станет возможным.

Если оптимальное расписание проверки компьютера подобрать не удалось, задачу *Поиск вредоносного ПО* можно запускать не только по времени, но и по особым условиям – при запуске приложения, при загрузке обновлений в хранилище, при обнаружении вирусной атаки и при завершении другой задачи. Также с помощью функции Wake-on-LAN можно включать выключенные компьютеры за некоторое время до запуска задачи. Вы можете настроить запуск проверки компьютера с функцией Wake-on-LAN только для задачи *Поиск вредоносного ПО* в Kaspersky Security Center. Включить функцию Wake-on-LAN для проверки компьютера в интерфейсе приложения невозможно.

Как настроить расписание поиска вредоносного ПО в Web Console

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

   Откроется список задач.

2. Нажмите на задачу проверки.

   Откроется окно свойств задачи.

3. В окне свойств задачи выберите вкладку **Расписание**.

4. Настройте расписание запуска задачи проверки.

5. В зависимости от выбранной периодичности настройте дополнительные параметры, которые уточняют расписание запуска задачи (см. таблицу ниже).

6. Сохраните внесенные изменения.

Параметры расписания проверки

Параметр	Описание
Запуск задачи	**Вручную**. Режим запуска, при котором вы запускаете проверку вручную в удобное для вас время. По расписанию. Режим запуска задачи проверки, при котором приложение выполняет задачу проверки по сформированному вами расписанию. Если выбран этот режим запуска задачи проверки, вы также можете запускать задачу проверки вручную.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Endpoint Security запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени. Если флажок снят, Kaspersky Endpoint Security не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.

Параметр	Описание
Использовать автоматическое определение случайного интервала между запусками задачи	Если флажок установлен, задача запускается на компьютерах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит распределенный запуск задачи. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества компьютеров, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако, когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Использовать автоматическую случайную задержку запуска задачи в интервале	Если флажок установлен, задача запускается на компьютерах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Включать устройства перед запуском задачи функцией Wake-on-LAN	Если флажок установлен, операционная система на компьютере будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут. Установите флажок, если вы хотите запустить выполнение задачи на всех компьютерах, включая компьютеры, которые выключены.
Выключать устройства после выполнения задачи	Если флажок установлен, компьютер будет выключен после выполнения задачи. Например, вы можете включить эту функцию для проверки компьютера в пятницу после рабочего дня. После завершения работы задачи приложение выключает компьютер на выходные.
Остановить, если задача выполняется дольше	Ограничение длительности выполнения задачи. По истечении заданного времени Kaspersky Endpoint Security останавливает выполнение задачи. При этом задача не будет завершена. Следующий запуск задачи Kaspersky Endpoint Security выполнит сначала и по расписанию.

Как настроить расписание поиска вредоносного ПО в командной строке

Для запуска задачи один раз в определенное время выполните команду

```
kesl-control --set-schedule 2 RuleType=Once StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>'
```

Для запуска задачи раз в месяц выполните команду

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='<hh>:<mm>:<ss>;<day of the month>'
```

Для запуска задачи в определенный день недели выполните команду

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='<hh>:<mm>:<ss>;<day of the week>'
```

Для регулярного запуска задачи, с интервалом в днях, выполните команду

```
kesl-control --set-schedule 2 RuleType=Daily StartTime='<hh>:<mm>:<ss>;<interval between runs (in days)>'
```

Для регулярного запуска задачи с определенной даты, с заданным интервалом в часах, выполните команду

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>;
<interval between runs (in hours)>'
```

Для регулярного запуска задачи с определенного времени, с заданным интервалом в минутах, выполните команду

```
kesl-control --set-schedule 2 RuleType=Minutely StartTime='<hh>:<mm>:<ss>;<interval between runs (in minutes)>'
```

Для запуска задачи сразу после запуска приложения выполните команду

```
kesl-control --set-schedule 2 RuleType=PS
```

Для запуска задачи сразу после обновления баз выполните команду

```
kesl-control --set-schedule 2 RuleType=BR
```

Для выключения запуска задачи по расписанию выполните команду

```
kesl-control --set-schedule 2 RuleType=Manual
```

Для настройки дополнительных параметров расписания запуска задачи выполните команду

```
kesl-control --set-schedule 2 RandomInterval=<time interval (minutes)> RunMissedStartRules=<Yes|No>
UseWorkingTimeout=<Yes|No> WorkingTimeout=<maximum task completion time (minutes)> QueueScanTasks=<Yes|No>
```

Для проверки текущих значений параметров задачи выполните следующую команду

```
kesl-control --get-schedule 2
```

Условные обозначения

Параметры расписания запуска задачи

Параметр	Описание
`RuleType`	Расписание запуска задачи. • `Once` – запускать задачу один раз. • `Monthly` – запускать задачу каждый месяц в указанный день и в указанное время. • `Weekly` – запускать задачу каждую неделю в указанный день и в указанное время. • `Daily` – запускать задачу регулярно, с заданным интервалом в днях. • `Hourly` – запускать задачу регулярно, с заданным интервалом в часах, начиная с указанных даты и времени. • `Minutely` – запускать задачу регулярно, с заданным интервалом в минутах, начиная с указанного времени. • `Manual` – запускать задачу вручную. • `PS` – запускать задачу после запуска приложения. • `BR` – запускать задачу после обновления баз приложения.
`StartTime`	Дата и время запуска задачи. Формат параметра зависит от значения `RuleType`. Допустимые значения: • `<year>`: 1970 – 2099; • `<month>`: JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC; • `<day of the month>`: 1 – 31; • `<day of the week>`: Mon, Tue, Wed, Thu, Fri, Sat, Sun; • `<hh>`: 0 – 23; • `<mm>`: 0 – 59; • `<ss>`: 0 – 59; • `<interval between runs (in days)>`: 0 – 364; • `<interval between runs (in hours)>`: 0 – 23; • `<interval between runs (in minutes)>`: 0 – 59.
`RandomInterval`	Запуск задачи на компьютерах случайным образом в течение определенного интервала времени (от 0 до указанного значения). Это позволяет избежать одновременный запуск задач. Значение по умолчанию: 99 минут. Допустимые значения: 0 – 999.
`RunMissedStartRules`	Запуск пропущенной задачи после запуска приложения. • `Yes` (значение по умолчанию) – запуск пропущенной задачи включен. Если во время запуска задачи по расписанию приложение остановлено или компьютер выключен, Kaspersky Endpoint Security запускает задачу сразу после запуска приложения. Это позволяет не пропустить запуск критически важных задач. • `No` – запуск пропущенной задачи выключен. Если во время запуска задачи по расписанию приложение остановлено или компьютер выключен, приложение пропускает запуск этой задачи. Это позволяет избежать повышенной нагрузки при запуске приложения.
`UseWorkingTimeout`	Остановка задачи при достижении максимального времени выполнения задачи, заданного параметром `WorkingTimeout`. Задача будет остановлена, даже если она не завершена. Следующий запуск задачи будет выполнен по расписанию. • `Yes` – останавливать задачу при достижении максимального времени выполнения задачи. • `No` (значение по умолчанию) – не останавливать задачу при достижении максимального времени выполнения задачи.

Параметр	Описание
`WorkingTimeout`	Максимальное время выполнения задачи (в минутах), при достижении которого приложение останавливает выполнение задачи, если значение параметра `UseWorkingTimeout=Yes`. Значение по умолчанию: 120 минут. Допустимые значения: 1 – 999.

Пример запуска проверки каждые 10 часов

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='2030/May/28 12:00:00;10'
```

Пример запуска задачи проверки 15-го числа каждого месяца

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='12:00:00;15'
```

Пример запуска задачи каждый вторник

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='12:00:00;Tue'
```

Как проверить отдельный файл или директорию

Kaspersky Endpoint Security позволяет проверять отдельные файлы на вирусы и другие приложения, представляющие угрозу, в командной строке. Например, вы можете выборочно проверять архивы, проверка которых с помощью Защиты от файловых угроз по умолчанию выключена.

По умолчанию приложение проверяет файл с параметрами задачи *Scan_File (ID:3)*, рекомендованными специалистами "Лаборатории Касперского". Параметры по умолчанию обеспечивают рекомендованный уровень защиты и оптимальное потребление ресурсов. По умолчанию приложение сохраняет копию зараженного объекта в резервном хранилище и пытается вылечить объект. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. Вы можете выбрать другое действие при обнаружении угрозы, а также настроить другие параметры задачи.

Как запустить проверку отдельного файла или директории в командной строке

```
kesl-control --scan-file <path to the file or directory>
```

В результате Kaspersky Endpoint Security сформирует отчет в следующем виде:

```
Проверенные объекты: N

Всего обнаружено объектов: N

Зараженные и другие объекты: N

Вылеченные объекты: N

Помещено в резервное хранилище: N

Удаленные объекты: N

Невылеченные объекты: N

Ошибки проверки: N
```

```
Объекты, защищенные паролем: N

Пропущено объектов: N

Обнаружено с помощью Cloud Sandbox: N
```

Как оптимизировать запуск задач выборочной проверки

Для оптимизации выборочной проверки вы можете ограничить одновременный запуск нескольких задач. Если пользователь попытается запустить слишком много задач выборочной проверки, приложение не запустит задачи, которые превышают ограничение. Это позволит контролировать потребление ресурсов клиентского устройства и, например, избежать слишком большой нагрузки на сервер. По умолчанию ограничение на количество задач выборочной проверки равно 100.

Kaspersky Endpoint Security ограничивает запуск задач только для непривилегированных пользователей. Пользователь с root-правами может запускать задачи выборочной проверки без ограничений.

Вы можете настроить ограничение запуска задач выборочной проверки в командной строке с помощью общих параметров приложения. Настроить ограничение запуска задач в Консоли администрирования и в Web Console невозможно.

Как оптимизировать запуск задач выборочной проверки в командной строке

```
kesl-control --set-app-settings LimitNumberOfScanFileTasks=<number of tasks>
```

Проверка важных областей

Для проверки только критически важных областей компьютера предназначена отдельная задача проверки – *Проверка важных областей*. Задача *Проверка важных областей* позволяет быстро проверить области компьютера, в которых чаще всего скрывается вредоносное ПО. В область проверки этой задачи входят загрузочные секторы, объекты автозапуска, память ядра и запущенные процессы.

Компрометация важных областей компьютера предоставляет вредоносному ПО возможность реализовать свои функции и скрывать свое присутствие. По умолчанию приложение выполняет задачу с параметрами, рекомендованными специалистами "Лаборатории Касперского". Параметры по умолчанию обеспечивают рекомендованный уровень защиты и оптимальное потребление ресурсов.

Специалисты "Лаборатории Касперского" не рекомендуют изменять параметры задачи *Проверка важных областей*, заданные по умолчанию.

Если у пользователя с root-правами отсутствует доступ к файлу на удаленной директории, смонтированной на устройстве по протоколу NFSv4, приложение пропустит этот файл во время проверки.

Мастер первоначальной настройки Сервера администрирования автоматически создает задачу *Проверка важных областей*. Для создания задачи *Проверка важных областей* во время работы мастера установите плагин управления Kaspersky Endpoint Security для Linux. При необходимости вы можете создавать пользовательские задачи *Проверка важных областей*.

Как запустить проверку важных областей в Web Console

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

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

   b. В раскрывающемся списке **Тип задачи** выберите **Проверка важных областей**.

   c. В поле **Название задачи** введите короткое описание, например, *Проверка важных областей после заражения компьютера*.

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

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

5. Завершите работу мастера.

6. Нажмите на задачу проверки.

   Откроется окно свойств задачи.

7. Выберите вкладку **Параметры приложения**.

8. Настройте параметры задачи проверки (см. таблицу ниже).

9. Если требуется, настройте расписание запуска задачи на вкладке **Расписание**.

10. Сохраните внесенные изменения.

11. Запустите задачу проверки.

Параметры задачи Проверка важных областей

Параметр	Описание
Область проверки	Таблица, содержащая области, проверяемые задачей. По умолчанию область проверки включает в себя все директории локальной файловой системы, память ядра, память запущенных процессов, объекты автозапуска и загрузочные секторы.
Действие при обнаружении угрозы	• **Лечить. Удалять, если лечение невозможно** (по умолчанию). При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. • **Лечить. Информировать, если лечение невозможно**. При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), то приложение сохраняет в журнал информацию об этом. • **Информировать**. При выборе этого действия приложение сохраняет в журнале информацию о зараженном объекте.

Параметр	Описание
Проверять архивы	Если функция включена, приложение проверяет архивы. Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Не проверять файлы размером более (МБ)**. По умолчанию функция включена.
Проверять дистрибутивы и самораспаковывающиеся архивы	Если функция включена, приложение проверяет самораспаковывающиеся архивы. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. По умолчанию функция включена.
Проверять файлы почтовых форматов	Проверка файлов сообщений электронной почты в текстовом формате. По умолчанию функция выключена.
Проверять почтовые базы	Если функция включена, приложение проверяет почтовые базы приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. По умолчанию функция выключена.
Не проверять файлы размером более (МБ)	Вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–9999. Если установлено значение 0, приложение проверяет файлы любого размера. По умолчанию функция выключена.
Пропускать файл, если его проверка длится более (сек.)	Вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. По умолчанию функция выключена.
Не запускать несколько задач проверки одновременно	Отложенный запуск задач проверки, если проверка уже выполняется. Kaspersky Endpoint Security ставит новые задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, приложение запустило задачу полной проверки по расписанию. Если пользователь пытается запустить быструю проверку в интерфейсе приложения, Kaspersky Endpoint Security поставит задачу быстрой проверки в очередь и автоматически запустит ее после завершения полной проверки. По умолчанию функция выключена.
Использовать технологию iChecker	Если функция включена, приложение проверяет только новые и измененные с момента последней проверки файлы. Если функция выключена, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию функция включена.

Как запустить проверку важных областей в командной строке

1. Если требуется, настройте параметры задачи (см. таблицу ниже).

```
kesl-control --set-settings 4 <setting name>=<setting value>
```

2. Если требуется, настройте расписание запуска задачи.

3. Для проверки текущих значений параметров задачи выполните следующую команду:

```
kesl-control --get-settings 4 [--json]
```

где `--json` – выводить данные в формате JSON.

4. Для запуска задачи выполните команду:

```
kesl-control --start-task 4 [-W] [--progress]
```

Где:

- `[-W]` – включить вывод текущих событий, связанных задачей.
- `[--progress]` – отображать ход выполнения задачи.

При необходимости вы можете создавать пользовательские задачи *Проверка важных областей*.

Параметры задачи Проверка важных областей

Параметр	Описание	Значения
`ScanFiles`	Включение проверки файлов.	`Yes` – проверять файлы. `No` (значение по умолчанию) – не проверять файлы.
`ScanBootSectors`	Включение проверки загрузочных секторов.	`Yes` (значение по умолчанию) – проверять загрузочные секторы. `No` – не проверять загрузочные секторы.
`ScanComputerMemory`	Включение проверки памяти процессов и памяти ядра.	`Yes` (значение по умолчанию) – проверять память процессов и память ядра. `No` – не проверять память процессов и память ядра.
`ScanStartupObjects`	Включение проверки объектов автозапуска.	`Yes` (значение по умолчанию) – проверять объекты автозапуска. `No` – не проверять объекты автозапуска.
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	`Yes` (значение по умолчанию) – проверять архивы. Если для параметра `ActionOnThreat` указано значение `DisinfectDeleteIfNotPossible` и лечение невозможно, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` (значение по умолчанию) – проверять самораспаковывающиеся архивы. `No` – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронной почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.

Параметр	Описание	Значения
`QueueScanTasks`	Отложенный запуск задач проверки, запланированных по расписанию, если запущенная ранее проверка по расписанию еще выполняется. Kaspersky Endpoint Security ставит запланированные задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, запланировано запускать задачу проверки в 18:00 и в 20:00. Задача проверки, которая должна запуститься в 20:00, будет отложена, если задача проверки, запущенная в 18:00, еще выполняется. Задача запустится после завершения задачи, запущенной в 18:00.	`Yes` – ставить в очередь задачи проверки, запланированные по расписанию, если текущая проверка еще выполняется. `No` (значение по умолчанию) – запускать запланированные задачи проверки по расписанию, даже если текущая проверка еще не завершена.
`ActionOnThreat`	Выбор действия, которое приложение будет выполнять над зараженными объектами.	`DisinfectDeleteIfNotPossible` (лечить; удалять, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. `DisinfectInformIfNotPossible` (лечить; информировать, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение сохраняет в журнале информацию об этом. `Inform` (информировать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Включение исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.
	Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Включение исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats.item_#`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`.

Параметр	Описание	Значения

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (значение по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.
`UseOASExclusions`	Включение использования исключений Защиты от файловых угроз при проверке.	`Yes` (значение по умолчанию) – использовать исключения Защиты от файловых угроз. `No` – не использовать исключения Защиты от файловых угроз.
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию о незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию о проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию о необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (значение по умолчанию) – включить эвристический анализатор. `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка, минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) – рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.

Параметр	Описание	Значения
DeviceNameMasks.item_#	Список имен устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску имени устройства.	AllObjects – проверять загрузочные секторы всех устройств. <device name mask> – проверять загрузочные секторы устройств, имена которых содержат указанную маску. Значение по умолчанию: /** – любой набор символов в имени устройства, включая символ /.
Секция [ScanScope.item_#] содержит следующие параметры:		
AreaDesc	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: All objects. Пример AreaDesc="Mail bases scan"
UseScanArea	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	Yes (значение по умолчанию) – проверять указанную область. No – не проверять указанную область.
AreaMask.item_#	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: * (проверять все объекты). Пример AreaMask.item_<item number>=*doc
Path	Путь к директории с проверяемыми объектами.	<path to local directory> – проверять объекты в указанной директории. По умолчанию указан путь / – приложение проверяет все директории локальной файловой системы. Shared:NFS – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. Shared:SMB – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. Mounted:NFS – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. Mounted:SMB – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. AllRemoteMounted – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. AllShared – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. <file system type> – проверять все ресурсы указанной файловой системы устройства.
Секция [ExcludedFromScanScope.item_#] содержит следующие параметры.		
AreaDesc	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
UseScanArea	Исключение указанной области из проверки.	Yes (значение по умолчанию) – исключать указанную область. No – не исключать указанную область.

Параметр	Описание	Значения
`AreaMask.item_#`	Ограничение области исключения из проверки. В области исключения приложение исключает только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать все объекты).
`Path`	Путь к директории с исключаемыми объектами.	`<path to local directory>` – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать маски. В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида `/.snapshots/*/snapshot/`. По умолчанию указан путь `/` – приложение исключает из проверки все директории локальной файловой системы. `Mounted:NFS` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `<file system type>` – исключать из проверки все ресурсы указанной файловой системы устройства. Удаленные директории исключаются из проверки приложением, только если они были смонтированы до запуска задачи. Удаленные директории, смонтированные после запуска задачи, из проверки не исключаются.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.

Проверка контейнеров

Kaspersky Endpoint Security может выполнять проверку контейнеров и образов на наличие вредоносного ПО в режиме реального времени и по требованию

Для использования функциональности проверки контейнеров требуется лицензия, которая включает эту функцию.

Компонент недоступен для устройств с процессором Эльбрус.

Мониторинг контейнеров

Компонент *Мониторинг контейнеров* проверяет в реальном времени запущенные контейнеры и пространства имен. По умолчанию компонент Мониторинг контейнеров включен.

Для работы компонента Мониторинг контейнеров должен быть включен компонент Защита от файловых угроз. Во время проверки контейнеров и пространств имен используются параметры защиты от файловых угроз.

Рекомендуемый сценарий настройки Мониторинга контейнеров состоит из следующих этапов:

1. **Настройте интеграцию приложения с инструментами для управления контейнерами**

   Приложение поддерживает интеграцию с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

2. **Сформируйте область защиты**

   Определите устройства, на которых требуется проверять контейнеры и пространства имен.

3. **В настройках Мониторинга контейнеров выберите действие Пропустить контейнер**

   При обнаружении зараженного объекта в контейнере приложение Kaspersky Endpoint Security может сразу остановить контейнер, не выполнять никаких действий с контейнером или остановить контейнер, если не удалось вылечить зараженный объект или устранить угрозу. Выберите действие **Пропустить контейнер**, чтобы проверить работу компонента. Приложение не будет выполнять действий над контейнером при обнаружении зараженного объекта, но будет записывать в журнал информацию об обнаруженных угрозах.

4. **Соберите статистику работы Мониторинга контейнеров**

   Вы можете получить статистику работы компонента Мониторинг контейнеров с помощью отчетов.

5. **Выберите действие над контейнером при обнаружении зараженного объекта**

   Выберите действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта.

Проверка контейнеров по требованию

Приложение может по требованию проверять контейнеры и образы на наличие вирусов и других вредоносных программ. Для этого используется предустановленная задача *Проверка контейнеров (Container_Scan)*. Вы можете настраивать предустановленную задачу, а также создавать пользовательские задачи проверки контейнеров с помощью командной строки, Web Console или Консоли администрирования.

Приложение может выполнять одновременно несколько задач проверки контейнеров.

Рекомендуемый сценарий настройки проверки контейнеров состоит из следующих этапов:

1. **Настройте интеграцию приложения с инструментами для управления контейнерами**

   Приложение поддерживает интеграцию с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

2. **Сформируйте область проверки**

   По умолчанию приложение проверяет все контейнеры на защищаемом устройстве. Если вам нужно проверять только отдельные контейнеры, вы можете указать их имена или маски имен.

3. **В настройках Проверки контейнеров выберите действия Пропустить контейнер и Пропустить образ**

   При обнаружении зараженного объекта в контейнере приложение Kaspersky Endpoint Security может сразу остановить контейнер, не выполнять никаких действий с контейнером или остановить контейнер, если не удалось вылечить зараженный объект или устранить угрозу. При обнаружении зараженного объекта в образе контейнера приложение Kaspersky Endpoint Security может удалить образ контейнера или не выполнять никаких действий с образом контейнера. Выберите действия **Пропустить контейнер** и **Пропустить образ**, чтобы проверить работу задачи. Приложение не будет выполнять действий над контейнером и образом при обнаружении зараженного объекта, но будет записывать в журнал информацию об обнаруженных угрозах.

4. **Соберите статистику работы Проверки контейнеров**

   Вы можете получить статистику работы задачи Проверка контейнеров с помощью отчетов.

5. **Оптимизируйте работу приложения**

   После анализа полученной информации оптимизируйте работу приложения:

   - добавьте глобальные исключения
   - добавьте исключения из проверки
   - оптимизируйте проверку контейнеров

6. **Выберите действие над контейнером и над образом при обнаружении зараженного объекта**

   Выберите действия, которые приложение будет выполнять над контейнером и над образом контейнера при обнаружении зараженного объекта.

Выборочная проверка контейнеров

Задача *Выборочная проверка контейнеров* предназначена для настройки и хранения параметров, которые используются во время проверки указанных контейнеров и образов по команде:

```
kesl-control --scan-container
```

Выборочная проверка выполняется с параметрами, которые хранятся в предустановленной задаче *Custom_Container_Scan* (ID:19). Вы можете настраивать параметры выборочной проверки контейнеров и образов, изменяя параметры этой задачи. По умолчанию для задачи *Custom_Container_Scan* заданы такие же параметры, как для задачи *Container_Scan* (ID:18).

В результате выполнения команды приложение создает и запускает временную задачу проверки контейнеров и образов, которая автоматически удаляется после завершения. При этом в консоль выводятся результаты проверки.

Особенности и ограничения

- Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен. При этом в командной строке отображается статус компонента Мониторинг контейнеров "Задача доступна и не выполняется", в Kaspersky Security Center отображается статус "Остановлена".
- Выбор действия Мониторинга контейнеров доступен только при использовании приложения по лицензии, которая включает эту функцию.

Как настроить интеграцию с инструментами для управления контейнерами

Приложение поддерживает интеграцию с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc. Вы можете настроить интеграцию с этими инструментами управления контейнерами.

Как настроить интеграцию с инструментами для управления контейнерами в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки проверки контейнеров**.
5. Убедитесь, что переключатель работы компонента Мониторинг контейнеров находится в положении **Проверка пространств имен и контейнеров ВКЛЮЧЕНА**.
6. В блоке **Настройки проверки контейнеров** нажмите на кнопку **Настроить**.

7. В открывшемся окне **Настройки проверки** установите флажки рядом с инструментами управления контейнерами, которые установлены и используются в операционной системе защищаемых устройств, и укажите необходимые параметры:

   - **Использовать Docker** – флажок включает использование системы управления контейнерами Docker. По умолчанию флажок установлен.

     - **Путь Docker-сокета** – поле ввода пути или URI (универсальный идентификатор ресурса) Docker-сокета. Значение по умолчанию: /var/run/docker.sock.

   - **Использовать CRI-O** – флажок включает использование среды CRI-O. По умолчанию флажок установлен.

     - **Путь к файлу** – поле ввода пути к конфигурационному файлу CRI-O. Значение по умолчанию: /etc/crio/crio.conf.

   - **Использовать Podman** – флажок включает использование утилиты Podman. По умолчанию флажок установлен.

     - **Путь к файлу** – поле ввода пути к исполняемому файлу утилиты Podman. Значение по умолчанию: /usr/bin/podman

     - **Корневая директория** – поле ввода пути к корневой директории хранилища контейнеров.

   - **Использовать runc** – флажок включает использование утилиты runc. По умолчанию флажок установлен.

     - **Путь к файлу** – поле ввода пути к исполняемому файлу утилиты runc. Значение по умолчанию: /usr/bin/runc

     - **Корневая директория** – поле ввода пути к корневой директории хранилища состояний контейнеров. Значение по умолчанию: /run/runc.

8. Сохраните внесенные изменения.

Как настроить интеграцию с инструментами для управления контейнерами в командной строке

В командной строке вы можете включать и выключать мониторинг пространств имен и контейнеров в реальном времени с помощью параметра `NamespaceMonitoring=<Yes|No>` из общих параметров приложения.

Вы можете изменять значение параметра `NamespaceMonitoring` с помощью конфигурационного файла, который содержит все общие параметры приложения, или с помощью ключей командной строки.

Включить мониторинг пространств имен и контейнеров с помощью ключей командной строки

```
kesl-control --set-app-settings NamespaceMonitoring=Yes
```

При проверке пространств имен и контейнеров в реальном времени используются параметры проверки контейнеров. Вы можете просматривать и изменять эти параметры с помощью специальных команд управления Kaspersky Endpoint Security:

- Вы можете выводить текущие значения параметров проверки контейнеров в консоль или в конфигурационный файл. Этот файл вы можете использовать для изменения параметров.
- Вы можете изменять все параметры проверки контейнеров, используя конфигурационный файл, который содержит параметры. Конфигурационный файл вы можете получить с помощью команды вывода общих параметров проверки контейнеров.
- Вы можете изменять отдельные параметры, используя ключи командной строки в формате `<setting name>=<setting value>`. Текущие значения параметров вы можете получить с помощью команды вывода параметров проверки контейнеров.

Вывести в консоль текущие значения параметров проверки контейнеров

```
kesl-control --get-container-settings [--json]
```

Где `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Вывести в файл текущие значения параметров проверки контейнеров

```
kesl-control --get-container-settings --file <path to configuration file> [--json]
```

Где:

- `--file <path to configuration file>` – путь к файлу, в который будут сохранены параметры проверки контейнеров. Если вы укажете имя файла, не указав путь к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, файл не будет создан.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Чтобы изменить значения параметров проверки контейнеров с помощью конфигурационного файла:

1. Выведите параметры проверки контейнеров в конфигурационный файл, как описано выше.
2. Измените значения нужных параметров в файле и сохраните изменения.
3. Выполните команду:

   ```
   kesl-control --set-container-settings --file <path to configuration file> [--json]
   ```

   Где:

   - `--file <path to configuration file>` – полный путь к конфигурационному файлу с параметрами проверки контейнеров.
   - `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Все значения параметров проверки контейнеров, заданные в файле, будут импортированы в приложение.

Изменить значения параметров проверки контейнеров с помощью ключей командной строки

```
kesl-control --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Где `<setting name>=<setting value>` – имя и значение одного из параметров проверки контейнеров.

Значения указанных параметров проверки контейнеров будут изменены.

Как сформировать область проверки контейнеров и образов по требованию

Область проверки

Область проверки – список имен контейнеров, которые Kaspersky Endpoint Security проверяет во время выполнения задачи *Проверка контейнеров*.

По умолчанию задача *Проверка контейнеров* проверяет все контейнеры на защищаемом устройстве. Если вам нужно проверять только отдельные контейнеры, вы можете указать их имена или маски имен.

Как сформировать область проверки в Web Console

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

   Откроется список задач.

2. В списке задач выберите задачу проверки контейнеров Kaspersky Endpoint Security и нажмите на название задачи.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. В блоке **Дополнительные настройки проверки** → **Настройки проверки контейнеров** в поле **Маска имени** введите имя контейнера или маску имени контейнера, который вы хотите проверять. По умолчанию проверяются все контейнеры.

5. В блоке **Дополнительные настройки проверки** → **Настройки проверки образов** в поле **Маска имени** введите имя образа контейнера или маску имени образа контейнера, который вы хотите проверять. По умолчанию проверяются все образы.

6. Сохраните внесенные изменения.

Как сформировать область проверки в командной строке

1. Настройте область проверки с помощью следующей команды:

   ```
   kesl-control --set-settings <task ID|name> ScanContainers=Yes ContainerNameMask=<container name or mask>
   ScanImages=Yes ImageNameMask=<image name or mask>
   ```

Где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

- `<container name or mask>` – имя контейнера или маска имени контейнера, который вы хотите проверять. Маски указываются в формате командной оболочки. Вы можете использовать символы `?` и `*`. По умолчанию проверяются все контейнеры.

- `<image name or mask>` – имя образа или маска имени образа, который вы хотите проверять. Маски указываются в формате командной оболочки. Вы можете использовать символы `?` и `*`. По умолчанию проверяются все образы.

2. Также вы можете настроить область проверки с помощью конфигурационного файла:

   a. Выведите параметры задачи в конфигурационый файл с помощью следующей команды:

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Откройте конфигурационный файл для редактирования.

   c. Добавьте в файл следующие параметры:

   - `ScanContainers=Yes` – включить проверку указанных контейнеров.

   - `ContainerNameMask=<container name or mask>` – имя контейнера или маска имени контейнера, который вы хотите проверять. Маски указываются в формате командной оболочки. Вы можете использовать символы `?` и `*`. По умолчанию проверяются все контейнеры.

- `ScanImages=Yes` – включить проверку указанных образов.

- `ImageNameMask=<image name or mask>` – имя образа или маска имени образа, который вы хотите проверять. Маски указываются в формате командной оболочки. Вы можете использовать символы `?` и `*`. По умолчанию проверяются все образы.

```
Пример проверки контейнера с именем my_container

ContainerNameMask=my_container
```

```
Пример проверки всех контейнеров, имена которых начинаются с my_container

ContainerNameMask=my_container*
```

```
Пример проверки всех контейнеров, имена которых начинаются с my_, затем содержат пять любых символов, затем
слово _container и заканчиваются любой последовательностью символов

ContainerNameMask=my_?????_container*
```

```
Пример проверки образов с именем my_image и значением тега latest

ImageNameMask=my_image:latest
```

```
Пример проверки всех образов, имена которых начинаются с my_image_, имеющие любое значения тега

ImageNameMask=my_image*
```

d. Сохраните изменения в конфигурационном файле.

e. Импортируйте параметры из конфигурационного файла в задачу с помощью следующей команды:

```
kesl- <task ID|name> --file <path> [--json]
```

Где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

- `--file <path>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры задачи.

- `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ --json, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Все значения параметров задачи, заданные в файле, будут импортированы в приложение.

Исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Endpoint Security не проверяет объект на вирусы и другие приложения, представляющие угрозу. Исключения из проверки позволяют работать с легальными приложениями, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие приложения не имеют вредоносных функций, но могут быть использованы злоумышленниками. Подробную информацию о легальных приложениях, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского".

Также вы можете исключить из области проверки отдельные доверенные директории, чтобы оптимизировать производительность приложения.

Вы можете исключать из проверки объекты следующими способами:

- **Исключения по маске**. Введите имя файла с помощью маски. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

  Используйте маски:

  - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и директорий в путях к файлам и директориям). Например, маска `/dir/*/*.txt` будет включать все пути к файлам с расширением txt, расположенным в директориях внутри директории dir, но не в поддиректориях.

  - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или директории, включая символы `\` и `/` (разделители имен файлов и директорий в путях к файлам и директориям). Например, маска `/dir/**/*.txt` будет включать все пути к файлам с расширением txt в директориях, вложенных в директорию dir, кроме самой директории dir.

  - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и директорий в путях к файлам и директориям). Например, маска `/dir/???.txt` будет включать пути ко всем расположенным в директории dir файлам с расширением txt и именем, состоящим из трех символов.

- **Исключения по названию угрозы**. Введите название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`). Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, приложение исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

Kaspersky Endpoint Security также позволяет исключать из проверки файлы определенных форматов: архивы, почтовые базы, текстовые файлы, сообщения электронной почты в текстовом формате.

Как добавить исключения из проверки в Web Console

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

   Откроется список задач.

2. В списке задач выберите задачу проверки контейнеров Kaspersky Endpoint Security и нажмите на название задачи.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Области исключения**.

5. При необходимости добавьте исключения по маске:

   a. В блоке **Исключения по маске** нажмите на кнопку **Добавить**.

   b. В открывшемся окне задайте шаблоны для имен файлов, которые Kaspersky Endpoint Security будет исключать из проверки.

   c. Нажмите на кнопку **Добавить**.

   Добавленные исключения отобразятся в списке.

6. При необходимости добавьте исключения по названию угрозы:

   a. В блоке **Исключения по названию угрозы** нажмите на кнопку **Добавить**.

   b. В открывшемся окне задайте шаблоны для названий угроз. Приложение не будет блокировать указанные угрозы.

   Например, если вы используете утилиту для получения информации о сети, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

   Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.

7. При необходимости вы можете импортировать или экспортировать исключения для каждого из списков:

   - Для экспорта списка исключений нажмите на кнопку **Экспортировать**.

     Kaspersky Endpoint Security сохранит в стандартной папке загрузок файл export.json.

   - Для импорта списка исключений выполните следующие действия:

     a. Нажмите на кнопку **Импортировать**.

     b. Выберите JSON-файл, из которого вы хотите импортировать области исключений.

     c. Откройте файл.

     d. Выберите способ импорта: добавить исключения к уже существующему списку или заменить список исключений.

     e. Сохраните внесенные изменения.

     Правила, содержащиеся в JSON-файле, отобразятся в списке.

8. Сохраните внесенные изменения.

Как добавить исключения из проверки в командной строке

1. Добавьте область исключения с помощью следующей команды:

```
kesl-control --set-settings <task ID|name> --add-exclusion <path>
```

где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

- `--add-exclusion <path>` – добавить путь к директории с объектами, которые вы хотите исключить из проверки.

В параметры задачи будет добавлена новая секция `[ExcludedFromScanScope.item_#]`. Приложение будет исключать из проверки объекты в директории, указанной параметром `Path`. Остальные параметры области исключения принимают значения по умолчанию.

Если в параметрах задачи уже есть секция `[ExcludedFromScanScope.item_#]` с указанным значением параметра `Path`, дублирующая секция не добавляется.

Если для параметра `UseScanArea` установлено значение `No`, после выполнения этой команды значение изменится на `Yes` и объекты, расположенные в этой директории, будут исключаться из проверки.

2. Также вы можете добавить область исключения с помощью конфигурационного файла:

   a. Выведите параметры задачи в конфигурационный файл с помощью следующей команды:

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Откройте конфигурационный файл для редактирования.

   c. Добавьте в файл секцию `[ExcludedFromScanScope.item_#]` со следующими параметрами:

   - `AreaDesc` – описание области исключения, содержащее дополнительную информацию об области исключения.

   - `UseScanArea` – включить исключение указанной области.

   - `Path` – путь к директории с исключаемыми объектами. Вы можете указывать путь к локальной директории или исключать удаленные директории, смонтированные на клиентском устройстве. Возможные значения параметра зависят от типа задачи.

   - `AreaMask.item_#` – ограничение области исключения. Вы можете указать маску имени файлов, которые вы хотите исключить из области проверки. По умолчанию исключаются все объекты области.

     Пример

     ```
     [ExcludedFromScanScope.item_0000]
     AreaDesc=
     UseScanArea=Yes
     Path=/tmp/notchecked
     AreaMask.item_0000=*
     ```

   d. Вы можете указать несколько секций `[ExcludedFromScanScope.item_#]`.

   Приложение будет обрабатывать области по индексу в порядке возрастания.

   e. Сохраните изменения в конфигурационном файле.

f. Импортируйте параметры из конфигурационного файла в задачу с помощью следующей команды:

```
kesl-control --set-settings <task ID|name> --file <path>
```

3. При необходимости вы можете удалить область исключения, выполнив команду:

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--del-exclusion <path>` – удалить путь к директории с исключаемыми объектами.

Секция `[ExcludedFromScanScope.item_#]`, содержащая указанный путь, будет удалена из параметров задачи. Приложение не будет исключать из проверки объекты в указанной директории.

Как оптимизировать проверку контейнеров

Настройте проверку файлов, чтобы оптимизировать работу задачи. Это позволит снизить нагрузку на процессор защищаемого устройства. Вы можете ограничить проверку архивов, задать максимальный размер проверяемых объектов и максимальную длительность проверки объектов. Kaspersky Endpoint Security также позволяет исключать файлы определенных форматов: архивы, почтовые базы, текстовые файлы, сообщения электронной почты в текстовом формате.

Как настроить проверку файлов в Web Console

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

   Откроется список задач.

2. В списке задач выберите задачу проверки контейнеров Kaspersky Endpoint Security и нажмите на название задачи.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. В блоке **Настройки проверки** настройте проверку файлов:

   - **Проверять архивы**. Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива). По умолчанию проверка выключена.
   - **Проверять самораспаковывающиеся архивы**. Проверка самораспаковывающихся архивов, которые имеют в своем составе исполняемый модуль-распаковщик. По умолчанию проверка выключена.
   - **Проверять почтовые базы**. Проверка почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. По умолчанию проверка выключена.
   - **Проверять файлы почтовых форматов**. Проверка файлов сообщений электронной почты в текстовом формате. По умолчанию проверка выключена.

- **Пропускать файл, если его проверка длится более (сек.)**. Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра. По умолчанию приложение пытается проверить объект в течение минуты.

- **Пропускать файл, если его размер более (МБ)**. Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.

- **Пропускать файл, если его размер более (МБ)**. Отложенный запуск задач проверки, если проверка уже выполняется. Kaspersky Endpoint Security ставит новые задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, приложение запустило задачу полной проверки по расписанию. Если пользователь пытается запустить быструю проверку в интерфейсе приложения, Kaspersky Endpoint Security поставит задачу быстрой проверки в очередь и автоматически запустит ее после завершения полной проверки.

5. Сохраните внесенные изменения.

Как настроить проверку файлов в командной строке

1. Выполните следующую команду:

```
kesl --set-settings <task ID|name> ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<object size (MB)>
TimeLimit=<scan time (sec)> QueueScanTasks=<Yes|No>
```

где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

- `<object size (MB)>` – максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке. Значение по умолчанию: `0`.

- `<scan time (sec)>` – максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра. Значение по умолчанию: `0`.

2. Также вы можете настроить параметры с помощью конфигурационного файла:

   a. Выведите параметры задачи в конфигурационый файл с помощью следующей команды:

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Откройте конфигурационный файл для редактирования.

   c. Добавьте в файл следующие параметры задачи *Проверка контейнеров*, которые применяются к объектам внутри контейнеров и образов: `ScanArchived`, `ScanSfxArchived`, `ScanMailBases`, `ScanPlainMail`, `SizeLimit`, `TimeLimit`, `QueueScanTasks`.

   d. Сохраните изменения в конфигурационном файле.

e. Импортируйте параметры из конфигурационного файла в задачу с помощью следующей команды:

```
kesl-control --set-settings <task ID|name> --file <path> [--json]
```

где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--file <path>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры задачи.
- `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Все значения параметров задачи, заданные в файле, будут импортированы в приложение.

Как выбрать действие над контейнером при обнаружении зараженного объекта

При обнаружении зараженного объекта в контейнере приложение Kaspersky Endpoint Security может сразу остановить контейнер, не выполнять действий с контейнером или остановить контейнер, если не удалось вылечить зараженный объект или устранить угрозу. Вы можете выбрать действие, которое Kaspersky Endpoint Security будет выполнять над контейнером при обнаружении зараженного объекта, при проверке в режиме реального времени компонентом *Мониторинг контейнеров* или при проверке по требованию задачей *Проверка контейнеров*.

При обнаружении зараженного объекта в образе контейнера приложение Kaspersky Endpoint Security может удалить образ или не выполнять действий над образом. Вы можете выбрать действие, которое Kaspersky Endpoint Security будет выполнять над образом контейнера при обнаружении зараженного объекта, при проверке по требованию задачей *Проверка контейнеров*

Как выбрать действие Мониторинга контейнеров при обнаружении угрозы в Web Console

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

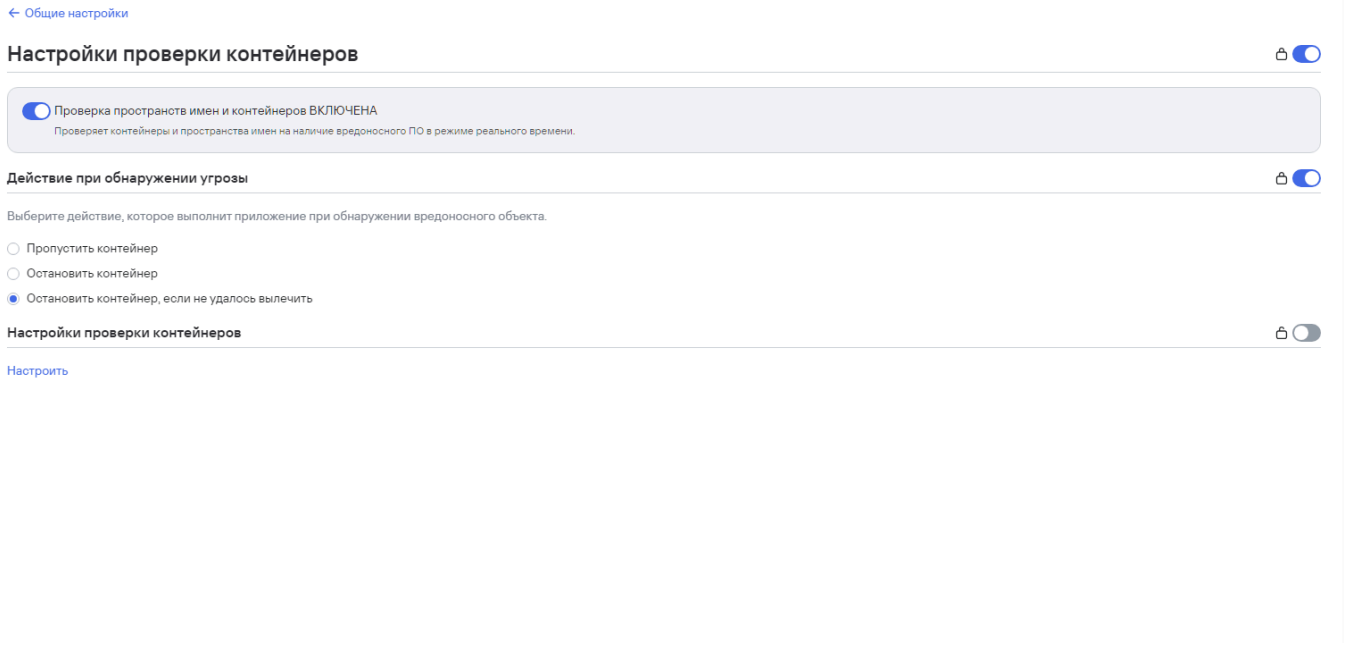
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки проверки контейнеров**.
5. Убедитесь, что переключатель работы компонента Мониторинг контейнеров находится в положении **Проверка пространств имен и контейнеров ВКЛЮЧЕНА**.

6. В блоке **Действие при обнаружении угрозы** выберите действие, которое выполнит приложение при обнаружении зараженного объекта в контейнере:

   - **Пропустить контейнер**. При обнаружении зараженного объекта в контейнере приложение не выполняет никаких действий над контейнером
   - **Остановить контейнер**. При обнаружении зараженного объекта в контейнере приложение останавливает контейнер.
   - **Остановить контейнер, если не удалось вылечить** (по умолчанию). При обнаружении зараженного объекта в контейнере приложение пытается вылечить зараженный объект. Если не удалось вылечить зараженный объект, приложение останавливает контейнер.

   > Из-за особенностей работы среды CRI-O зараженный объект не лечится и не удаляется в контейнере в среде CRI-O. Рекомендуется выбирать действие **Остановить контейнер**.

7. Сохраните внесенные изменения.



Настройки проверки контейнеров

Как выбрать действие Мониторинга контейнеров при обнаружении угрозы в командной строке

1. Выполните следующую команду:

```
kesl-control --set-container-settings OnAccessContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
```

> Настройка этого параметра доступна только при использовании приложения по лицензии, которая включает эту функцию.

2. Для проверки текущих значений параметров проверки контейнеров выполните следующую команду:

```
kesl-control --get-settings container-settings
```

Как выбрать действие Проверки контейнеров при обнаружении угрозы в Web Console

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

   Откроется список задач.

2. В списке задач выберите задачу проверки контейнеров Kaspersky Endpoint Security и нажмите на название задачи.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. В блоке **Дополнительные настройки проверки** → **Настройки проверки контейнеров** → **Действие при обнаружении угрозы** выберите действие, которое выполнит приложение при обнаружении зараженного объекта в контейнере:

   - **Пропустить контейнер**. При обнаружении зараженного объекта в контейнере приложение не выполняет никаких действий над контейнером
   - **Остановить контейнер**. При обнаружении зараженного объекта в контейнере приложение останавливает контейнер.
   - **Остановить контейнер, если не удалось вылечить** (по умолчанию). При обнаружении зараженного объекта в контейнере приложение пытается вылечить зараженный объект. Если не удалось вылечить зараженный объект, приложение останавливает контейнер.

     Из-за особенностей работы среды CRI-O зараженный объект не лечится и не удаляется в контейнере в среде CRI-O. Рекомендуется выбирать действие **Остановить контейнер**.

5. В блоке **Дополнительные настройки проверки** → **Настройки проверки образов** → **Действие при обнаружении угрозы** выберите действие, которое выполнит приложение при обнаружении зараженного объекта в образе:

   - **Пропустить образ** (по умолчанию). При обнаружении зараженного объекта в образе приложение не выполняет никаких действий над образом.
   - **Удалить образ** (не рекомендуется). При обнаружении зараженного объекта в образе приложение удаляет образ. Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.

6. Сохраните внесенные изменения.

Как выбрать действие Проверки контейнеров при обнаружении угрозы в командной строке

1. Выполните следующую команду:

   ```
   kesl-control --set-settings <task ID|name> ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
   ImageAction=<Skip|Delete>
   ```

   Где: `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

   Из-за особенностей работы среды CRI-O зараженный объект не лечится и не удаляется в контейнере в среде CRI-O. Рекомендуется выбирать действие `StopContainer`.

2. Также вы можете настроить действие с помощью конфигурационного файла:

   a. Выведите параметры задачи в конфигурационный файл с помощью следующей команды:

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Откройте конфигурационный файл для редактирования.

   c. Добавьте в файл следующие параметры задачи *Проверка контейнеров*:

   - `ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>` – действие над контейнером при обнаружении зараженного объекта. Значение по умолчанию: `StopContainerIfFailed`.
   - `ImageAction=<Skip|Delete>` – действие над образом контейнера при обнаружении зараженного объекта. Значение по умолчанию: `Skip`.

   d. Сохраните изменения в конфигурационном файле.

   e. Импортируйте параметры из конфигурационного файла в задачу с помощью следующей команды:

   ```
   kesl-control --set-settings <task ID|name> --file <path> [--json]
   ```

   Где:

   - `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
   - `--file <path>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры задачи.
   - `--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Все значения параметров задачи, заданные в файле, будут импортированы в приложение.

Как запустить выборочную проверку контейнеров и образов

Чтобы запустить выборочную проверку контейнеров в командной строке, выполните следующую команду:

```
kesl-control --scan-container <id|name[:tag]>
```

где `<id|name[:tag]>` – имя или идентификатор контейнера или образа. Для проверки нескольких объектов вы можете использовать маски.

Если существует несколько элементов с одинаковым именем, приложение проверяет их все.

В результате выполнения команды создается временная задача проверки контейнеров и образов, которая автоматически удаляется после завершения. При этом в консоль выводятся результаты проверки.

Пример проверки контейнера с именем my_container

```
kesl-control --scan-container my_container
```

Пример проверки образа с именем my_image (все теги)

```
kesl-control --scan-container my_image*
```

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Проверка съемных дисков

Kaspersky Endpoint Security проверяет все файлы, которые вы запускаете или копируете, даже если файл расположен на съемном диске. Приложение проверяет файлы на CD/DVD-приводах, дисках Blu-ray, флеш-накопителях (включая USB-модемы), внешних жестких дисках и дискетах. По умолчанию проверка съемных дисков выключена.

Как работает Проверка съемных дисков

При подключении съемных дисков приложение автоматически создает и запускает следующие задачи проверки с параметрами по умолчанию: *Проверка важных областей* для быстрой проверки и *Поиск вредоносного ПО* для подробной проверки. Эти задачи невозможно остановить. При обнаружении угрозы на съемном диске Kaspersky Endpoint Security пытается вылечить зараженный объект. Если лечение невозможно, приложение удаляет зараженный объект. После завершения проверки приложение автоматически удаляет эти задачи.

Типы проверки

- **Быстрая проверка**. Kaspersky Endpoint Security проверяет только файлы определенных расширений и не распаковывает составные объекты. Приложение выполняет быструю проверку с параметрами, которые заданы по умолчанию для задачи *Проверка важных областей*.

- **Подробная проверка**. Kaspersky Endpoint Security проверяет все файлы на съемных дисках. Приложение выполняет подробную проверку с параметрами, которые заданы по умолчанию для задачи *Поиск вредоносного ПО*.

Как выбрать тип проверки съемных дисков в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз** → **Проверка съемных дисков**.

5. Убедитесь, что переключатель работы компонента находится в положении **Проверка съемных дисков ВКЛЮЧЕНА**.

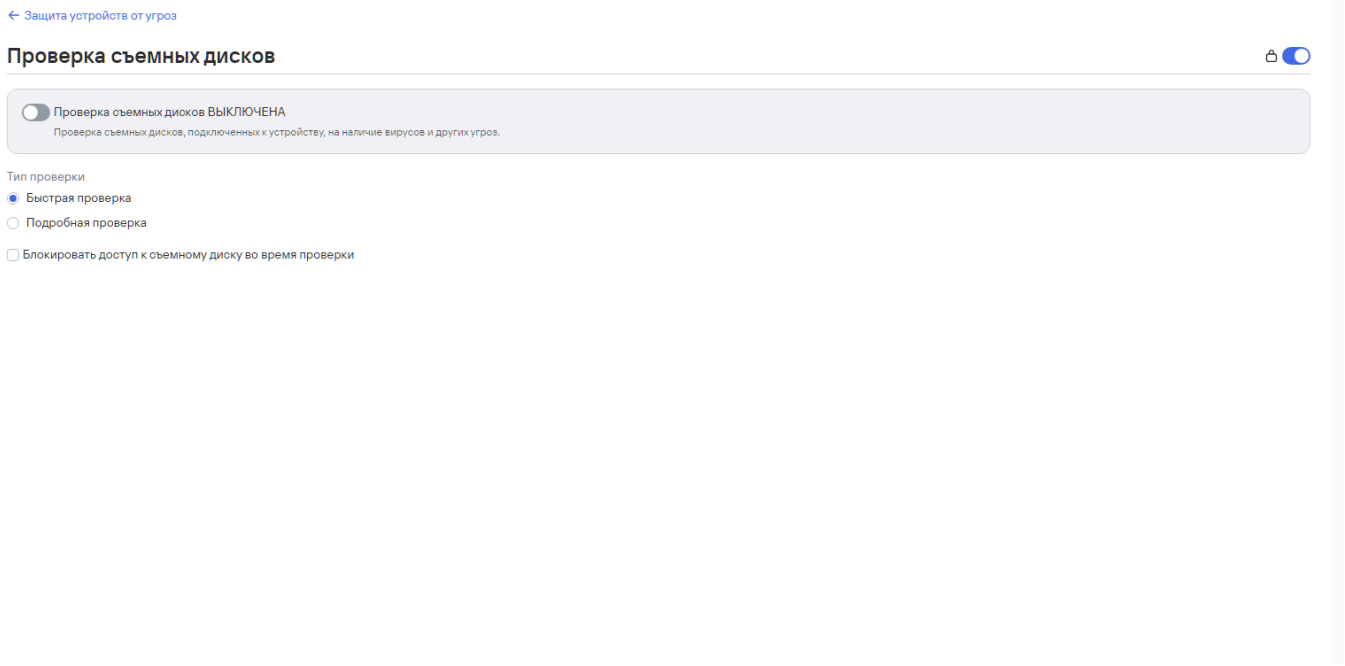
6. В блоке **Тип проверки** выберите тип проверки файлов на съемном диске: **Быстрая проверка** или **Подробная проверка**.

7. Если необходимо, установите флажок **Блокировать доступ к файлам во время проверки**.

   Блокирование доступа к файлам не позволит пользователю запустить вредоносное ПО, пока выполняется проверка.

   При проверке загрузочных секторов приложение не блокирует файлы.

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



Проверка съемных дисков

Как выбрать тип проверки съемных дисков в командной строке

1. Выберите тип проверки при подключении съемных дисков:

```
kesl-control --set-settings 16 ScanRemovableDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

2. Выберите тип проверки при подключении CD/DVD-приводов и дисков Blu-ray:

```
kesl-control --set-settings 16 ScanOpticalDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

3. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 16
```

Условные обозначения

Параметры команды

Параметр	Описание
`ScanRemovableDrives`	Тип проверки при подключении съемных дисков: • `DetailedScan`. Подробная проверка. • `QuickScan`. Быстрая проверка. • `NoScan` (по умолчанию). Приложение не запускает проверку.
`ScanOpticalDrives`	Тип проверки при подключении CD/DVD-приводов и дисков Blu-ray: • `DetailedScan`. Подробная проверка. • `QuickScan`. Быстрая проверка. • `NoScan` (по умолчанию). Приложение не запускает проверку.

Параметр	Описание
`BlockDuringScan`	Блокирование доступа к файлам на подключенном диске при проверке. По умолчанию приложение не блокирует доступ к файлам. Блокирование доступа к файлам не позволит пользователю запустить вредоносное ПО, пока выполняется проверка. При проверке загрузочных секторов приложение не блокирует файлы.

Анализ поведения

Компонент Анализ поведения позволяет контролировать активность приложений, способную нанести вред компьютеру или данным пользователя (открытие файлов, установка соединений и т.п.). Компонент отслеживает шаблоны опасного поведения приложений. Если активность приложения совпадает с одним из таких шаблонов, Kaspersky Endpoint Security выполняет выбранное ответное действие. Эта функциональность Kaspersky Endpoint Security обеспечивает проактивную защиту компьютера.

Для оптимальной работы компонента Анализ поведения рекомендуется включить компонент Защита от веб-угроз.

Как работает Анализ поведения

1. **Приложение отслеживает события в операционной системе**

   Приложение получает поток телеметрии, который состоит из событий: создание и завершение процессов, открытие файлов, установка соединения и т.п. Также приложение обогащает события необходимыми метаданными (имя процесса, PID, IP-адрес и так далее).

2. **Приложение сравнивает поток телеметрии с шаблонами опасного поведения**

   Если действия стороннего приложения совпадают с шаблоном опасного поведения, Kaspersky Endpoint Security выполняет ответное действие при обнаружении угрозы (например, останавливает стороннее приложение).

3. **Приложение отправляет телеметрию в KSN**

   Приложение фильтрует события и отправляет их в KSN для дальнейшего анализа.

Настройка Анализа поведения

1. **В настройках Анализа поведения выберите действие Информировать**

   По умолчанию компонент Анализ поведения включен. Рекомендуем в настройках Анализа поведения в качестве действия при обнаружении угрозы выбрать **Информировать** и проверить работу установленных приложений. Kaspersky Endpoint Security будет разрешать любую активность приложений и вести журнал работы компонента.

Как выбрать действие при обнаружении вредоносной активности в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

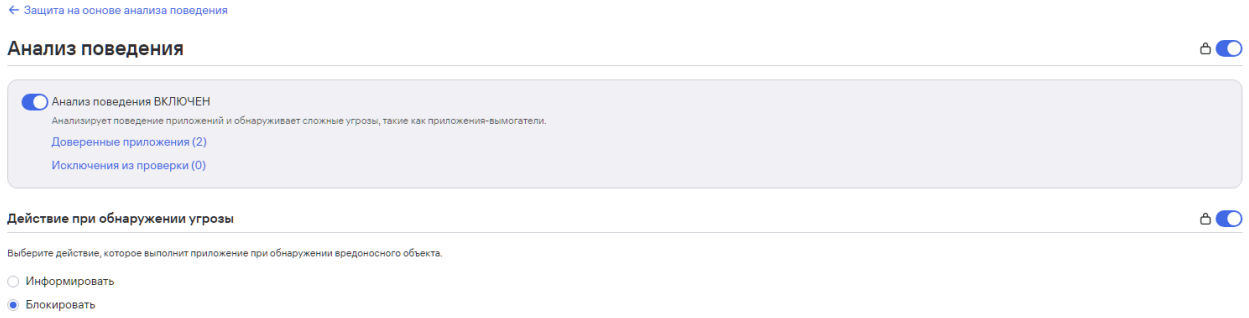
4. Перейдите в раздел **Защита устройств от угроз** → **Защита на основе анализа поведения** → **Анализ поведения**.

5. В блоке **Действие при обнаружении угрозы** выберите нужное действие:

   - **Информировать**. При обнаружении вредоносной активности Kaspersky Endpoint Security не завершает работу этого приложения, а только записывает событие об обнаружении вредоносной активности в журнал событий.

   - **Блокировать**. При обнаружении вредоносной активности Kaspersky Endpoint Security завершает процесс приложения, которое осуществляет вредоносную активность, и записывает в журнал событий информацию об обнаруженной вредоносной активности.

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



Анализ поведения

Как выбрать действие при обнаружении вредоносной активности в командной строке

1. Выполните команду:

```
kesl-control --set-settings 20 TaskMode=<Block|Notify>
```

2. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 20
```

Условные обозначения

Параметры команды

Параметр	Описание
`TaskMode`	Действие при обнаружении вредоносной активности: • `Block` (по умолчанию). При обнаружении вредоносной активности Kaspersky Endpoint Security завершает процесс приложения, которое осуществляет вредоносную активность, и записывает в журнал событий информацию об обнаруженной вредоносной активности. • `Notify`. При обнаружении вредоносной активности Kaspersky Endpoint Security не завершает работу этого приложения, а только записывает событие об обнаружении вредоносной активности в журнал событий.

2. **Соберите статистику работы Анализа поведения**

   Вы можете получить статистику работы Анализа поведения с помощью отчетов.

3. **Оптимизируйте работу приложения**

   После анализа полученной информации оптимизируйте работу приложения и добавьте исключения.

4. **В настройках Анализа поведение выберите действие Блокировать**

   Включите блокировку вредоносной активности приложений. После этого Kaspersky Endpoint Security будет завершать процессы приложений, осуществляющих вредоносную активность.

Особенности и ограничения

- Для корректной работы компонента Анализ поведения при интеграции Kaspersky Endpoint Security с решениями Kaspersky Managed Detection and Response и Kaspersky Anti Targeted Attack Platform убедитесь, что для auditd в конфигурационных файлах установлен режим без блокировки конфигурации `enabled 1`.

Защита от эксплойтов

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на устройстве для получения эксплойтом прав администратора или выполнения вредоносных действий.

Для работы компонента Защита от эксплойтов должны быть запущены следующие компоненты:

- Анализ поведения
- Обновляемый модуль ядра

Компонент недоступен для устройств с процессором Эльбрус.

Как работает Защита от эксплойтов

1. **Приложение отслеживает события в операционной системе**

   Приложение получает поток телеметрии, который состоит из событий: создание и завершение процессов, открытие файлов, установка соединения и т.п. Также приложение обогащает события необходимыми метаданными (имя процесса, PID, IP-адрес и так далее).

2. **Приложение сравнивает поток телеметрии с шаблонами опасного поведения**

   Если действия стороннего приложения совпадают с шаблоном опасного поведения, Kaspersky Endpoint Security выполняет ответное действие при обнаружении угрозы (например, останавливает стороннее приложение).

Настройка Защиты от эксплойтов

1. **В настройках Защиты от эксплойтов выберите действие Информировать**

   По умолчанию компонент Защита от эксплойтов выключен. Рекомендуем в настройках Защиты от эксплойтов в качестве действия при обнаружении угрозы выбрать **Информировать** и проверить работу установленных приложений. Kaspersky Endpoint Security будет разрешать любую активность приложений и записывать в журнал информацию об обнаруженных угрозах.

   Как выбрать действие при обнаружении эксплойта в Web Console

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

      Откроется окно свойств политики.
   3. Выберите вкладку **Параметры приложения**.
   4. Перейдите в раздел **Защита устройств от угроз** → **Защита на основе анализа поведения** → **Защита от эксплойтов**.
   5. Используйте переключатель **Защита от эксплойтов**, чтобы включить или выключить компонент.
   6. В блоке **Действие при обнаружении угрозы** выберите нужное действие:
      - **Блокировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security блокирует операции этого эксплойта и создает в журнале запись, содержащую информацию об этом эксплойте.
      - **Информировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security создает в журнале запись, содержащую информацию об этом эксплойте, и добавляет информацию об этом эксплойте в список активных угроз.
   7. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

   Как выбрать действие при обнаружении эксплойта в командной строке

   1. Для включения Защиты от эксплойтов выполните команду:

      ```
      kesl-control --set-settings 20 UseAEP=Yes
      ```

   2. Выберите действие при обнаружении эксплойта:

      ```
      kesl-control --set-settings 20 AEPMode=<Block|Notify>
      ```

3. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 20
```

Условные обозначения

Параметры команды

Параметр	Описание
`UseAEP`	Включение компонента: • `Yes` – включить Защиту от эксплойтов. • `No` (значение по умолчанию) – выключить Защиту от эксплойтов.
`AEPMode`	Действие при обнаружении эксплойта: • `Block` (по умолчанию). Kaspersky Endpoint Security блокирует операции этого эксплойта и создает в журнале запись, содержащую информацию об этом эксплойте. • `Notify`. Kaspersky Endpoint Security создает в журнале запись, содержащую информацию об этом эксплойте, и добавляет информацию об этом эксплойте в список активных угроз.

2. **Соберите статистику работы Защиты от эксплойтов**

   Вы можете получить статистику работы Защиты от эксплойтов с помощью отчетов.

3. **Оптимизируйте работу приложения**

   После анализа полученной информации оптимизируйте работу приложения:

   - добавьте глобальные исключения
   - добавьте исключения

4. **В настройках Защиты от эксплойтов выберите действие Блокировать**

   Включите блокировку вредоносной активности приложений в операционной системе.

Защита от шифрования

Компонент Защита от шифрования обеспечивает защиту от удаленного шифрования, анализируя активность удаленных устройств в общих сетевых директориях компьютера. Защита от шифрования анализирует файлы, которые передаются на защищаемый компьютер по протоколам NFS и SMB.

Если активность совпадает с одним из шаблонов поведения, характерного для внешнего шифрования, Kaspersky Endpoint Security блокирует эту активность или информирует вас об этом.

Как работает Защита от шифрования

1. **Приложение перехватывает NFS- и SMB-запросы**

   Приложение получает поток телеметрии о создании и изменении файлов, передаваемых по протоколам NFS и SMB.

2. **Приложение сравнивает поток телеметрии с базами сигнатур**

   Если действия стороннего приложения совпадают с шифровальщиком, Kaspersky Endpoint Security выполняет выбранное действие при обнаружении угрозы (например, блокирует соединение с удаленным компьютером).

Настройка Защиты от шифрования

1. **Настройте область защиты**

   По умолчанию приложение проверяет все общие директории. Если вам нужно проверять только отдельную директорию (например, директорию, в которую автоматически загружаются файлы из внешнего источника), вы можете указать только эту директорию в качестве области защиты. В остальных случаях рекомендуем оставить область защиты по умолчанию и оптимизировать область с помощью исключений.

2. **В настройках Защиты от шифрования выберите действие Информировать**

   По умолчанию Защита от шифрования выключена. Рекомендуем включить Защиту от шифрования, в качестве действия при обнаружении угрозы выбрать **Информировать** и проверить доступ ко всем корпоративным ресурсам. Kaspersky Endpoint Security будет разрешать доступ ко всем ресурсам, расположенным в общих директориях, и записывать в журнал информацию об обнаруженных угрозах.

3. **Соберите статистику работы Защиты от шифрования**

   Вы можете получить статистику работы Защиты от шифрования с помощью отчетов.

4. **Оптимизируйте работу приложения**

   После анализа полученной информации оптимизируйте работу приложения:

   - добавьте глобальные исключения;
   - добавьте исключения.

5. **В настройках Защиты от шифрования выберите действие Блокировать соединение**

   Включите блокировку сетевого трафика от удаленного атакующего устройства.

Особенности и ограничения

- Компонент Защита от шифрования корректно работает с протоколами SMB1, SMB2, SMB3, NFS3, TCP/UDP и IP. Работа с протоколами NFS2 и NFS4 не поддерживается. Рекомендуется настроить сервер таким образом, чтобы протоколы NFS2 и NFS4 было невозможно использовать для подключения ресурсов.
- Для корректной работы компонента Защита от шифрования требуется, чтобы в операционной системе была установлена хотя бы одна из служб: Samba или NFS. Для службы NFS требуется установленный пакет rpcbind.
- Kaspersky Endpoint Security не блокирует доступ к сетевым файловым ресурсам, пока действия удаленного устройства не расцениваются как вредоносные. Таким образом, минимум один файл будет зашифрован, прежде чем приложение обнаружит вредоносную активность.

Как выбрать действие при обнаружении вредоносного шифрования

При обнаружении вредоносного шифрования приложение может блокировать сетевой трафик от удаленного атакующего устройства или только информировать об обнаружении вредоносного шифрования.

При блокировании сетевого трафика Kaspersky Endpoint Security создает динамическое правило для сетевого экрана. Сетевой экран временно блокирует сетевой трафик для атакующего устройства. Также приложение добавляет атакующее устройство в список заблокированных. Заблокированным устройствам запрещен доступ к общим сетевым директориям.

Для информирования администратора об обнаружении вредоносного шифрования приложение формирует событие *Обнаружено шифрование*.

По умолчанию приложение блокирует сетевой трафик атакующего устройства на 60 минут. По истечении времени блокировки приложение удаляет это устройство из списка заблокированных устройств, доступ устройства к сетевым файловым ресурсам автоматически восстанавливается.

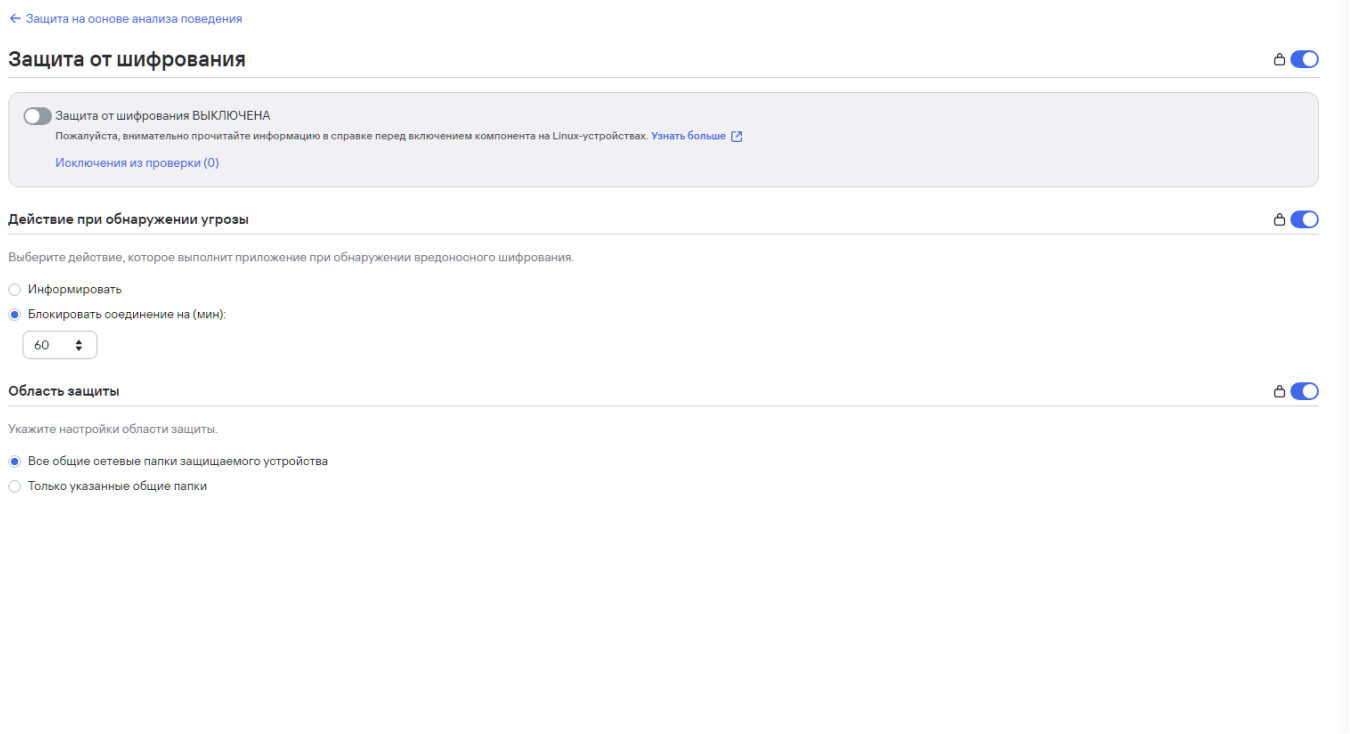
Вы можете посмотреть список заблокированных устройств и вручную разблокировать эти устройства локально на компьютере пользователя. В Kaspersky Security Center нет инструментов мониторинга и управления заблокированными устройствами, кроме событий *Обнаружено шифрование*.

Как настроить действия при обнаружении вредоносного шифрования в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Защита на основе анализа поведения** → **Защита от шифрования**.
5. Убедитесь, что переключатель работы компонента находится в положении **Защита от шифрования ВКЛЮЧЕНА**.
6. В блоке **Действие при обнаружении угрозы** выберите действие, которое выполнит приложение при обнаружении угрозы: **Информировать** или **Блокировать соединение на (мин)**.
7. Если выбран вариант **Блокировать соединение на (мин)**, задайте время блокировки атакующего устройства в минутах. По умолчанию устройство блокируется на 60 минут.

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



Защита от шифрования

Как настроить действия при обнаружении вредоносного шифрования в командной строке

1. Выполните команду:

```
kesl-control --set-settings 13 ActionOnDetect=<Block|Notify>
```

2. Выберите период блокирования для действия `Block`.

```
kesl-control --set-settings 13 BlockTime=<Blocking period>
```

3. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 13
```

Условные обозначения

Параметры команды

Параметр	Описание
`ActionOnDetect`	Действие при обнаружении внешнего шифрования: • `Block` (по умолчанию) – блокировать сетевой трафик для атакующего устройства и создавать событие *Обнаружено шифрование*. • `Notify` – создавать событие *Обнаружено шифрование* и не блокировать сетевой трафик.
`BlockTime`	Период блокировки атакующего устройства в минутах.

Как сформировать область защиты

Область защиты – список путей к общим сетевым директориям, в которых Kaspersky Endpoint Security отслеживает файловую активность. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски. По умолчанию приложение автоматически определяет общие сетевые директории и отслеживает в них файловую активность.

При необходимости вы можете ограничить, в каких директориях приложение будет отслеживать файловую активность на наличие вредоносного шифрования. Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории настройки безопасности могли отличаться от родительской.

Исключение директории из области защиты позволит сократить количество ложных срабатываний, если в вашей организации используется шифрование данных при обмене файлами с помощью общих сетевых директорий. Например, Защита от шифрования 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 общей сетевой директории для защиты данных, добавьте эту директорию в исключения.

Как сформировать область защиты в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Защита на основе анализа поведения** → **Защита от шифрования**.
5. Убедитесь, что переключатель работы компонента находится в положении **Защита от шифрования ВКЛЮЧЕНА**.
6. В блоке **Область защиты** выберите вариант **Только указанные общие папки**.
7. В списке директорий нажмите **Добавить**.
8. В открывшемся окне выберите тип файловой системы:
   - **Локальная**. Директории, расположенные на жестком диске и доступные без сетевого подключения.
   - **Общая**. Директории компьютера, доступные по протоколу Samba (SMB) или NFS.
   - **Все общие**. Все директории компьютера, доступные по протоколам Samba и NFS.
9. Для локальной файловой системы укажите путь к директории (например, `/path/to/folder`).
10. Укажите маски расширений объектов (например, `*.txt`). Разделяйте маски запятой.
11. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как сформировать область защиты в командной строке

1. Выполните команду:

```
kesl-control --set-settings 13 ScanScope.item_#.UseScanArea=Yes \
        [ScanScope.item_#.AreaDesc=<description of the area>] \
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>] \
        [ScanScope.item_#.Path=<path to the directory>]
```

2. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 13
```

Условные обозначения

Параметры команды

Параметр	Описание
`ScanScope.item_#.UseScanArea=Yes`	Включение защиты области с номером `#`. Вы можете временно исключить область защиты для приложения, а не удалять область. Для этого задайте значение `ScanScope.item_#.UseScanArea=No`.
`ScanScope.item_#.AreaDesc`	Описание области защиты, содержит дополнительную информацию об области защиты `#`.
`ScanScope.item_#.AreaMask.item_#`	Ограничение области защиты. В области защиты приложение защищает только объекты, указанные с помощью масок в формате shell. Пример `ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt.`
`ScanScope.item_#.Path`	Путь к директории с защищаемыми объектам. Возможные значения: • `AllShared` (по умолчанию). Все директории компьютера, доступные по протоколам Samba и NFS. • `Shared:SMB`. Директории, доступные по протоколу Samba (SMB). • `Shared:NFS`. Директории, доступные по протоколу NFS. • `<path to local directory>`. Директории, расположенные на жестком диске и доступные без сетевого подключения. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

Пример области защиты, которая включает в себя только директорию /home

```
kesl-control --set-settings 13 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

Защита от атак BadUSB

Злоумышленники могут использовать уязвимости в прошивке USB-устройства (например, флешки) и перепрограммировать его так, чтобы операционная система определяла такое USB-устройство при подключении как клавиатуру. В результате зараженное подключенное USB-устройство может выполнять команды под вашей учетной записью, например, загружать вредоносное приложение.

Компонент Защита от атак BadUSB позволяет предотвратить подключение к устройству зараженного USB-устройства.

Компонент недоступен для устройств с процессором Эльбрус.

Как работает Защита от атак BadUSB

1. **Приложение предлагает авторизовать USB-устройство**

   Когда к устройству подключается USB-устройство, приложение предлагает пользователю ввести цифровой код, сформированный приложением. Эта процедура называется *авторизацией*.

2. **Пользователь вводит код авторизации**

   Пользователь может ввести код с помощью подключаемого USB-устройства (клавиатуры или сканера штрихкодов) или экранной клавиатуры, если она доступна. Нельзя ввести код с помощью уже подключенного USB-устройства.

3. **Приложение разрешает использование авторизованного USB-устройства или блокирует использование USB-устройства, не прошедшего авторизацию**

   Если цифровой код введен правильно, приложение сохраняет идентификационные параметры – VID/PID USB-устройства и номер порта, по которому оно подключено, – в списке авторизованных USB-устройств. Авторизация USB-устройства при его повторном подключении или перезагрузке операционной системы не требуется.

   Если цифровой код введен неправильно, приложение формирует новый. Вы можете настроить максимальное количество попыток для ввода цифрового кода. Если цифровой код введен неправильно несколько раз, приложение блокирует ввод с этого USB-устройства на определенное время. По истечении времени блокировки USB-устройства вы можете продолжить попытки авторизации USB-устройства. Вы можете настроить таймаут, по истечении которого можно продолжить попытки ввода кода авторизации.

При подключении авторизованного USB-устройства через другой USB-порт приложение снова запрашивает его авторизацию.

Настройка Защиты от атак BadUSB

1. **Включите Защиту от атак BadUSB**

   По умолчанию компонент Защита от атак BadUSB выключен. Определите устройства, которые физически доступны недоверенным лицам и которые требуется защитить от внешних злоумышленников, и включите компонент Защита от атак BadUSB на этих устройствах. После включения Защиты от атак BadUSB приложение будет требовать авторизацию подключенных USB-устройств, и пользователь не сможет использовать неавторизованные USB-устройства до тех пор, пока они не будут авторизованы. При этом USB-устройства, подключенные до включения Защиты от атак BadUSB, по умолчанию считаются авторизованными и не требуют авторизации.

   Не подключайте к устройству недоверенные USB-устройства до включения и настройки Защиты от атак BadUSB.

2. **Настройте Защиту от атак BadUSB**

   В зависимости от типа подключаемых USB-устройств (клавиатуры или сканеры штрихкодов), настройте отображение кода авторизации в виде штрихкода или оставьте числовой код, отображаемый по умолчанию.

При необходимости настройте авторизацию USB-устройств:

- максимальное количество попыток ввода кода авторизации;
- время блокировки USB-устройства при достижении максимального количества попыток.

Как настроить авторизацию USB-устройств

Когда к управляемому устройству подключается USB-устройство, определенное операционной системой как устройство ввода, приложение предлагает пройти авторизацию USB-устройства с помощью цифрового кода или штрихкода. Если код авторизации введен неправильно, приложение формирует новый. Если код авторизации введен неправильно несколько раз или закрыто окно авторизации, приложение блокирует ввод с этого USB-устройства. По истечении времени блокировки USB-устройства или перезагрузке операционной системы приложение снова предлагает пройти авторизацию.

Kaspersky Endpoint Security позволяет настроить авторизацию USB-устройств:

- максимальное количество попыток авторизации;
- время блокировки USB-устройства при достижении максимального количества попыток.

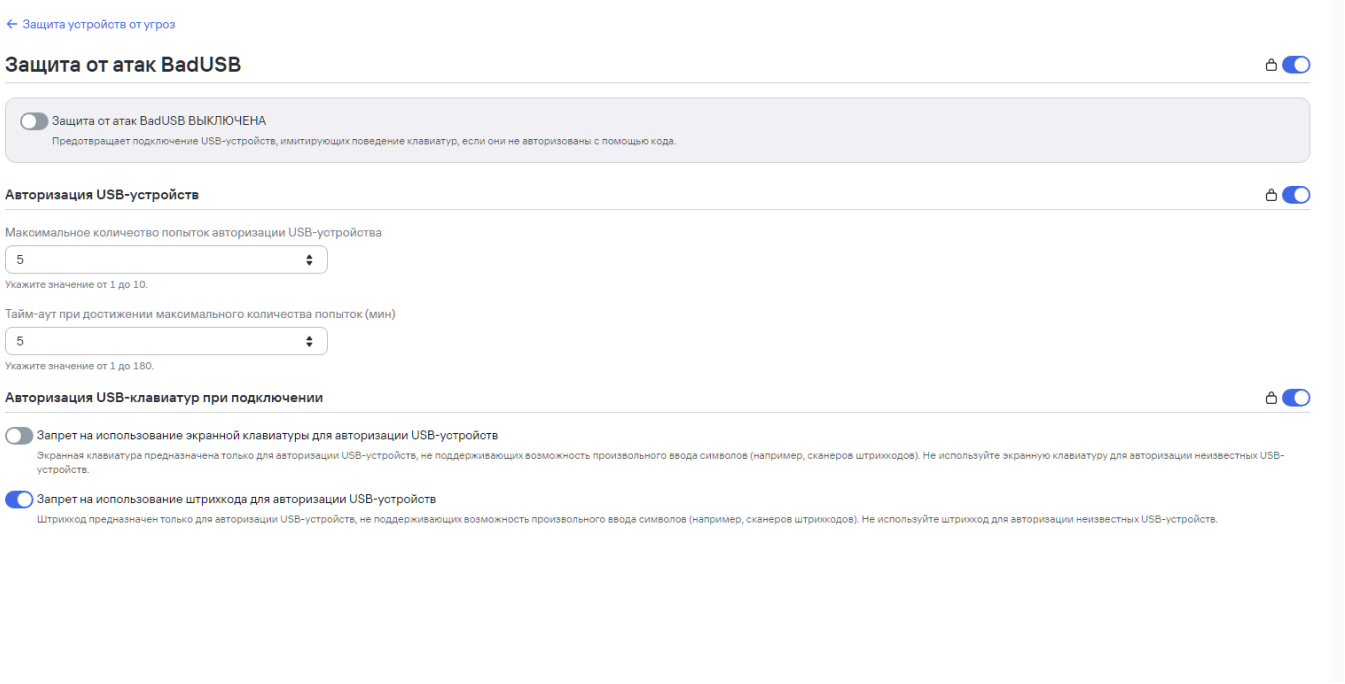
Как настроить авторизацию USB-устройств в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Защита от атак BadUSB**.
5. Убедитесь, что переключатель работы компонента находится в положении **Защита от атак BadUSB ВКЛЮЧЕНА**.
6. В блоке **Авторизация USB-устройств** настройте параметры авторизации:

   - **Максимальное количество попыток авторизации USB-устройства**. Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Endpoint Security покажет время блокировки USB-устройства. По истечении указанного времени вам будут снова доступны 5 попыток ввода кода авторизации.
   - **Тайм-аут при достижении максимального количества попыток (мин)**. Время блокировки USB-устройства после заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).

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



Защита от атак BadUSB

Как настроить авторизацию USB-устройств в командной строке

1. Выполните команду:

```
kesl-control --set-settings 37 MaxAuthAttempts=<number of attempts> TimeoutAfterAttempts=<timeout (minutes)>
```

2. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 37
```

Условные обозначения

Параметры команды

Параметр	Описание
`MaxAuthAttempts`	Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Endpoint Security покажет время блокировки USB-устройства. По истечении указанного времени вам будут снова доступны 5 попыток ввода кода авторизации. Значение по умолчанию: 5.
`TimeoutAfterAttempts`	Время блокировки USB-устройства после заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут). Значение по умолчанию: 5 минут.

Как разрешить подключение USB-устройств с помощью экранной клавиатуры

Возможность использовать экранную клавиатуру предназначена только для авторизации USB-устройств, не поддерживающих произвольный ввод символов (например, сканеров штрихкодов). Не рекомендуется использовать экранную клавиатуру для авторизации неизвестных вам USB-устройств. По умолчанию использование экранной клавиатуры разрешено.

Рекомендуется использовать экранную клавиатуру только для авторизации известных пользователю USB-стройств.

Как разрешить использование экранной клавиатуры при авторизации USB-устройств в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Защита от атак BadUSB**.
5. Убедитесь, что переключатель работы компонента находится в положении **Защита от атак BadUSB ВКЛЮЧЕНА**.
6. Убедитесь, что выключен переключатель **Запрет на использование экранной клавиатуры для авторизации USB-устройств**. По умолчанию переключатель выключен.
7. Для применения политики на устройствах закройте замки 🔒, сохраните внесенные изменения.

Как разрешить использование экранной клавиатуры при авторизации USB-устройств в командной строке

Выполните команду:

```
kesl-control --set-settings 37 ProhibitOnScreenKeyboard=No
```

Как разрешить подключение USB-устройств с помощью сканера штрихкодов

При подключении к устройству сканера штрихкодов компонент Защита от атак BadUSB определяет сканер как устройство ввода и предлагает выполнить процедуру авторизации. Для авторизации сканера штрихкодов вам нужно считать штрихкод с экрана. Приложение формирует штрихкод в формате Code39. Этот формат поддерживают большинство сканеров штрихкодов и сканеров QR-кодов.

Приложение также поддерживает другой способ авторизации сканеров штрихкодов. Если вы используете устройства с сенсорным экраном, для авторизации сканера штрихкодов вы можете ввести код с помощью экранной клавиатуры. Для этого вам нужно разрешить использование экранной клавиатуры. Этот способ удобен, например, для стационарных сканеров штрихкодов в составе кассовых аппаратов. Другие способы авторизации сканеров штрихкодов запрещены. По умолчанию приложение не использует штрихкод для авторизации USB-устройств.

Как разрешить использование сканера штрихкодов при авторизации USB-устройств в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита устройств от угроз** → **Защита от атак BadUSB**.
5. Убедитесь, что переключатель работы компонента находится в положении **Защита от атак BadUSB ВКЛЮЧЕНА**.
6. Выключите переключатель **Запрет на использование штрихкода для авторизации USB-устройств**.
7. Для применения политики на устройствах закройте замки 🔒, сохраните внесенные изменения.

Как разрешить использование сканера штрихкодов при авторизации USB-устройств в командной строке

Выполните команду:

```
kesl-control --set-settings 37 ProhibitBarcodeScanner=No
```

Защита сетевых соединений и средств коммуникации

Защита от почтовых угроз

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других приложений, представляющих угрозу. Компонент обеспечивает защиту устройства с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Защита от почтовых угроз может проверять и получаемые, и отправляемые сообщения. Приложение поддерживает протоколы POP3, SMTP и IMAP во всех почтовых клиентах. Также приложение поддерживает и расширенные версии протоколов – POP3S, SMTPS и IMAPS.

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

> Для работы компонента Защита от почтовых угроз в параметрах сети должны контролироваться сетевые порты 25, 110, 143, 465, 587, 993 и 995. Эти сетевые порты добавлены в список контролируемых по умолчанию. Их удаление из списка может привести к нарушению работы компонента.

По умолчанию компонент Защита от почтовых угроз включен.

Как работает Защита от почтовых угроз

При установке Kaspersky Endpoint Security приложение добавляет самоподписной сертификат – *Kaspersky Anti-Virus Personal Root Certificate*. Приложение помещает этот сертификат в локальное хранилище доверенных сертификатов (`/etc/ssl/certs`). Приложение проверяет наличие сертификата при каждом запуске. Если сертификат был удален, приложение восстанавливает сертификат автоматически.

1. **Приложение перехватывает почтовый трафик**

   Kaspersky Endpoint Security проверяет соединение, проходящее по протоколам POP3, SMTP и IMAP.

2. **Приложение проверяет входящие и исходящие сообщения**

   Защита от почтовых угроз проверяет трафик с помощью следующих технологий:

   - Антивирусные базы
   - Облачные службы Kaspersky Security Network
   - Эвристический анализ – технология позволяет выявлять угрозы, которые еще не внесены в базы данных "Лаборатории Касперского".

3. **Приложение завершает проверку**

   Если входящее сообщение содержит угрозу во вложении или в теле письма, Kaspersky Endpoint Security выполняет действие при обнаружении угрозы. Если угроза обнаружена в исходящем сообщении, Защита от почтовых угроз блокирует отправку такого сообщения.

Настройка Защиты от почтовых угроз

1. **Определите группу для тестового развертывания компонента**

   Выделите небольшую группу устройств, на которых вы проведете тестовую настройку компонента Защита от почтовых угроз. Это позволит убедиться в корректной настройке компонента и обеспечить стабильную работу почтового клиента, избежав возможных сбоев.

2. **Настройте фильтр вложений**

   По умолчанию фильтр вложений Защиты от почтовых угроз настроен специалистами "Лаборатории Касперского" и обеспечивает рекомендуемый уровень защиты. Если у вас особые требования к безопасности почты, вы можете изменить параметры фильтра вложений.

3. **Настройте проверку сообщений**

   Если необходимо, настройте проверку сообщений электронной почты в соответствии с параметрами почтового сервера. Например, вы можете ограничить размер проверяемых архивов, чтобы снизить нагрузку на почтовый сервер.

4. **Проверьте, что Защита от почтовых угроз работает корректно**

   Сформируйте тестовое письмо с вредоносным вложением. Отправьте письмо на электронную почту выделенной группы устройств и убедитесь, что вредоносное содержимое письма обработано согласно настройкам компонента.

   Также вы можете проверить, что приложение сформировало соответствующее событие *Обнаружена угроза*, с помощью команды:

   ```
   kesl-control -E -q "TaskName == 'Mail_Monitoring'"
   ```

5. **Распространите настройки Защиты от почтовых угроз на все устройства в организации**

Особенности и ограничения

- Если почтовый клиент на защищаемых устройствах не использует локальное хранилище доверенных сертификатов, добавьте вручную сертификат *Kaspersky Anti-Virus Personal Root Certificate* в хранилище доверенных сертификатов почтового клиента. Подробнее о добавлении сертификата см. в официальной документации почтового клиента.

- Защита от почтовых угроз не пытается лечить вредоносные вложения в исходящей почте. Исходящие сообщения с вредоносными вложениями либо полностью блокируются, либо пропускаются.

Что делать при обнаружении почтовой угрозы

При обнаружении зараженного объекта во вложении *исходящего сообщения* приложение запрещает его отправку.

При обнаружении зараженного объекта во *входящем сообщении* приложение может попытаться вылечить объект, а затем либо удалить, либо заблокировать доступ к объекту. Kaspersky Endpoint Security также добавляет информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

При настройке Защита от почтовых угроз вы можете выбрать действия, которые будет выполнять Kaspersky Endpoint Security при обнаружении угрозы в сообщениях электронной почты.

Как настроить действия при обнаружении угрозы в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Защита от почтовых угроз**.

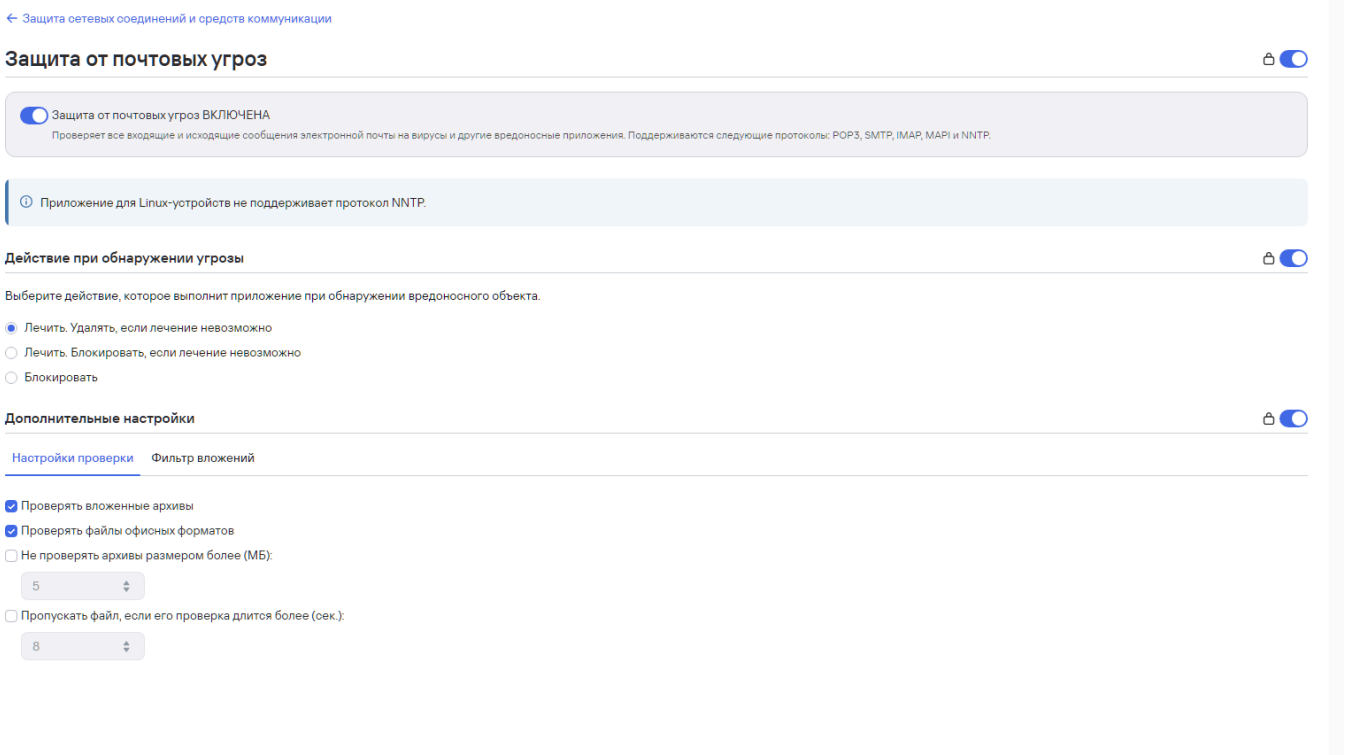
5. В блоке **Действие при обнаружении угрозы** выберите действие, которое выполнит приложение при обнаружении угрозы:

   - **Лечить. Удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

   - **Лечить. Блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

   - **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

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



Защита от почтовых угроз

Как настроить действия при обнаружении угрозы в командной строке

1. Убедитесь, что компонент Защита от почтовых угроз включен:

   ```
   kesl-control --get-task-state 35
   ```

   Компонент должен иметь статус **Запущена**.

2. Если компонент выключен, выполните команду:

   ```
   kesl-control --start-task 35
   ```

3. Выберите действие при обнаружении почтовой угрозы во входящий сообщениях:

   ```
   kesl-control --set-settings 35 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
   ```

4. Для проверки текущих значений параметров компонента выполните следующую команду:

   ```
   kesl-control --get-settings 35
   ```

Условные обозначения

Параметры команды

Параметр	Описание
`ActionOnThreat`	Действие при обнаружении угрозы: • `DisinfectDeleteIfNotPossible` (по умолчанию). При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку. • `DisinfectBlockIfNotPossible`. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку. • `Block`. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку.

Как оптимизировать проверку вложений в сообщениях электронной почты

Настройте проверку вложений электронной почты, чтобы оптимизировать работу компонента Защита от почтовых угроз. Это позволит снизить нагрузку на процессор защищаемого устройства. Вы можете ограничить проверку вложенных архивов, задать максимальный размер проверяемых объектов, вложенных в сообщения, и задать максимальную длительность проверки объектов.

Как оптимизировать проверку вложений в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Защита от почтовых угроз**.
5. В блоке **Дополнительные настройки** перейдите на вкладку **Настройки проверки**.
6. Настройте проверку вложений электронной почты:
   - **Проверять вложенные архивы**. Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).
   - **Проверять файлы офисных форматов**. Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.
   - **Не проверять архивы размером более (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.
   - **Пропускать файл, если его проверка длится более (сек.)**. Если флажок установлен, то время проверки архивов, вложенных в сообщения электронной почты, ограничено указанным периодом.
7. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Как оптимизировать проверку вложений в командной строке

1. Убедитесь, что компонент Защита от почтовых угроз включен:

   ```
   kesl-control --get-task-state 35
   ```
2. Компонент должен иметь статус `Started`.
3. Если компонент выключен, выполните команду:

   ```
   kesl-control --start-task 35
   ```
4. Выберите действие при обнаружении почтовой угрозы во входящий сообщениях:

   ```
   kesl-control --set-settings 35 [ScanFileArchive=<Yes|No>] [UseSizeLimit=<Yes|No>] [SizeLimit=<archive size
   (MB)>] [UseTimeLimit=<Yes|No>] [TimeLimit=<scan time (sec)>] [ScanFileOffice=<Yes|No>]
   ```

5. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 35
```

Условные обозначения

Параметры команды

Параметр	Описание
`ScanFileArchive`	Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива). По умолчанию приложение проверяет вложенные архивы.
`UseSizeLimit` `SizeLimit`	Ограничение размера проверяемых вложенных архивов. Защита от почтовых угроз исключает из проверки вложенные в сообщения электронной почты архивы, размер которых больше заданного. По умолчанию приложение проверяет архивы любого размера.
`UseTimeLimit` `TimeLimit`	Ограничение времени проверки вложенных архивов. По умолчанию время проверки вложенных архивов не ограничено.
`ScanFileOffice`	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка. По умолчанию приложение проверяет вложенные файлы офисных форматов.

Зачем нужен фильтр вложений электронной почты

Фильтр вложений не применяется для исходящих сообщений электронной почты.

Вредоносные приложения могут распространяться в виде вложений в сообщениях электронной почты. Вы можете настроить фильтрацию по типу вложений в сообщениях, чтобы автоматически переименовывать или удалять файлы указанных типов. Переименовав вложение определенного типа, Kaspersky Endpoint Security может защитить ваш компьютер от автоматического запуска вредоносного приложения.

Например, вы можете настроить фильтрацию вложений для HTML-файлов. Файл формата HTML может содержать вредоносные скрипты. Если приложение переименует такой файл, пользователь не сможет открыть HTML-страницу двойным кликом в сообщении электронной почты. Для открытия HTML-файла пользователю нужно будет загрузить файл и переименовать его. Таким образом, у пользователя будет время проанализировать полученное сообщение и предотвратить запуск вредоносного скрипта.

По умолчанию приложение переименовывает файлы с расширениями CMD, COM, EXE, JS, JSE, MSI, SCR, VBE, VBS, SH. Приложение заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_).

Как настроить фильтр вложений в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Защита от почтовых угроз**.

5. В блоке **Дополнительные настройки** перейдите на вкладку **Фильтр вложений**.

6. Выберите действие, которое выполнит приложение над вложением в электронном письме:

   - **Не изменять вложения**. Если выбран этот вариант, компонент Защита от почтовых угроз не фильтрует файлы, вложенные в сообщения электронной почты.

   - **Переименовывать вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_). Таким образом, чтобы открыть файл, пользователю нужно переименовать файл.

   - **Удалять вложения указанных типов**. Если выбран этот вариант, компонент Защита от почтовых угроз удаляет из сообщений электронной почты вложенные файлы указанных типов.

7. Если на предыдущем шаге инструкции вы выбрали вариант **Переименовывать вложения указанных типов** или вариант **Удалять вложения указанных типов**, включите нужные типы файлов.

8. Если в списке нет нужного типа файлов, добавьте новый тип вложения:

   a. Нажмите на кнопку **Добавить**.

   Откроется форма добавления нового типа вложения.

   b. В поле **Типы вложения** укажите маски расширений в формате `*.<extension>` (например, `*.doc`).

   Если вы хотите указать несколько типов файлов, каждый тип файлов нужно вводить с новой строки.

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

Как настроить фильтр вложений в командной строке

1. Убедитесь, что компонент Защита от почтовых угроз включен:

```
kesl-control --get-task-state 35
```

2. Компонент должен иметь статус `Started`.

3. Если компонент выключен, выполните команду:

```
kesl-control --start-task 35
```

4. Выберите действие, которое выполнит приложение над вложением в электронном сообщении:

```
kesl-control --set-settings 35 ExtensionFilter=<Disable|Rename|Delete>
ExtensionMasks.item_#.UseExtensionMask=Yes\
[ExtensionMasks=*.<extention>]
```

5. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 35
```

Условные обозначения

Параметры команды

Параметр	Описание
`ExtensionFilter`	Действие, которое выполнит приложение над вложением в электронном письме: `Disable`. Если выбран этот вариант, компонент Защита от почтовых угроз не фильтрует файлы, вложенные в сообщения электронной почты. `Rename` (по умолчанию). 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. `Delete`. Если выбран этот вариант, компонент Защита от почтовых угроз удаляет из сообщений электронной почты вложенные файлы указанных типов.
`UseExtensionMask=Yes`	Добавление типа файлов в фильтр вложений. Вы можете временно исключить тип файлов из фильтра вложений, а не удалять тип файлов. Для этого задайте значение `ExtensionMasks.item_#.UseExtensionMask=No`
`ExtensionMasks=*.<extention>`	Расширение для типа вложений, которое нужно переименовывать или удалять из сообщений электронной почты.

Защита от веб-угроз

Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует соединение с вредоносными и фишинговыми веб-сайтами. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Как работает Защита от веб-угроз

При установке Kaspersky Endpoint Security приложение добавляет самоподписной сертификат – *Kaspersky Anti-Virus Personal Root Certificate*. Приложение помещает этот сертификат в локальное хранилище доверенных сертификатов (`/etc/ssl/certs`) и в хранилище сертификатов браузеров. Приложение проверяет наличие сертификата при каждом запуске. Если сертификат был удален, приложение восстанавливает сертификат автоматически.

1. **Перехват исходящего соединения**

   Стороннее приложение (например, браузер) инициирует соединение с сервером. Kaspersky Endpoint Security подменяет сертификат сервера собственным сертификатом, подписанным Kaspersky Anti-Virus Personal Root Certificate. Далее приложение перехватывает ключ шифрования и расшифровывает сеанс связи. Kaspersky Endpoint Security делает это незаметно для пользователя, так как Kaspersky Anti-Virus Personal Root Certificate расположен в хранилище доверенных сертификатов.

2. **Проверка сетевого трафика**

   Защита от веб-угроз проверяет трафик с помощью следующих технологий:

   - Антивирусные базы
   - Облачные службы Kaspersky Security Network
   - Эвристический анализ – технология позволяет выявлять угрозы, которые еще не внесены в базы данных "Лаборатории Касперского".

3. **Завершение проверки**

   Если веб-сайт относится к категории вредоносных или фишинговых, Kaspersky Endpoint Security выполняет действие, заданное в параметрах компонента Защита от веб-угроз: блокирует соединение или показывает предупреждение.

Настройка Защиты от веб-угроз

1. **Настройте правила сетевого экрана ОС**

   Если в системе настроены свои сетевые правила или правила firewalld с Drop-политиками, то для корректной работы приложения вам нужно добавить правило для разрешения входящих соединений локального устройства (loopback).

   Пример команды для iptables:

   ```
   iptables -A INPUT -i lo -j ACCEPT
   ```

2. **Выберите режим перехвата сетевого трафика**

   При получении сетевых пакетов Защита от веб-угроз извлекает данные для проверки на наличие угроз. Для перехвата сетевого трафика доступны следующие режимы:

   - eBPF.
   - iptables (по умолчанию).

   Выбор режима перехвата сетевого трафика зависит от инфраструктуры организации. Для закрытого периметра рекомендуем использовать eBPF. В остальных случаях используйте iptables.

   > Рекомендуем разделить устройства по режиму перехвата сетевого трафика в разные группы администрирования.

3. **Настройте политику проверки сертификатов**

   Защита от веб-угроз по умолчанию расшифровывает и проверяет сетевой трафик, передаваемый по защищенным соединениям. При этом компонент может использовать интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата. Если устройство не имеет прямого выхода в интернет, вам нужно выбрать локальный способ проверки сертификатов приложением (без использования интернета) или использовать прокси-сервер для доступа в интернет.

   В политику проверки сертификатов также входят следующие параметры:

   - доступ к веб-сайтам с недоверенным сертификатом;
   - доступ к веб-сайтам с ошибкой проверки сертификата.

   Kaspersky Endpoint Security по умолчанию разрешает переход на домен с недоверенным сертификатом и добавляет домен с ошибкой проверки сертификата в исключения. Ошибки проверки сертификатов могут возникать при работе, например, с банковскими приложениями или облачными хранилищами. Домены, к которым принадлежат эти сервисы, могут отклонить Kaspersky Anti-Virus Personal Root Certificate. Вы можете настроить собственную политику проверки сертификатов.

4. **Добавьте доверенные сертификаты**

   Если ваша организация использует частные Центры сертификации для выпуска сертификатов для внутренних серверов, Kaspersky Endpoint Security может блокировать доступ к веб-ресурсам из-за ошибок проверки сертификатов. Добавьте эти сертификаты в список доверенных, чтобы исключить веб-ресурсы из проверки зашифрованных соединений.

5. **В настройках Защиты от веб-угроз выберите действие Информировать**

   По умолчанию Защита от веб-угроз выключена. Рекомендуем включить Защиту от веб-угроз, в качестве действия при обнаружении угрозы выбрать **Информировать** и проверить доступ ко всем корпоративным ресурсам. Kaspersky Endpoint Security будет разрешать доступ ко всем веб-сайтам и записывать в журнал информацию об обнаруженных угрозах.

6. **Соберите статистику веб-сайтов, которые Защита от веб-угроз считает небезопасными**

   Вы можете получить статистику веб-сайтов, которые Защита от веб-угроз считает небезопасными, с помощью отчетов.

7. **Добавьте доверенные веб-адреса**

   После анализа отчетов о работе Защиты от веб-угроз добавьте веб-адреса, содержанию которых вы доверяете, в список доверенных. Если с помощью списка доверенных веб-адресов не удается разрешить конфликт сетевого взаимодействия Kaspersky Endpoint Security и сторонних приложений, вы можете использовать разрешающую цепочку правил kesl_bypass. *Цепочка kesl_bypass* – это специальный список правил, который приложение Kaspersky Endpoint Security создает в таблице mangle сетевого экрана операционной системы (iptables/ip6tables).

8. **В настройках Защиты от веб-угроз выберите действие Блокировать**

   Включите блокировку зараженных объектов в веб-трафике.

Особенности и ограничения

- Приложение проверяет входящий трафик для TCP-портов и использует для перехвата соединений порт 9879 на localhost. Если порт 9879 занят, то приложение для перехвата соединений автоматически выбирает любой свободный порт.
- Включение или выключение приложения, а также включение или выключение компонентов Защита от веб-угроз и Защита от сетевых угроз приводит к разрыву соединений в перехватываемых портах.
- Kaspersky Endpoint Security проверяет HTTP- и HTTPS-трафик. Kaspersky Endpoint Security проверяет URL- и IP-адреса.
- Приложение поддерживает следующие исполняемые файлы браузеров, в том числе и snap-формата:
  - chrome;
  - chromium;
  - chromium-browser;
  - firefox;
  - firefox-esr;
  - google-chrome;
  - opera;
  - yandex-browser;

- Если пользователь пытается открыть вредоносный сайт, то приложение выполняет следующие действия:
  - **HTTP**. Приложение блокирует доступ и показывает предупреждение.
  - **HTTPS**. Приложение блокирует доступ, браузер показывает страницу с ошибкой.
- Удаление сертификатов приложения может привести к некорректной работе компонента Защита от веб-угроз.

Полезные статьи

Что делать с предупреждением "Переход на домен с недоверенным сертификатом"

Как выбрать действие при обнаружении веб-угрозы

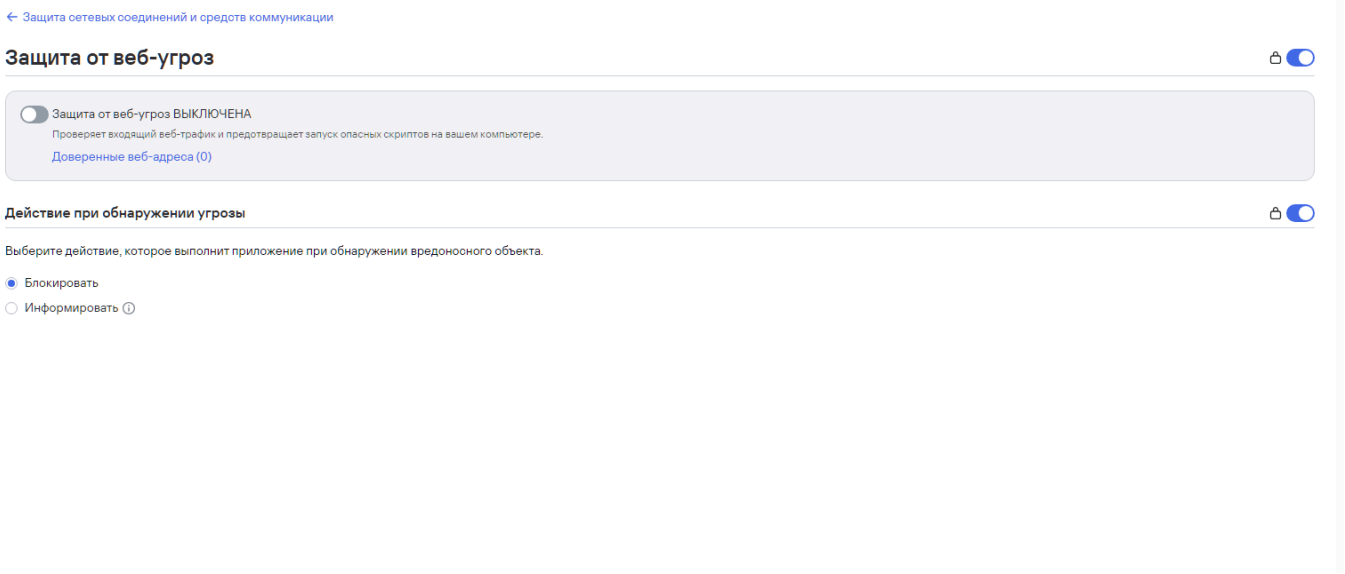
При обнаружении веб-угрозы приложение Kaspersky Endpoint Security может блокировать доступ к опасным объектам или только информировать об обнаружении опасного объекта.

Как настроить действия при обнаружении веб-угроз в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Защита от веб-угроз**.
5. В блоке **Действие при обнаружении угрозы** выберите действие, которое выполнит приложение при обнаружении угрозы:
   - **Блокировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере.
   - **Информировать**. Kaspersky Endpoint Security информирует пользователя об обнаружении зараженного объекта в веб-трафике. Защита от веб-угроз позволяет загрузить объект на устройство. При этом приложение записывает в журнал и добавляет в список активных угроз информацию о зараженном объекте.

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



Защита от веб-угроз

Как настроить действия при обнаружении веб-угроз в командной строке

1. Выполните команду:

```
kesl-control --set-settings 14 ActionOnDetect=<Block|Notify>
```

2. Выберите базы, по которым следует проверять ссылки:

```
kesl-control --set-settings 14 CheckMalicious=<Yes|No> CheckAdware=<Yes|No> CheckOther=<Yes|No>
```

3. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 14
```

Условные обозначения

Параметры команды

Параметр	Описание
`ActionOnDetect`	Действие при обнаружении угрозы: • `Block` (по умолчанию). 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. • `Notify`. 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.
`CheckMalicious`	Проверка ссылок на принадлежность к базе вредоносных веб-адресов позволяет отследить веб-сайты, которые находятся в списке запрещенных веб-адресов. База вредоносных веб-адресов формируется специалистами "Лаборатории Касперского", входит в комплект поставки приложения и пополняется при обновлении баз приложения Kaspersky Endpoint Security. По умолчанию проверка включена (`Yes`).
`CheckAdware`	Проверка ссылок по базе рекламных веб-адресов. По умолчанию проверка выключена (`No`).
`CheckOther`	Проверка ссылок по базе веб-адресов, содержащих легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным. По умолчанию проверка выключена (`No`).

Что такое Анти-Фишинг

Защита от веб-угроз проверяет ссылки на принадлежность к фишинговым веб-адресам. Это позволяет избежать *фишинговых атак*. Частным примером фишинговых атак может служить сообщение электронной почты якобы от банка, клиентом которого вы являетесь, со ссылкой на официальный веб-сайт банка в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его веб-адрес в браузере, однако находитесь на фиктивном веб-сайте. Все ваши дальнейшие действия на веб-сайте отслеживаются и могут быть использованы для кражи ваших денежных средств.

Поскольку ссылка на фишинговый веб-сайт может содержаться не только в сообщении электронной почты, но и, например, в сообщении мессенджера, компонент Защита от веб-угроз отслеживает попытки перейти на фишинговый веб-сайт на уровне проверки веб-трафика и блокирует доступ к таким веб-сайтам. Списки фишинговых веб-адресов включены в комплект поставки Kaspersky Endpoint Security.

Вы можете настроить функцию Анти-Фишинг только с помощью командной строки. Настроить функцию Анти-Фишинг в Web Console невозможно. По умолчанию функция Анти-Фишинг с использованием эвристического анализа включена.

Как включить Анти-Фишинг в командной строке

1. Убедитесь, что компонент Защита от веб-угроз включен:

   ```
   kesl-control --get-task-state 14
   ```

   Компонент должен иметь статус **Запущена**.

2. Если компонент выключен, выполните команду:

   ```
   kesl-control --start-task 14
   ```

3. Включите Анти-Фишинг:

   ```
   kesl-control --set-settings 14 CheckPhishing=Yes
   ```

4. Настройте использование эвристического анализа при проверке веб-страниц на наличие фишинговых ссылок:

   ```
   kesl-control --set-settings 14 UseHeuristicForPhishing=<Yes|No>
   ```

   Параметр неприменим для устройств с процессором Эльбрус.

5. Для проверки текущих значений параметров компонента выполните следующую команду:

   ```
   kesl-control --get-settings 14
   ```

Защита от сетевых угроз

Компонент *Защита от сетевых угроз* (также Intrusion Detection System (IDS) – система обнаружения вторжений) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, приложение блокирует сетевое соединение с атакующим компьютером. Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах приложения. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей приложения.

Как работает Защита от сетевых угроз

1. **Приложение анализирует входящие пакеты**

   Для проверки входящего трафика компонент Защита от сетевых угроз принимает подключения по всем портам, номера которых получает из баз приложения. При проверке сети в режиме перехвата трафика iptables это может выглядеть как открытый порт на устройстве, даже если никакое приложение в системе его не прослушивает. Неиспользуемые порты рекомендуется закрывать средствами сетевого экрана.

2. **Приложение проверяет входящий трафик**

   Защита от сетевых угроз проверяет входящий трафик с помощью следующих технологий:

   - Антивирусные базы
   - Облачные службы Kaspersky Security Network
   - Эвристический анализ – технология позволяет выявлять угрозы, которые еще не внесены в базы данных "Лаборатории Касперского".

3. **Завершение проверки**

   При обнаружении сетевой угрозы приложение блокирует все сетевые соединения от атакующего устройства на определенное время.

Настройка Защиты от сетевых угроз

1. **Настройте правила сетевого экрана ОС**

   Чтобы обеспечить совместимость правил REDIRECT (например, перенаправление с 443 порта на 8443) с правилами перехвата Защиты от сетевых угроз, вам нужно удалить правила REDIRECT и добавить правила перехвата.

   Пример команды удаления правил REDIRECT:

   ```
   iptables -t nat -D PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
   ```

   Пример команд добавления правил перехвата:

   ```
   iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports 8443
   ```

   ```
   iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT -
   -to-destination :8443
   ```

2. **Сформируйте список контролируемых сетевых портов**

   По умолчанию приложение контролирует известные и зарегистрированные порты, например, 443 порт для HTTPS-соединений, 143 порт для работы почтового протокола IMAP и другие. Параметры по умолчанию обеспечивают рекомендуемый уровень защиты и оптимальное потребление ресурсов компьютера. Если нужно, вы можете изменить список контролируемых портов или включить контроль всех портов.

3. **Выберите режим перехвата трафика**

   При получении сетевых пакетов Защита от сетевых угроз извлекает данные для проверки на наличие угроз. Для перехвата входящего трафика доступны следующие режимы:

   - eBPF.
   - iptables (по умолчанию).

   Выбор режима перехвата трафика зависит от инфраструктуры организации. Для закрытого периметра рекомендуем использовать eBPF. В остальных случаях используйте iptables.

   > Рекомендуем разделить устройства по режиму перехвата трафика в разные группы администрирования.

4. **Включите Защиту от веб-угроз в режиме информирования**

   По умолчанию Защита от сетевых угроз выключена. Перед включением Защиты от сетевых угроз в режиме блокирования рекомендуем включить компонент в режиме информирования. Так Kaspersky Endpoint Security не будет нарушать работу сетевых соединений, при этом выявляя подозрительную сетевую активность и записывая в журнал информацию об обнаруженных сетевых атаках. Проверьте доступ сторонних корпоративных приложений к сетевым ресурсам. Убедитесь, что контроль сетевых портов не замедляет работу этих приложений.

5. **Соберите статистику IP-адресов, с которых Защита от сетевых угроз наблюдает подозрительную сетевую активность**

   Вы можете получить статистику IP-адресов, которые Защита от сетевых угроз считает небезопасными с помощью отчетов. Приложение формирует события *Обнаружена сетевая атака*.

6. **Добавьте доверенные IP-адреса**

   После анализа отчетов о работе Защиты от сетевых угроз вам нужно добавить IP-адреса тех устройств, сетевым соединениям с которых вы доверяете, в список доверенных. Вы можете добавить в список исключений адрес конкретного устройства или подсети. Пакеты, приходящие от такого устройства, Защита от сетевых угроз не будет перехватывать и проверять.

7. **Включите Защиту от сетевых угроз в режиме Блокировать**

   После добавления IP-адресов доверенных устройств в список исключений включите компонент в режиме блокирования. Сетевая активность недоверенных устройств будет заблокирована, информация об этом появится в отчетах.

Особенности и ограничения

- Приложение проверяет входящий трафик для TCP-портов. Приложение использует для перехвата соединений фиксированный порт 9789 на localhost.
- Включение или выключение приложения, а также включение или выключение компонентов Защита от веб-угроз и Защита от сетевых угроз приводит к разрыву соединений в перехватываемых портах.
- Защита от сетевых угроз не работает на компьютерах под управлением CentOS 5.2 и 5.4, так как на этих компьютерах отсутствует поддержка механизма TProxy.

Как выбрать действие при обнаружении сетевой угрозы

При обнаружении попытки сетевой атаки на защищаемое устройство приложение блокирует сетевую активность со стороны атакующего устройства и создает событие *Обнаружена сетевая атака*.

При блокировании сетевого трафика Kaspersky Endpoint Security создает динамическое правило для сетевого экрана. Сетевой экран временно блокирует сетевой трафик для атакующего устройства. Также приложение добавляет скомпрометированное устройство в список заблокированных. Заблокированным устройствам запрещен доступ к общим сетевым директориям.

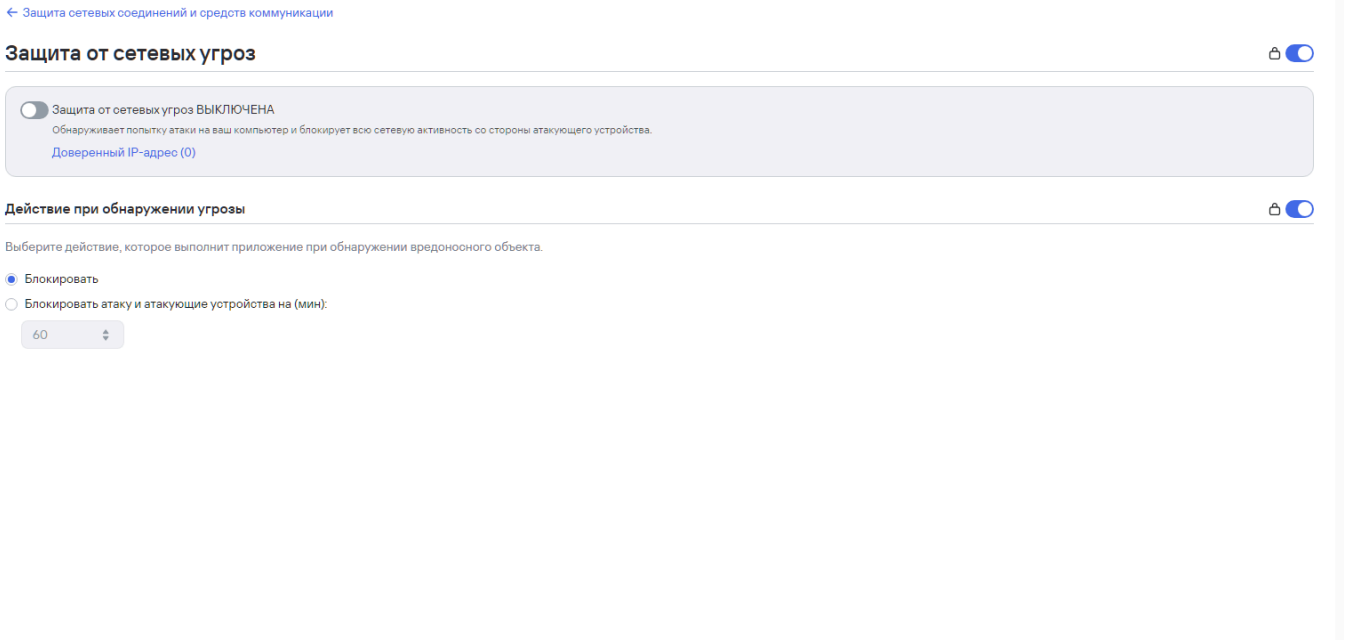
Как настроить действия при обнаружении сетевых атак в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Защита от сетевых угроз**.
5. Убедитесь, что переключатель работы компонента находится в положении **Защита от сетевых угроз ВКЛЮЧЕНА**.
6. Установите флажок **Включить Защиту от сетевых угроз для Linux-устройств**.
7. В блоке **Действие при обнаружении угрозы** выберите действие, которое выполнит приложение при обнаружении угрозы: **Блокировать** или **Блокировать атаку и атакующие устройства на (мин)**.

8. Если выбран вариант **Блокировать атаку и атакующие устройства на (мин)**, задайте время блокировки скомпрометированного устройства в минутах. По умолчанию устройство блокируется на 60 минут. Доступны значения от 1 до 999.

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



Защита от сетевых угроз

Как настроить действия при обнаружении сетевых атак в командной строке

1. Убедитесь, что компонент Защита от сетевых угроз включен:

```
kesl-control --get-task-state 17
```

Компонент должен иметь статус **Запущена**.

2. Если компонент выключен, выполните команду:

```
kesl-control --start-task 17
```

3. Выберите действие при обнаружении сетевой угрозы:

```
kesl-control --set-settings 17 ActionOnDetect=<Block|Notify>
```

4. Настройте блокирование скомпрометированного устройства:

```
kesl-control --set-settings 17 BlockAttackingHosts=<Yes|No>
```

5. Выберите период блокирования для действия `BlockAttackingHosts=Yes`:

```
kesl-control --set-settings 17 BlockDurationMinutes=<Blocking period>
```

6. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 17
```

Условные обозначения

Параметры команды

Параметр	Описание
`ActionOnDetect`	Действие при обнаружении сетевой угрозы: • `Block` (по умолчанию) – блокировать сетевой трафик для скомпрометированного устройства и создавать событие *Обнаружена сетевая атака*. • `Notify` – создавать событие *Обнаружена сетевая атака* и не блокировать сетевой трафик.
`BlockAttackingHosts`	Блокирование сетевой активности атакующего устройства. По умолчанию блокирование устройства включено.
`BlockDurationMinutes`	Период блокировки удаленного устройства, с которого ведется вредоносная активность или шифрование данных.

Как управлять заблокированными устройствами

В ходе защиты устройства от сетевых угроз и от удаленного вредоносного шифрования приложение Kaspersky Endpoint Security может блокировать удаленные устройства, действия которых расцениваются как вредоносные. Защиту устройств от таких типов угроз обеспечивают компоненты Защита от шифрования и Защита от сетевых угроз. Kaspersky Endpoint Security блокирует сетевой трафик временно. По истечению периода блокировки Kaspersky Endpoint Security восстанавливает сетевой трафик. По умолчанию приложение блокирует сетевой трафик атакующего устройства на 60 минут. По истечении времени блокировки приложение удаляет это устройство из списка заблокированных устройств.

Если Kaspersky Endpoint Security заблокировал доверенное устройство, вам нужно добавить IP-адрес этого устройства в список исключений.

Как посмотреть список заблокированных устройств

```
kesl-control -H --get-blocked-hosts
```

В результате выполнения команды приложение выводит список заблокированных устройств в консоль.

Список заблокированных устройств

```
Blocked devices: 1
Host                : 10.69.119.234
Block date          : 2026-04-29 15:44
Will be unblocked   : 2026-04-29 16:44
Task name           : Network_Threat_Protection
```

Как разблокировать устройство

```
kesl-control -H --allow-hosts <address>
```

Где `<address>` – один или несколько IP-адресов устройств или подсетей (IPv4/IPv6, включая адреса в короткой форме). Вы можете указать несколько IP-адресов устройств или подсетей, разделяя их пробелами.

Управление сетевым экраном

Сетевой экран операционной системы контролирует всю сетевую активность устройства во время работы в интернете или локальной сети. Сетевой экран защищает данные на устройстве от несанкционированного доступа и блокирует большую часть угроз, например, попытки атак на устройство из сети. Сетевой экран позволяет обнаружить все сетевые соединения на устройстве пользователя и предоставить список их IP-адресов.

Приложение управляет сетевым экраном операционной системы через компонент Управление сетевым экраном. Компонент добавляет сетевые пакетные правила в сетевой экран операционной системы, чтобы контролировать сетевую активность устройств. С помощью сетевых пакетных правил вы можете задать нужный уровень защиты устройства, от полной блокировки доступа в интернет для всех приложений до разрешения неограниченного доступа.

По умолчанию компонент Управление сетевым экраном выключен.

При включении компонента Управление сетевым экраном приложение Kaspersky Endpoint Security автоматически удаляет все пользовательские правила, настроенные для сетевого экрана средствами операционной системы. После выключения компонента эти правила не восстанавливаются.

Если Управление сетевым экраном включено, Kaspersky Endpoint Security проверяет сетевой экран операционной системы каждые 60 секунд. Если стороннее приложение или утилита добавляет или удаляет сетевое пакетное правило, Kaspersky Endpoint Security после проверки восстанавливает набор правил сетевого экрана, созданных с помощью приложения.

Kaspersky Endpoint Security по-прежнему проверяет сетевой экран операционной системы, когда управление сетевым экраном выключено. Это позволяет приложению восстанавливать динамические правила.

Перед включением компонента Управление сетевым экраном выполните следующие действия:

- Выключите другие средства управления сетевым экраном операционной системы.
- Сохраните пользовательские правила сетевого экрана, настроенные до включения компонента Управление сетевым экраном.

Как создать сетевое пакетное правило

Сетевой экран фильтрует всю сетевую активность на защищаемых устройствах в соответствии с *сетевыми пакетными правилами*. Сетевые пакетные правила ограничивают сетевые пакеты или соединения независимо от приложения. Правила разрешают или запрещают сетевую активность по следующим условиям:

- протокол и порт соединения;
- направление трафика;
- IP-адрес устройства, которое отправляет или принимает сетевой трафик.

Приоритеты сетевых пакетных правил

По умолчанию все исходящие пакеты и соединения разрешены. Правила по умолчанию выполняются с самым низким приоритетом: если не сработало никакое другое сетевое пакетное правило или другие сетевые пакетные правила не указаны, активность разрешается.

Сетевой экран применяет сетевые пакетные правила в соответствие с их приоритетом. Приоритет правил задается порядком их расположения в списке, сверху вниз. Сетевой экран фильтрует сетевое соединение по первому правилу в списке и либо разрешает, либо блокирует сетевую активность. Если правило не подходит, сетевой экран применяет следующее правило и так далее по списку. Затем компонент игнорирует все последующие сетевые пакетные правила для данного сетевого соединения.

Рекомендации по созданию сетевых пакетных правил

Для создания сетевых пакетных правил через командную строку вы можете воспользоваться ключами командной строки или конфигурационным файлом. Если вы хотите добавить несколько правил, добавьте их с помощью конфигурационного файла.

Добавление большого количества правил по одному с помощью ключей командной строки может временно увеличить нагрузку на центральный процессор.

Как создать сетевое пакетное правило в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Сетевой экран**.
5. Убедитесь, что переключатель работы компонента находится в положении **Сетевой экран ВКЛЮЧЕН**.
6. На вкладке **Сетевые пакетные правила** нажмите на кнопку **Добавить**.

   Откроется форма нового сетевого правила (см. рис. ниже).
7. В поле **Имя правила** введите название правила.

   Вы можете выбрать предустановленный шаблон правила по ссылке **Выбрать шаблон правила**. Шаблоны правила содержат настройки наиболее часто используемых сетевых соединений.

   Все настройки сетевого правила, кроме приоритета и действия сетевого экрана над таким соединением, будут заполнены автоматически.
8. В поле **Приоритет** укажите приоритет правила. По умолчанию правило будет создано с высшим приоритетом.
9. В блоке **Действие** выберите, как сетевой экран будет обрабатывать сетевую активность при срабатывании правила: **Разрешать** или **Блокировать**.

10. В поле **Направление** выберите, к какой сетевой активности будет применяется правило:

    - **Входящее**. Сетевой экран применяет сетевое правило ко всем входящим сетевым пакетам.
    - **Входящее (пакет)**. 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.
    - **Входящее / Исходящее (пакеты)**. Сетевой экран применяет сетевое правило ко всем входящим и исходящим сетевым пакетам.

11. Установите флажок **Записывать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете. В соответствии с действием правила приложение создаст событие *Сетевая активность заблокирована* или *Сетевая активность разрешена*.

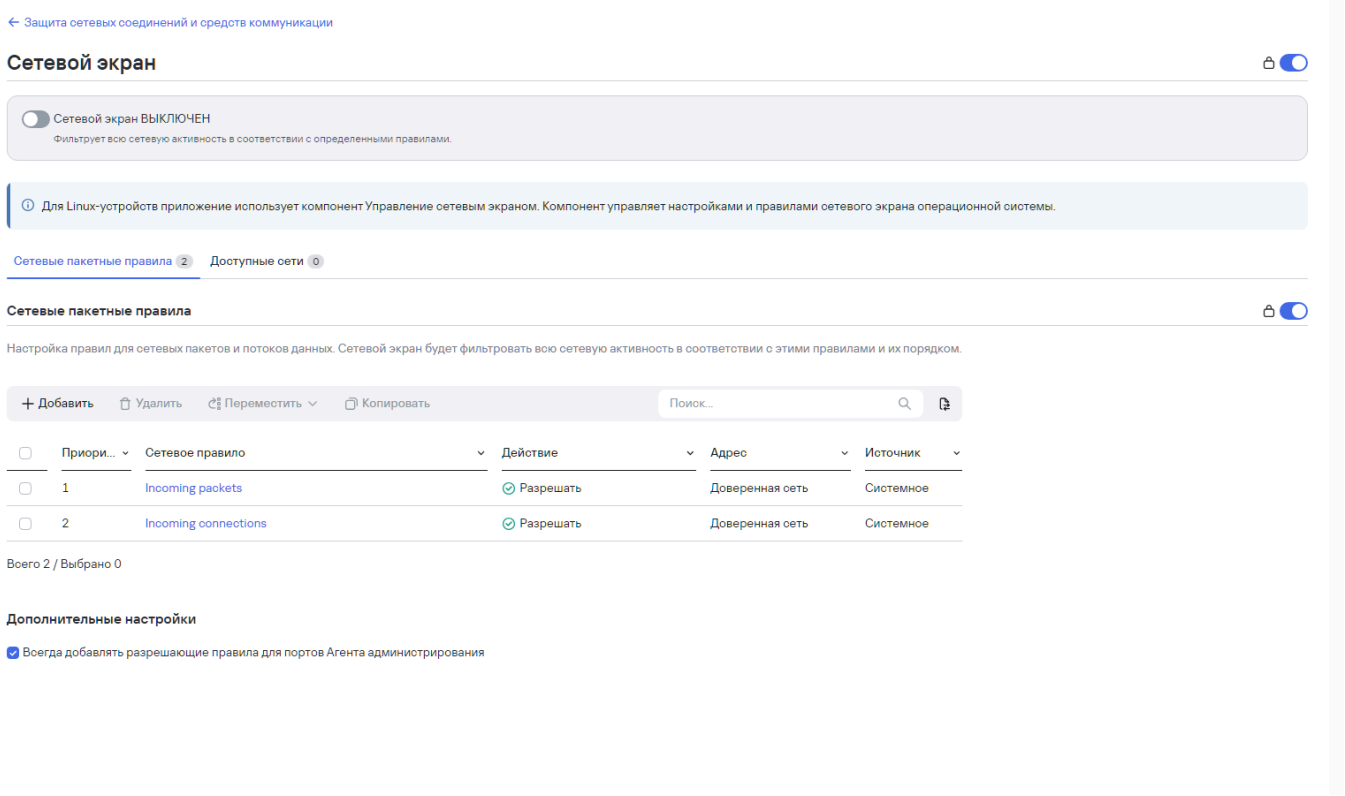
12. На вкладке **Настройки протокола** выберите протокол передачи данных, для которого правило будет фильтровать сетевую активность

13. Перейдите на вкладку **Удаленные сетевые адреса**.

14. В поле **Удаленный** укажите сетевые адреса удаленных компьютеров, которые могут передавать / получать сетевые пакеты. Сетевой экран будет применять правило к указанным адресам.

15. В поле **Локальный** укажите сетевые адреса компьютеров с установленным приложением Kaspersky Endpoint Security, которые могут передавать / получать сетевые пакеты. Сетевой экран будет применять правило к указанным адресам.

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



Сетевой экран

Как создать сетевое пакетной правило в командной строке

1. Убедитесь, что компонент Управление сетевым экраном включен:

```
kesl-control --get-task-state 12
```

Компонент должен иметь статус **Запущена**.

2. Если компонент выключен, выполните команду:

```
kesl-control --start-task 12
```

3. Добавьте новое сетевое пакетное правило:

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

Если вы хотите добавить несколько правил, добавьте их с помощью конфигурационного файла:

a. Выведите параметры компонента в конфигурационный файл:

```
kesl-control --get-settings 12 --file <path to file> [--json]
```

b. Откройте конфигурационный файл и добавьте сетевые пакетные правила секциями следующего вида:

```
[PacketRules.item_#]
Name=<rule name>
FirewallAction=<Allow|Block>
Protocol=<protocol>
Direction=<direction>
RemoteAddress=<remote address>
LocalAddress=<local address>
LogAttempts=<Yes|No>
```

c. Импортируйте настройки конфигурационного файла в приложение:

```
kesl-control --set-settings 12 --file <path to file> [--json]
```

4. Для просмотра списка сетевых пакетных правил выполните команду:

```
kesl-control -F --query
```

Приложение покажет общий список сетевых пакетных правил в следующем формате: `<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`.

Условные обозначения

Параметры команды

Параметр	Описание
`--name <rule name>` `Name`	Название сетевого пакетного правила. По умолчанию `Packet rule #<n>`.
`--action` `FirewallAction`	Действие, применяемое к соединениям, указанным в сетевом пакетном правиле: • `Allow` (по умолчанию) – разрешать соединения; • `Block` – запрещать соединения.
`--protocol` `Protocol`	Тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность: • `Any` (по умолчанию) – сетевой экран контролирует всю сетевую активность. • `TCP` • `UDP` • `ICMP` • `ICMPv6` • `IGMP` • `GRE`
`--direction` `Direction`	Направление отслеживаемой сетевой активности: • `IncomingOutgoing` или `InOut` (по умолчанию). Сетевой экран применяет сетевое правило ко всем входящим и исходящим сетевым пакетам. • `Incoming` или `In`. Сетевой экран применяет сетевое правило ко всем сетевым пакетам в рамках соединения, которое инициировал удаленный компьютер. • `Outgoing` или `Out`. Сетевой экран применяет сетевое правило ко всем сетевым пакетам в рамках соединения, которое инициировал компьютер пользователя. • `IncomingPacket` или `InPacket`. Сетевой экран применяет сетевое правило ко всем входящим сетевым пакетам. • `OutgoingPacket` или `OutPacket`. Сетевой экран применяет сетевое правило ко всем исходящим сетевым пакетам. • `IncomingOutgoingPacket` или `InOutPacket`. 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.

Параметр	Описание
`--remote <remote address[:<port>]>` `RemoteAddress=<remote address>`	Сетевой адрес удаленного устройства: • `Any` (по умолчанию) – контролируется отправка и / или получение сетевых пакетов удаленными устройствами с любым IP-адресом; • `Trusted` – заданная сетевая зона для доверенных сетей; • `Local` – заданная сетевая зона для локальных сетей; • `Public` – заданная сетевая зона для публичных сетей; • `d.d.d.d` – адрес версии IPv4, где d – десятичное число от 0 до 255; • `d.d.d.d – d.d.d.d` – диапазон адресов версии IPv4; • `d.d.d.d/p` – подсеть адресов версии IPv4, где `p` – число от 0 до 32; • `x:x:x:x:x:x:x:x` – адрес версии IPv6, где x – шестнадцатеричное число от 0 до ffff; • `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` – диапазон адресов версии IPv6; • `x:x:x:x:x:x:x:x/p` – подсеть адресов версии IPv6, где `p` – число от 0 до 128, можно использовать `::` для сокращения. Также вы можете указать удаленный порт: • `Any` (по умолчанию) – контролировать все удаленные порты; • `0 – 65535`.
`--local <local address[:<port>]>` `LocalAddress=<local address>`	Сетевой адрес устройства с установленным приложением Kaspersky Endpoint Security: • `Any` (по умолчанию) – контролируется отправка и / или получение сетевых пакетов локальными устройствами с любым IP-адресом; • `Trusted` – заданная сетевая зона для доверенных сетей; • `Local` – заданная сетевая зона для локальных сетей; • `Public` – заданная сетевая зона для публичных сетей; • `d.d.d.d` – адрес версии IPv4, где d – десятичное число от 0 до 255; • `d.d.d.d – d.d.d.d` – диапазон адресов версии IPv4; • `d.d.d.d/p` – подсеть адресов версии IPv4, где `p` – число от 0 до 32; • `x:x:x:x:x:x:x:x` – адрес версии IPv6, где x – шестнадцатеричное число от 0 до ffff; • `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` – диапазон адресов версии IPv6; • `x:x:x:x:x:x:x:x/p` – подсеть адресов версии IPv6, где `p` – число от 0 до 128, можно использовать `::` для сокращения. Также вы можете указать локальный порт: • `Any` (по умолчанию) – контролировать все локальные порты; • `0 – 65535`.
`--at <index>`	Индекс правила в списке сетевых пакетных правил. Если ключ `--at` не указан или его значение больше количества правил в списке, новое правило добавляется в конец списка.
`LogAttempts`	Включение записи в отчет действия сетевого правила. • `Yes` – записывать действия в отчет. • `No` (значение по умолчанию) – не записывать действия в отчет.

Пример правила, блокирующего все входящие и создаваемые соединения по протоколу TCP через порт 23

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote any
```

Пример правила, блокирующего входящие и создаваемые соединения по протоколу TCP через порт 23 для сетевой зоны Публичная

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote Public
```

Примеры использования сетевых пакетных правил

1. **Разрешить доступ в интернет только одному определенному компьютеру локальной сети, а для всех остальных заблокировать доступ**

   Правило для компьютера (192.168.2.22), которому доступ в интернет разрешен по протоколу TCP:

   ```
   kesl-control --add-rule --name InternetAccess --action Allow --protocol TCP --local 192.168.2.22
   ```

   Правило для остальных компьютеров, которым доступ в интернет заблокирован:

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.1.0/24
   ```

2. **Заблокировать доступ в интернет только для одного определенного компьютера локальной сети**

   Правило для компьютера (192.168.2.23), которому заблокирован доступ в интернет:

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.23
   ```

3. **Заблокировать доступ к определенному сайту из локальной сети**

   Правило для компьютеров локальной сети, которым запрещен доступ к сайту example.com (91.198.174.192) по протоколу HTTP:

   ```
   kesl-control --add-rule --name ExampleHTTP --action Block --protocol TCP --remote 91.198.174.192:80
   ```

   Правило для компьютеров локальной сети, которым запрещен доступ к сайту example.com (91.198.174.192) по протоколу HTTPS:

   ```
   kesl-control --add-rule --name ExampleHTTPS --action Block --protocol TCP --remote 91.198.174.192:443
   ```

4. **Разрешить определенному компьютеру локальной сети доступ только к одному указанному сайту**

   Правило для компьютера (192.168.2.24), которому разрешен доступ к сайту example.com (91.198.174.192) по протоколу HTTP:

   ```
   kesl-control --add-rule --name ExampleHTTP --action Allow --protocol TCP --remote 91.198.174.192:80 --local
   192.168.2.24
   ```

   Правило для компьютера (192.168.2.25), которому разрешен доступ к сайту example.com (91.198.174.192) по протоколу HTTPS:

   ```
   kesl-control --add-rule --name ExampleHTTPS --action Allow --protocol TCP --remote 91.198.174.192:443 --local
   192.168.2.25
   ```

   Правило для компьютера (192.168.2.26), которое запрещает доступ в интернет:

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.26
   ```

Как добавить IP-адрес в сетевую зону: Публичная, Локальная, Доверенная

Сетевой экран позволяет контролировать сетевую активность для *сетевых зон*. Сетевая зона – это группа IP-адресов или подсетей, объединенных под одним типом сетевого соединения. С помощью заданной сетевой зоны вы можете использовать одно правило для нескольких IP-адресов или подсетей, не создавая отдельное правило для каждого адреса или подсети.

В Kaspersky Endpoint Security выделяются три сетевые зоны:

- **Публичная сеть**. Сеть не защищена антивирусными приложениями, сетевыми экранами, фильтрами (например, Wi-Fi в кафе). Пользователю компьютера, подключенного к такой сети, Сетевой экран закрывает доступ к файлам и принтерам этого компьютера. Сторонние пользователи также не могут получить доступ к информации через папки общего доступа и удаленный доступ к рабочему столу этого компьютера.

- **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.

Как добавить IP-адрес в сетевую зону в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Сетевой экран**.

5. Перейдите на вкладку **Доступные сети**.

6. Нажмите на кнопку **Добавить**.

   Откроется форма добавления нового сетевого соединения.

7. В поле **Имя** введите название сетевого соединения.

8. В поле **Тип сети** выберите сетевую зону, к которой относится сетевое соединение: **Публичная сеть**, **Локальная сеть**, **Доверенная сеть**.

9. В поле **IP-адрес** укажите IP-адрес или подсеть, которые будут относится к сети.

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

Как добавить IP-адрес в сетевую зону в командной строке

1. Убедитесь, что компонент Управление сетевым экраном включен:

   ```
   kesl-control --get-task-state 12
   ```

   Компонент должен иметь статус **Запущена**.

2. Если компонент выключен, выполните команду:

   ```
   kesl-control --start-task 12
   ```

3. Добавьте адрес в сетевую зону:

   ```
   kesl-control -F --add-zone <Public|Local|Trusted> --address <IP address>
   ```

   Для просмотра списка сетевых пакетных правил выполните команду:

   ```
   kesl-control -F --query
   ```

Условные обозначения

Параметры команды

Параметр	Описание
`--add-zone`	Предустановленная сетевая зона: • `Public`. Публичная сеть. • `Local`. Локальная сеть. • `Trusted`. Доверенная сеть.
`--address`	Сетевой адрес или подсеть.

Пример

```
kesl-control -F --add-zone Local --address 10.28.0.0/24
```

Что такое динамические правила

Приложение Kaspersky Endpoint Security позволяет добавлять и удалять из сетевого экрана *динамические правила*, необходимые для правильной работы приложения. Например:

- Агент администрирования добавляет динамические правила, которые разрешают соединение с Kaspersky Security Center.
- Компонент Защита от шифрования добавляет динамические правила для перехвата трафика по протоколам передачи и хранения файлов NFS и SMB. Это позволяет компоненту блокировать сетевой трафик для устройств, чьи действия приложение расценивает как вредоносное шифрование.
- Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, в сетевой экран автоматически добавляются динамические правила, которые разрешают соединения с SVM и Сервером интеграции.

Kaspersky Endpoint Security автоматически создает динамические правила для доступа компонентов приложения к сетевым ресурсам. Динамические правила не зависят от состояния компонента Управление сетевым экраном (включен/выключен) или от изменения параметров работы компонента. Приоритет выполнения динамических правил выше приоритета сетевых пакетных правил. Приложение восстанавливает набор динамических правил, если какие-либо из них были удалены, например, с помощью утилиты iptables. При аварийном завершении процесса kesl Watchdog-сервером все ссылки на цепочки правил, созданные приложением в процессе работы (кроме kesl-bypass), удаляются из iptables.

Вы можете просмотреть набор динамических правил с помощью команды:

```
kesl-control -F --query
```

Приложение покажет общий список сетевых пакетных правил в следующем формате: `<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`. Динамические правила выделены в отдельные цепочки: `kesl_input`, `kesl_output`, `kesl_prerouting`, `kesl_postrouting`, `kesl_forward`.

Изменить параметры динамических правил невозможно.

Пример

```
ipv4 mangle kesl_output -p tcp -m tcp --dport 80 -m mark ! --mark 0x400/0x400 -m conntrack --ctdir ORIGINAL -m
addrtype ! --dst-type LOCAL -j MARK --set-xmark 0x100/0x100 tag WebAv
```

Как создать правила для соединения с Kaspersky Security Center

Для взаимодействия с Kaspersky Security Center приложение использует Агент администрирования. Для постоянного соединения Агента администрирования с Kaspersky Security Center вам нужно добавить разрешающие правила для портов Агента администрирования. В этом случае, даже если вы неправильно настроили сетевой экран и случайно запретили все соединения, у вас будет возможность удаленно настроить сетевой экран в консоли Kaspersky Security Center.

Набор портов отличается в зависимости от назначения устройства (например, точка распространения). Подробнее о портах, которые будут открыты на компьютере, см. в справке Kaspersky Security Center.

Как добавить разрешающие правила для Агента администрирования в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Защита сетевых соединений и средств коммуникации** → **Сетевой экран**.
5. Убедитесь, что переключатель работы компонента находится в положении **Сетевой экран ВКЛЮЧЕН**.
6. Установите флажок **Всегда добавлять разрешающие правила для портов Агента администрирования**.
7. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как добавить разрешающие правила для Агента администрирования в командной строке

1. Убедитесь, что компонент Управление сетевым экраном включен:

   ```
   kesl-control --get-task-state 12
   ```

   Компонент должен иметь статус **Запущена**.

2. Если компонент выключен, выполните команду:

   ```
   kesl-control --start-task 12
   ```

3. Выполните команду:

   ```
   kesl-control --set-settings 12 OpenNagentPorts=Yes
   ```

4. Для проверки текущих значений параметров компонента выполните следующую команду:

   ```
   kesl-control --get-settings 12
   ```

Контроль безопасности

Контроль устройств

Контроль устройств управляет доступом пользователей к устройствам, установленным или подключенным к клиентскому устройству (например, к жестким дискам, камерам или модулям Wi-Fi). Это позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных.

Как работает Контроль устройств

По умолчанию компонент Контроль устройств включен с предзаданными настройками.

1. **Пользователь пытается получить доступ к устройству**
2. **Контроль устройств управляет доступом на следующих уровнях:**
   - **Тип устройства** по классификации компонента Контроль устройств (например, принтеры, съемные диски, CD/DVD-приводы). Для каждого типа устройств может применяться один из следующих *режимов доступа*:
     - *Разрешать* – предоставлять доступ к устройствам этого типа.
     - *Запрещать* – запрещать доступ к устройствам этого типа.

- *Зависит от шины* – разрешать или запрещать доступ к устройствам в зависимости от режима доступа для шины, по которой подключено устройство.
- *Пользовательское* – разрешать или запрещать доступ к устройствам в зависимости от правил доступа к устройствам.
- *Только чтение* – разрешать доступ к устройствам выбранного типа только на чтение, при этом запись будет запрещена.

- **Шина подключения**. *Шина подключения* – это интерфейс, с помощью которого устройства подключаются к клиентскому устройству (например, USB, FireWire). Для шин подключения может применяться один из следующих режимов доступа:
  - *Разрешать* – предоставлять доступ к устройствам, подключенным по этой шине подключения.
  - *Запрещать* – запрещать доступ к устройствам, подключенным по этой шине подключения.

Например, может быть запрещен доступ ко всем устройствам, подключенным по шине USB.

3. **Завершение проверки**

   Если устройство, к которому пытается получить доступ пользователь, не является доверенным для этого пользователя, или у пользователя нет разрешения на доступ к устройству в соответствии с режимом доступа, приложение заблокирует доступ к устройству этому пользователю.

   Пользователь может отправить запрос администратору организации об ошибочной блокировке, если доступ, по мнению пользователя, заблокирован ошибочно, или может запросить временный доступ к устройству.

При выключении компонента Контроль устройств приложение разблокирует доступ к заблокированным устройствам.

Настройка Контроля устройств

1. **Настройте доверенные устройства**

   Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства. Вы можете предоставить доступ к доверенными устройствам отдельному пользователю, группе пользователей или всем пользователям организации. Например, вы можете разрешить доступ к конкретным USB-устройствам или только к USB-накопителям, при этом доступ к остальным USB-устройства будет запрещен.

2. **Настройте режим доступа**

   Вы можете настроить режим доступа для типов устройств и для шин подключения. По умолчанию для всех типов устройств выбран режим доступа *Зависит от шины*, для шин подключения выбран режим доступа *Разрешать*. В соответствии с этими параметрами Контроль устройств предоставляет пользователям полный доступ ко всем устройствам.

3. **Настройте правила доступа**

   Для устройств хранения данных (жесткие диски, съемные диски, дискеты и CD/DVD-приводы) вы можете настроить *правила доступа* к устройству.

4. **Настройте шаблон сообщения**

   При необходимости вы можете настроить текст шаблона сообщений пользователю о запрете доступа к устройству или о запрете операции с устройством.

5. **Настройте получение временного доступа к устройству**

   Если требуется, настройте возможность получения пользователем временного доступа к заблокированному устройству.

Особенности и ограничения

- При первом включении компонента Контроль устройств для всех обнаруженных устройств с известным типом устройства или шины формируется событие *Доступ к устройству разрешен*, при следующих запусках повторные события для этих устройств не формируются, если не было изменений в параметрах контроля для этих устройств.
- Контроль устройств не блокирует системные диски. Если приложению не удалось автоматически определить системный диск, работа компонента Контроль устройств завершается с ошибкой.
- Блокировка устройств по типу устройства и по шине подключения через системный драйвер устройства не поддерживается на ядрах ОС Linux: 3.10, 5.14, 5.15, 5.17, 6.1, 6.8. На этих ядрах, а также при режиме доступа *По правилам* блокируются только открытие файлов и чтение директорий (то есть получение имен файлов и директорий). На системах, не поддерживающих технологию fanotify, не поддерживается блокировка чтения директорий.
- Контроль устройств игнорирует исключение точек монтирования. Доступ к устройству, смонтированному в исключенной точке монтирования, может быть ограничен в соответствии с настроенными параметрами Контроля устройств.
- Если в общих параметрах приложения выключена блокировка доступа к файлам во время проверки, то заблокировать доступ к устройствам с помощью расписания доступа для устройств невозможно.

Как управлять списком доверенных устройств в командной строке

Список доверенных устройств содержит информацию об устройствах, к которым разрешен доступ (для определенных пользователей или групп).

В командной строке вы можете просматривать список доверенных устройств, добавлять в него устройства и удалять из него устройства, а также импортировать список доверенных устройств из файла.

Просмотреть список доверенных устройств

```
kesl-control --trusted-devices --list
```

Добавить устройство в список доверенных устройств

```
kesl-control --trusted-devices --add <device id or mask>
```

где `<device id or mask>` – идентификатор устройства или маска идентификатора устройства.

Удалить устройство из списка доверенных устройств

```
kesl-control --trusted-devices --delete <device id or mask>
```

где `<device id or mask>` – идентификатор устройства или маска идентификатора устройства.

```
Импортировать список доверенных устройств из файла

kesl-control --trusted-devices --merge|--add|--replace --file <file>
```

где:

- `--merge` – объединять списки доверенных устройств при импорте. Если в текущем списке и в импортируемом списке есть записи для устройства с одним и тем же идентификатором, то параметры существующей записи изменяются. Для устройств, которых нет в текущем списке, записи добавляются.
- `--add` – дополнять текущий список доверенных устройств при импорте. В список устройств добавляются только записи для устройств, которых ранее не было.
- `--replace` – заменять текущий список доверенных устройств. Существующий список доверенных устройств заменяется импортируемым списком.
- `--file <file>` – полный путь к файлу в формате JSON, из которого будет импортирован список доверенных устройств.

Как настроить режим доступа к устройствам

Для каждого типа устройств (по классификации компонента Контроль устройств, например, принтеры, съемные диски, CD/DVD-приводы) может применяться один из следующих *режимов доступа*:

- *Разрешать* – предоставлять доступ к устройствам этого типа.
- *Запрещать* – запрещать доступ к устройствам этого типа.
- *Зависит от шины* – разрешать или запрещать доступ к устройствам в зависимости от режима доступа для шины, по которой подключено устройство.
- *Пользовательское* – разрешать или запрещать доступ к устройствам в зависимости от правил доступа к устройствам. *Правило доступа к устройству* – это набор параметров, которые определяют, какие пользователи и в какое время могут получить доступ к устройствам, установленным на клиентском устройстве или подключенным к нему. Этот режим доступа можно указать только для устройств хранения данных (жесткие диски, съемные диски, дискеты, CD/DVD-приводы).
- *Только чтение* – разрешать доступ к устройствам выбранного типа только на чтение, при этом запись будет запрещена. Этот режим доступа можно указать только для устройств хранения данных (жесткие диски, съемные диски, дискеты, CD/DVD-приводы). Если для устройства назначен тип доступа "Только чтение", при назначении доверенного устройства на определенного пользователя, назначенный пользователь игнорируется и устройство становится доступным для записи всем пользователям.

Как настроить режим доступа для типов устройств в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности** → **Контроль устройств**.

5. Убедитесь, что переключатель работы компонента находится в положении **Контроль устройств ВКЛЮЧЕН**.

6. В блоке **Правила доступа к устройствам** в таблице выберите вкладку **Устройства и сети Wi-Fi**.

7. В столбце **Имя** выберите тип устройства, для которого вы хотите настроить режим доступа.

8. В раскрывающемся списке **Доступ** выберите один из режимов доступа:

   - **Разрешать** – разрешать доступ к устройствам выбранного типа.

   - **Запрещать** – запрещать доступ к устройствам выбранного типа.

   - **Зависит от шины** (значение по умолчанию) – разрешать или запрещать доступ к устройствам в зависимости от режима доступа для шины подключения.

   - **Пользовательское** – разрешать или запрещать доступ к устройствам в зависимости от правила доступа и расписания. Этот вариант доступен только для устройств хранения данных (Жесткие диски, Съемные диски, Дискеты, CD/DVD-приводы).

   - **Только чтение** – разрешать доступ к устройствам выбранного типа только на чтение. Этот вариант доступен только для устройств хранения данных (Жесткие диски, Съемные диски, Дискеты, CD/DVD-приводы).

9. В таблице ниже нажмите на кнопку **Добавить**.

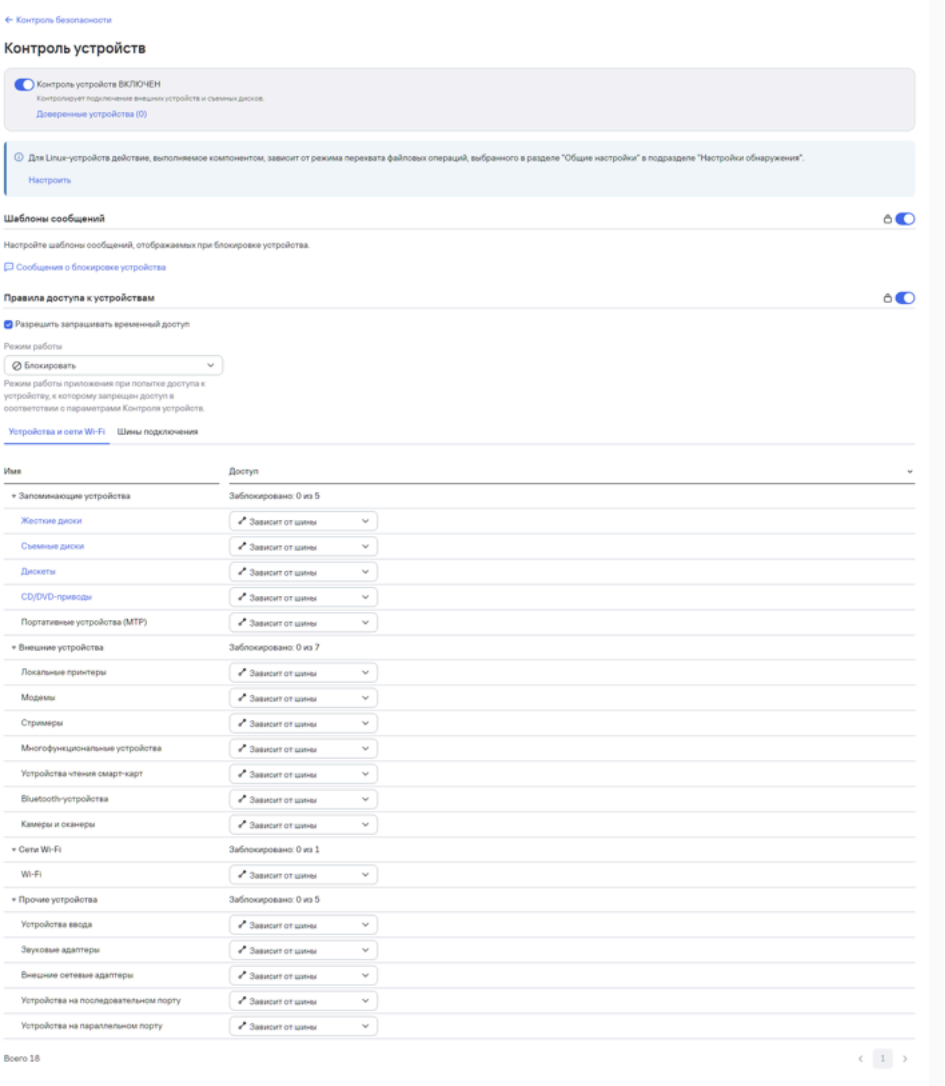
   Откроется окно добавления правила доступа.

10. В поле **Приоритет** задайте приоритет правила доступа.

11. Выберите пользователей или группу пользователей, для которых будет применяться правило доступа. По умолчанию правило применяется ко всем пользователям.

12. Если необходимо, задайте расписание доступа. По умолчанию правило применяется всегда.

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



Контроль устройств

Как настроить режим доступа для типов устройств в командной строке

1. Убедитесь, что компонент Контроль устройств запущен:

```
kesl-control --get-task-list
```

Компонент должен иметь статус **Запущена**.

2. Если компонент выключен, выполните команду:

```
kesl-control --start-task 15
```

3. Выберите режим работы при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств:

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

4. Укажите режим доступа для одного из типов устройств: `HardDrive`, `RemovableDrive`, `FloppyDrive`, `OpticalDrive`, `SerialPortDevice`, `ParallelPortDevice`, `Printer`, `Modem`, `TapeDrive`, `MultifuncDevice`, `SmartCardReader`, `WiFiAdapter`, `NetworkAdapter`, `PortableDevice`, `PortableDevice`, `BluetoothDevice`, `ImagingDevice`, `SoundAdapter`, `InputDevice`

```
kesl-control --set-settings 15 DeviceClass.<device type>=<Allow|Block>
```

5. Для просмотра параметров Контроля устройств выполните команду:

```
kesl-control --get-settings 15
```

Как настроить режим доступа к шине подключения в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль устройств**.
5. Убедитесь, что переключатель работы компонента находится в положении **Контроль устройств ВКЛЮЧЕН**.
6. В блоке **Правила доступа к устройствам** в таблице выберите вкладку **Шины подключения**.
7. В столбце **Имя** выберите шину, для которой вы хотите настроить режим доступа.
8. В раскрывающемся списке **Доступ** выберите один из режимов доступа:
   - **Разрешать** – предоставлять доступ к устройствам, подключенным по этой шине подключения.
   - **Запрещать** – запрещать доступ к устройствам, подключенным по этой шине подключения.
9. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Как настроить режим доступа к шине подключения в командной строке

1. Убедитесь, что компонент Контроль устройств запущен:

   ```
   kesl-control --get-task-list
   ```

   Компонент должен иметь статус **Запущена**.
2. Если компонент выключен, выполните команду:

   ```
   kesl-control --start-task 15
   ```

3. Выберите режим работы при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств:

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

4. Укажите режим доступа для шин подключения:

```
kesl-control --set-settings 15 DeviceBus.USB=<Allow|Block>
kesl-control --set-settings 15 DeviceBus.FireWire=<Allow|Block>
```

5. Для просмотра параметров Контроля устройств выполните команду:

```
kesl-control --get-settings 15
```

Как настроить правила доступа к устройствам

Для устройств хранения данных (жесткие диски, съемные диски, дискеты и CD/DVD-приводы) вы можете настроить правила доступа к устройству. *Правило доступа к устройству* – это набор параметров, которые определяют, какие пользователи и в какое время могут получить доступ к устройствам, установленным на клиентском устройстве или подключенным к нему. Этот режим доступа можно указать только для устройств хранения данных (жесткие диски, съемные диски, дискеты, CD/DVD-приводы). При подключении устройства, доступ к которому запрещен, приложение запрещает указанным в правиле пользователям доступ к этому устройству и выводит уведомление. При попытке чтения и записи на этом устройстве приложение запрещает чтение/запись указанным в правиле пользователям без вывода уведомления. Если при попытке совершить операцию с устройством, для которого установлен режим доступа *По правилам*, не нашлось правила, активного на момент доступа, операция с устройством будет запрещена.

Как настроить правило доступа к устройству в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль устройств**.
5. Убедитесь, что переключатель работы компонента находится в положении **Контроль устройств ВКЛЮЧЕН**.
6. В блоке **Правила доступа к устройствам** в таблице выберите вкладку **Устройства и сети Wi-Fi**.
7. В столбце **Имя** выберите тип устройства хранения данных, для которого вы хотите добавить правило доступа (жесткие диски, съемные диски, дискеты, CD/DVD-приводы).
8. В открывшемся окне в блоке **Правила доступа к устройствам** выберите **Пользовательское**.
9. В таблице ниже нажмите на кнопку **Добавить**.

   Откроется окно добавления правила доступа.

10. В поле **Приоритет** задайте приоритет правила доступа.

11. Выберите пользователей или группу пользователей, для которых будет применяться правило доступа. По умолчанию правило применяется ко всем пользователям.

12. Если необходимо, задайте расписание доступа. По умолчанию правило применяется всегда.

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

Как настроить правило доступа к устройству в командной строке

1. Убедитесь, что компонент Контроль устройств запущен:

```
kesl-control --get-task-list
```

   Компонент должен иметь статус **Запущена**.

2. Если компонент выключен, выполните команду:

```
kesl-control --start-task 15
```

3. Для просмотра параметров Контроля устройств выполните команду:

```
kesl-control --get-settings 15
```

4. Выберите режим работы при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств:

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

5. Добавьте новое правило доступа для одного из типов устройств: `HardDrivePrincipals.item_#.AccessRules.item_#`, `RemovableDrivePrincipals.item_#.AccessRules.item_#`, `FloppyDrivePrincipals.item_#.AccessRules.item_#` или `OpticalDrivePrincipals.item_#.AccessRules.item_#`.

   - Включите правило и укажите расписание по умолчанию:

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.UseRule=Yes
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.ScheduleName=Default
     ```

     Пример

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - Задайте действие Контроля устройств при срабатывании правила:

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.Access=Allow|Block
     ```

     Пример

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.Access=Allow
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - Если необходимо, укажите пользователей, для которых будет применяться правило:

     ```
     kesl-control --set-settings 15 <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.Principal=<Name>=
     <\Everyone|user name|@group name>
     ```

     Пример

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.Principal=\Everyone
     ```

   - Если необходимо, измените расписание правила:

     ```
     kesl-control --set-settings 15 Schedules.item_#.ScheduleName=<Name> Schedules.item_#.DaysHours=<All|day of
     the week|hour>
     ```

     Пример

     ```
     kesl-control --set-settings 15 Schedules.item_0001.ScheduleName=Default Schedules.item_0001.DaysHours=All
     ```

Как настроить шаблон сообщений Контроля устройств

При попытке пользователя обратиться к заблокированному устройству приложение выводит сообщение о запрете доступа к устройству или о запрете операции с устройством.

Для сообщений о запрете доступа предусмотрен шаблон, в котором описаны причины блокировки. Для текста шаблона сообщений предусмотрены специальные переменные (например, %USER_NAME%). Переменные позволяют использовать единый шаблон сообщений для разных устройств. При формировании сообщения приложение подставляет в сообщение значения переменных, соответствующие конкретному устройству, пользователю и событию.

Вы можете изменять содержание шаблона сообщений.

Как изменить шаблон сообщения в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль устройств**.
5. В блоке **Шаблоны сообщений** перейдите по ссылке **Сообщения о блокировке устройства**.

   Откроется окно настройки шаблона сообщения.
6. Настройте шаблон сообщения Контроля устройств на вкладке **Сообщение пользователю**.
7. Вы можете добавлять переменные и ссылки в текст сообщения для пользователя, используя кнопки **Добавить переменную** и **Добавить ссылку**. Для добавления переменной в текст шаблона установите курсор в нужное место в тексте, нажмите на кнопку **Добавить переменную** и выберите нужную переменную в раскрывающемся списке. Для добавления ссылки в текст шаблона установите курсор в нужное место в тексте и нажмите на кнопку **Добавить ссылку**.

   Если необходимо восстановить текст шаблона сообщения, нажмите на кнопку **Восстановить по умолчанию**.
8. Нажмите на кнопку **OK**.
9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Как изменить шаблон сообщения в Консоли администрирования

1. В дереве Консоли администрирования в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.
2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

   Вы также можете открыть окно свойств политики с помощью пункта **Свойства** контекстного меню политики или по ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.
4. В окне политики выберите **Контроль безопасности** → **Контроль устройств**.
5. В блоке **Шаблоны сообщений** нажмите на кнопку **Настроить**.
6. В открывшемся окне **Шаблоны сообщений** настройте шаблон сообщения Контроля устройства на вкладке **Сообщение о блокировке**.

Вы можете добавлять переменные и ссылки в текст сообщения для пользователя, используя кнопки **Переменная** и **Ссылка**. Для добавления переменной в текст шаблона установите курсор в нужное место в тексте, нажмите на кнопку **Переменная** и выберите нужную переменную в раскрывающемся списке. Для добавления ссылки в текст шаблона установите курсор в нужное место в тексте и нажмите на кнопку **Ссылка**.

Также вы можете восстановить текст шаблона сообщения, нажав на кнопку **По умолчанию**.

7. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **Применить**.

Предоставление временного доступа к устройству

При настройке Контроля устройств администратор может случайно запретить доступ к устройству, необходимому пользователю для работы. Если блокировка доступа к устройству или запрет операции с содержимым устройства, по мнению пользователя, произошли ошибочно, пользователь может запросить временный доступ к заблокированному устройству у администратора локальной сети организации.

Запрос временного доступа возможен, если администратор разрешил пользователю запрашивать временный доступ. Администратор может настроить это разрешение в свойствах политики в Web Console или в Консоли администрирования или в параметрах задачи Контроль устройств.

Предоставление доступа к заблокированному устройству состоит из следующих этапов:

1. Пользователь создает *файл запроса* и передает его администратору, например, по электронной почте или любым доступным способом (администратор может прописать это в шаблоне сообщения о блокировке). Пользователь может запрашивать временный доступ к заблокированному устройству в графическом интерфейсе или командной строке приложения.

2. Администратор создает из файла запроса *ключ доступа* и передает его пользователю, например, по электронной почте или любым доступным способом. Предоставление доступа к заблокированному устройству выполняется в Web Console.

3. Пользователь загружает ключ доступа и получает временный доступ к заблокированному устройству. Пользователь может загружать ключ доступа в графическом интерфейсе или командной строке приложения.

Предоставление доступа к заблокированному устройству доступно, только если в организации развернуто приложение Kaspersky Security Center 16.1 и клиентское устройство имеет возможность установить связь с Сервером администрирования.

Как создать ключ доступа к заблокированному устройству в Web Console

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство, и установите флажок рядом с его именем.

3. Над списком управляемых устройств нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**. Если кнопка не отображается над списком устройств, нажмите на кнопку с многоточием и выберите в меню пункт **Предоставить доступ к устройству в автономном режиме**.

4. В открывшемся окне **Параметры приложения** в разделе **Контроль устройств** нажмите на кнопку **Обзор** и загрузите полученный от пользователя файл запроса.

   Отобразится информация о заблокированном устройстве, к которому пользователь запросил доступ.

5. Если требуется, измените значение в часах в поле **Длительность доступа**.

   По умолчанию в поле **Длительность доступа** выбрано значение, указанное пользователем при формировании файла запроса доступа.

6. Если требуется, измените значение в поле **Укажите срок, в течение которого можно использовать ключ доступа на клиентском устройстве**.

   Поле содержит период времени, в течение которого пользователь может загрузить ключа доступа.

7. Нажмите на кнопку **Создать ключ**.

8. Сохраните файл с ключом доступа с расширением *.acode.

Как запросить и получить временный доступ в командной строке

Если блокировка доступа к устройству или запрет операции с содержимым устройства, по мнению пользователя, произошли ошибочно, пользователь может запросить временный доступ к заблокированному устройству у администратора локальной сети организации с помощью команды управления Контролем устройств:

Запросить временный доступ к заблокированному устройству

```
kesl-control --request-temporary-device-access --device-id <device identifier>  --access-duration <access duration> --path <path to the access request file>
```

где:

`--device-id <device identifier>` – идентификатор заблокированного устройства, к которому вы хотите получить доступ.

`--access-duration <access duration>` – период времени, на который вы хотите получить доступ к устройству (в часах). Возможные значения: 1–100.

`--path <path to the access request file>` – путь к директории, в которой вы хотите сохранить файл запроса доступа с расширением .akey.

В результате выполнения команды будет создан файл запроса доступа, который нужно передать администратору, например, по электронной почте или любым доступным способом (администратор может прописать это в шаблоне сообщения о блокировке).

После получения ключа доступа от администратора требуется загрузить ключ доступа, чтобы получить временный доступ к устройству.

Загрузить ключ доступа к заблокированному устройству

```
kesl-control --upload-temporary-device-access-key --path <path to the file with the access key>
```

где:

`--path <path to the file with the access key>` – путь к файлу с ключом доступа к устройству (файлу с расширением .acode).

В результате выполнения команды отобразится информация о предоставлении доступа к устройству и о периоде времени, на который предоставлен доступ к этому устройству.

Как запросить и получить временный доступ в графическом интерфейсе

При подключении устройства, доступ к которому запрещен Контролем устройств, открывается окно с сообщением о блокировке доступа к устройству.

Вы можете запросить временный доступ к заблокированному устройству у администратора локальной сети организации с помощью графического интерфейса следующими способами:

- из окна с сообщением о блокировке доступа к устройству, нажав на кнопку **OK**.
- из главного окна графического интерфейса приложения.

Чтобы запросить временный доступ к заблокированному устройству:

1. Откройте главное окно графического интерфейса приложения.
2. В нижней части главного окна нажмите на кнопку **Временный доступ**.

   Откроется окно **Временный доступ**.

   Вы также можете открыть окно **Временный доступ** из окна с сообщением о блокировке доступа к устройству по кнопке **OK**.
3. В разделе **Запрос доступа к заблокированному устройству** в списке подключенных устройств выберите устройство, к которому вы хотите получить доступ.
4. В поле **Длительность доступа к устройству в часах** укажите период времени, на который вы хотите получить доступ к устройству (в часах).
5. Нажмите на кнопку **Сформировать файл запроса**.
6. В открывшемся окне укажите путь к директории, в которой вы хотите сохранить файл запроса доступа с расширением .akey.
7. Передайте файл запроса доступа администратору, например, по электронной почте или любым доступным способом (администратор может прописать это в шаблоне сообщения о блокировке).

После получения ключа доступа от администратора вы можете загрузить ключ доступа, чтобы получить временный доступ к заблокированному устройству.

Чтобы получить временный доступ к заблокированному устройству:

1. Откройте главное окно графического интерфейса приложения.
2. В нижней части главного окна нажмите на кнопку **Временный доступ**.

   Откроется окно **Временный доступ**.
3. В разделе **Получение доступа к устройству** нажмите на кнопку **Загрузить ключ доступа**.
4. В открывшемся окне выберите файл с ключом доступа к устройству (файл с расширением .acode), полученный от администратора локальной сети организации.

5. Откроется окно с информацией об устройстве, к которому предоставлен доступ, и о периоде времени, на который предоставлен доступ к этому устройству.

6. Нажмите на кнопку **OK**.

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

Веб-Контроль позволяет ограничить доступ к веб-ресурсам по категории содержания, по типам данных, а также запрещать доступ к отдельным веб-сайтам. Вы можете ограничить доступ пользователей, например, к категории содержания "Социальные сети" или другим категориям. Тип данных приложение определяет по формату файла, а не по расширению.

Как работает Веб-Контроль

1. **Приложение проверяет обращения к веб-ресурсам**

   Веб-Контроль определяет категорию содержимого и тип данных веб-сайта с помощью следующих технологий:

   - Антивирусные базы
   - Облачные службы Kaspersky Security Network
   - Эвристический анализ – технология позволяет выявлять угрозы, которые еще не внесены в базы данных "Лаборатории Касперского".

2. **Приложение применяет правила**

   Приложение применяет правила Веб-Контроля в порядке их приоритета. Чем меньше числовое значение приоритета, тем выше приоритет правила. Если к веб-сайту относится несколько правил, Веб-Контроль применяет правило с высшим приоритетом.

   Например, приложение 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.

3. **Завершение проверки**

   Если правило запрещает обращение к веб-ресурсу, приложение отобразит в браузере сообщение о блокировке веб-сайта. Ресурс будет недоступен.

   Пользователь может отправить запрос администратору организации об ошибочной блокировке, если веб-страница, по мнению пользователя, заблокирована ошибочно.

Настройка Веб-Контроля

1. **Настройте правила Веб-Контроля**

   Веб-Контроль управляет доступом пользователей к веб-сайтам с помощью *правил доступа*. Эти правила позволяют ограничить доступ к веб-сайтам для отдельных пользователей, а также настроить расписание доступа.

   Например, вы можете ограничить доступ к веб-сайтом с категорией *Общение в сети* в рабочее время для всех пользователей организации, кроме IT-отдела.

2. **Настройте шаблоны сообщений**

   В зависимости от действия правила доступа, Веб-Контроль выводит сообщение пользователю о посещении нежелательного веб-сайта или о блокировке веб-сайта. При блокировке веб-сайта пользователь может отправить сообщение администратору локальной сети об ошибочной блокировке.

   Для таких сообщений предусмотрены шаблоны.

   > Изменить шаблоны в командной строке невозможно.

3. **Включите Веб-Контроль**

   По умолчанию Веб-Контроль выключен. Включите компонент в Web Console или в Консоли администрирования с помощью переключателя или в командной строке с помощью следующей команды:

   ```
   kesl-control --start-task 26
   ```

Особенности и ограничения

- Приложение не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, приложение определит тип данных "Архивы", а не "Графические файлы".
- Kaspersky Endpoint Security контролирует только HTTP- и HTTPS-трафик.
- При одновременной работе Защиты от веб-угроз и Веб-Контроля к веб-ресурсу сначала применяются параметры Защиты от веб-угроз. Таким образом, вредоносный или фишинговый веб-сайт будет заблокирован, даже если правила Веб-Контроля разрешают доступ к нему.

Как создать правило доступа к веб-ресурсам

Правило доступа к веб-ресурсам – набор фильтров и действий, которое Kaspersky Endpoint Security выполняет при посещении пользователями веб-ресурсов. Правила доступа могут включать в себя расписание работы правила.

Правила ограничивают доступ к веб-ресурсам по следующим фильтрам:

- **Категории содержания**. Веб-Контроль разделяет веб-ресурсы по категориям содержания и типам данных. Это позволяет ограничить доступ пользователей к веб-сайтам с определенной категорией содержания (например, *Платежные системы*) и / или с определенным типом данных (например, *Исполняемые файлы*).

- **Отдельные веб-сайты**. Веб-Контроль позволяет ограничить доступ пользователей к отдельным адресам или группам адресов веб-ресурсов.

  Домены веб-адресов не чувствительны к регистру. Если в правиле указан веб-адрес `examPLE.com`, Веб-Контроль ограничит доступ к адресу `example.com`.

  Если в правиле доступа одновременно заданы фильтр по категории содержания и фильтр по отдельным веб-сайтам, Веб-Контроль ограничивает доступ не ко всем веб-ресурсам указанной категории содержания, а только к указанным веб-адресам.

- **Фильтр по именам пользователей и групп пользователей**. Веб-Контроль позволяет ограничить доступ к веб-ресурсам для отдельных пользователей или групп пользователей. Например, вы можете ограничить доступ к веб-сайтам социальных сетей для всех пользователей организации, кроме IT-отдела.

- **Расписание работы правила**. Расписание работы правила определяет время, когда приложение контролирует доступ к веб-ресурсам, указанным в правиле. Например, вы можете ограничить доступ к нежелательным веб-сайтам только в рабочее время.

Если не создано ни одного запрещающего правила, расшифровка HTTPS-трафика не выполняется.

Как создать правило доступа в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности** → **Веб-Контроль**.

5. Убедитесь, что переключатель работы компонента находится в положении **Веб-Контроль ВКЛЮЧЕН**.

6. В блоке **Список правил** выберите действие Веб-Контроля по умолчанию:

   - **Разрешать все, не указанное в списке правил**

   - **Блокировать все, не указанное в списке правил**

7. Нажмите на кнопку **Добавить**.

   Откроется форма добавления правила доступа.

8. В поле **Имя правила** введите имя правила. Имя правила должно быть уникальным.

9. В поле **Приоритет** задайте приоритет правила доступа.

10. Выберите действие Веб-Контроля над веб-ресурсами при срабатывании правила:

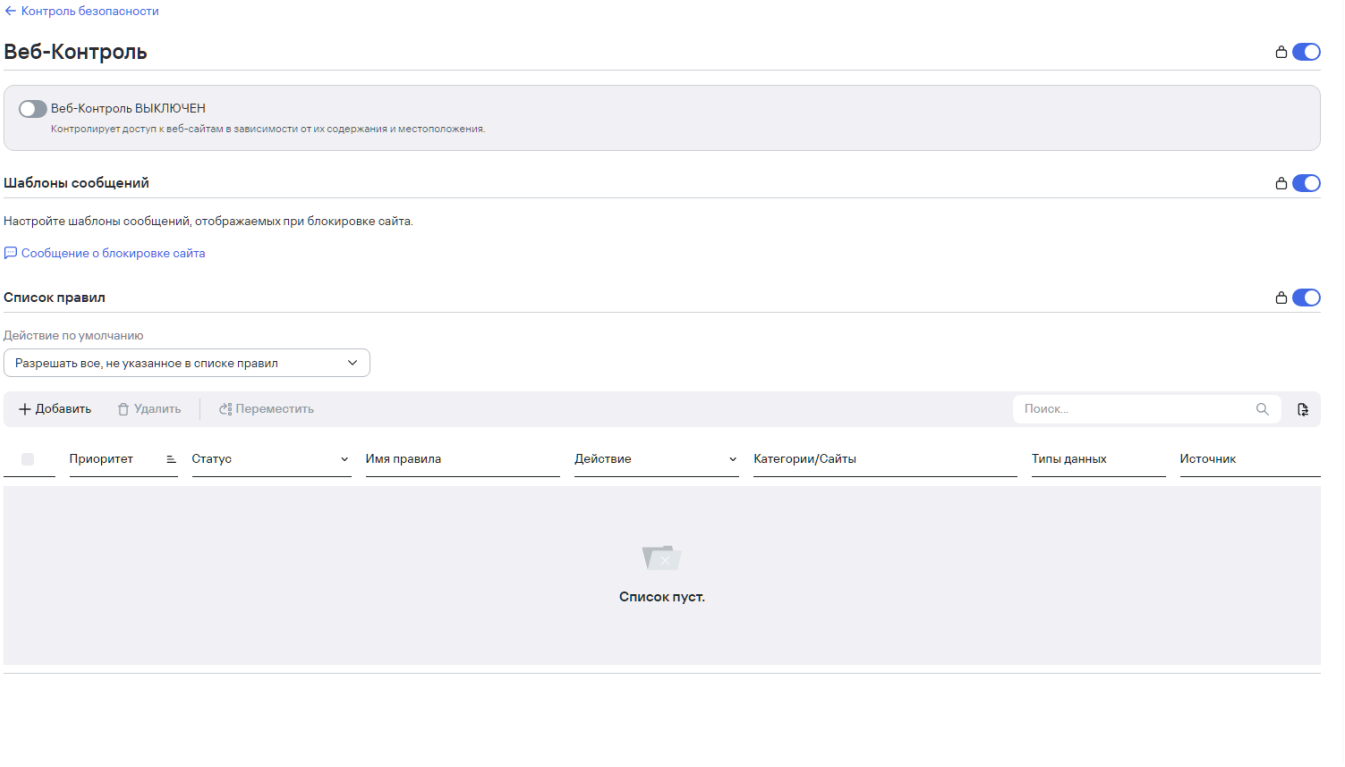
- **Разрешать**. Веб-Контроль разрешает доступ пользователя к веб-ресурсу.
- **Блокировать**. Веб-Контроль запрещает доступ пользователя к веб-ресурсу и выводит сообщение о запрете доступа. По ссылкам из сообщения о блокировке пользователь может отправить сообщение администратору локальной сети об ошибочной блокировке.
- **Информировать**. Веб-Контроль выводит предупреждение о посещении нерекомендованного веб-ресурса. Если, по мнению пользователя, предупреждение ошибочно, по ссылке из сообщения пользователь может перейти к веб-странице или отправить запрос администратору локальной сети организации.

11. Выберите фильтр правила доступа:

- **Категории содержания**. Укажите категории содержания, которые будет контролировать правило доступа. Вы можете выбрать несколько категорий.
- **Отдельные веб-сайты**. Укажите адрес веб-сайта или группу веб-сайтов.

> Задать одновременно фильтр по категории содержания и фильтр по отдельным веб-сайтам в Web Console невозможно.

12. Если необходимо, укажите типы данных, которые будут фильтроваться приложением.
13. Выберите пользователей или группу пользователей, для которых будет применяться правило доступа. По умолчанию правило применяется ко всем пользователям.
14. Если необходимо, задайте расписание доступа. По умолчанию правило применяется всегда.
15. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.



Веб-Контроль

Как создать правило доступа в командной строке

1. Убедитесь, что компонент Веб-Контроль включен:

```
kesl-control --get-settings 26
```

   Компонент должен иметь статус **Запущена**.

2. Если компонент выключен, выполните команду:

```
kesl-control --start-task 26
```

3. Выберите действие Веб-Контроля по умолчанию:

```
kesl-control --set-settings 26 WebControlDefaultAction=<Allow|Block>
```

4. Добавьте новое правило доступа с идентификатором `#`:

   a. Включите правило:

```
kesl-control --set-settings 26 Rules.item_#.Enabled=Yes
```

   b. Задайте имя правила:

```
kesl-control --set-settings 26 Rules.item_#.Name=<rule name>
```

   c. Задайте действие Веб-Контроля над веб-ресурсами при срабатывании правила:

```
kesl-control --set-settings 26 Rules.item_#.WebControlAction=<Allow|Block|Notify>
```

   d. Если необходимо фильтровать веб-ресурсы по категории содержания:

```
kesl-control --set-settings 26 Rules.item_#.UseCategories=<ContentOnly|FormatOnly|ContentAndFormat>
kesl-control --set-settings 26 Rules.item_#.ContentCategories.item_#.ContentCategory=<category>
[Rules.item_#.FormatCategories.item_#.FormatCategory=<format>]
```

   e. Если необходимо фильтровать отдельные веб-ресурсы:

```
kesl-control --set-settings 26 Rules.item_#.UseUrls=Yes
kesl-control --set-settings 26 Rules.item_#.Urls.item_#=<web address>
```

   f. Если необходимо, укажите пользователей, для которых будет применяться правило:

```
kesl-control --set-settings 26 Rules.item_#.UsePrincipals=Yes
kesl-control --set-settings 26 Rules.item_#.Principals.item_#.Name=<user name|@group name>
```

g. Если необходимо, задайте расписание правила:

```
kesl-control --set-settings 26 Rules.item_#.Schedules.item_#.Id=<ID> Rules.item_#.Schedules.item_#.Name=
<schedule name> Rules.item_#.Schedules.item_#.DaysHours=<day of the week|hour>
```

5. Для просмотра списка правил Веб-Контроля выполните команду:

```
kesl-control --get-settings 26
```

Условные обозначения

Параметры команды

Параметр	Описание
`WebControlDefaultAction`	Действие, которое Веб-Контроль применяет к веб-ресурсам, не указанным в правилах доступа.
`Enabled=Yes`	Включение правила доступа с идентификатором `#`.
`Name`	Имя правила. Имя правила должно быть уникальным.
`WebControlAction`	Действие Веб-Контроля над веб-ресурсами при срабатывании правила: `Allow` (значение по умолчанию) – разрешать доступ к веб-ресурсу. `Block` – запрещать доступ к веб-ресурсу. `Notify` – выводить предупреждение о посещении нерекомендованного веб-ресурса. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
`UseCategories`	Использование в правиле фильтров по категориям содержания и по категориям типов данных: `None` (значение по умолчанию) – не использовать фильтр содержимого веб-ресурсов. `ContentOnly` – использовать в правиле фильтр по категориям содержания. `FormatOnly` – использовать в правиле фильтр категориям типов данных. `ContentAndFormat` – использовать в правиле фильтр по категориям содержания и категориям типов данных.
`ContentCategories.item_#.ContentCategory`	Категория содержания.
`FormatCategories.item_#.FormatCategory`	Категория типов данных: `Video` – Видеофайлы `Audio` – Звуковые файлы `OfficeDocument` – Файлы офисных приложений `Executable` – Исполняемые файлы `Archives` – Архивы `Images` – Графические файлы `Scripts` – Скрипты
`UseUrls=Yes`	Использование в правиле фильтра отдельных веб-сайтов.
`Urls.item_#`	Адрес веб-ресурса, доступ к которому регулирует правило. Для указания адреса веб-ресурса вы можете использовать маски.
`UsePrincipals=Yes`	Использование фильтра пользователей, на которых распространяется правило доступа к веб-ресурсам.
`Principals.item_#.Name`	Пользователь или группа пользователей, на которых распространяется правило доступа к веб-ресурсам: `<user name>` – имя пользователя, для которого применяется правило. `@<group name>` – название группы пользователей, для которых применяется правило.
`Schedules.item_#.Id`	Идентификатор расписания.
`Schedules.item_#.Name`	Название расписания.

Параметр	Описание
`Schedules.item_#.DaysHours`	Интервалы времени для расписания: `<day of week>` – день недели. Вы можете использовать как полные названия дней недели, так и аббревиатуры (например, для понедельника можно указать `Mo`, `Mon` или `Monday`). Для дней недели можно указывать либо интервалы, либо конкретные дни. Неделя начинается с воскресенья. `<hour>` – часы [0:24]. Для часов вы можете указывать только интервалы.

Как изменить шаблоны сообщений Веб-Контроля

В зависимости от действия правила доступа, при попытке получить доступ к веб-ресурсам Веб-Контроль выводит сообщение пользователю (подменяет ответ HTTP-сервера HTML-страницей с сообщением):

- **Сообщение-предупреждение**. Сообщение, которое отображается пользователю при попытке открыть нерекомендованный ресурс. Приложение выводит такое сообщение, если выбрано действие правила **Информировать**.

  Если, по мнению пользователя, предупреждение ошибочно, по ссылке из сообщения пользователь может перейти к веб-странице или отправить запрос администратору локальной сети организации.

- **Сообщение о блокировке веб-ресурса**. Сообщение, которое отображается пользователю при блокировке нежелательного веб-ресурса. Приложение выводит такое сообщение, если выбрано действие правила **Блокировать**.

  Если, по мнению пользователя, веб-ресурс заблокирован ошибочно, по ссылке из сообщения о блокировке веб-ресурса пользователь может отправить запрос администратору локальной сети организации.

Для сообщения-предупреждения, сообщения о блокировке веб-ресурса и запроса к администратору локальной сети организации предусмотрены шаблоны. Для работы с шаблонами сообщений предусмотрены специальные переменные (например, `%USER_NAME%`). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров. При формировании сообщения Kaspersky Endpoint Security определяет значение переменной из настроек операционной системы и подставляет это значение в сообщение, соответствующие конкретному компьютеру, пользователю и событию.

Изменить шаблоны в командной строке невозможно.

Как изменить шаблон сообщения в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Веб-Контроль**.
5. В блоке **Шаблоны сообщений** перейдите по ссылке **Сообщение о блокировке сайта**.

   Откроется окно с шаблонами сообщений.

6. Настройте шаблоны сообщений Веб-Контроля:

   - **Предупреждение**. Шаблон предупреждения, которое отображается пользователю при попытке открыть нерекомендованный ресурс.

   - **Сообщение о блокировке**. Шаблон сообщения, появляющегося при блокировке веб-страницы или сайта, не рекомендованного для посещения.

   - **Сообщение администратору**. Шаблон сообщения администратору. Используется в случае, если веб-страница, по мнению пользователя, заблокирована ошибочно. После того, как пользователь запрашивает доступ, приложение отправляет в Kaspersky Security Center событие *Сообщение администратору о запрете доступа к веб-странице*. Описание события содержит сообщение администратору с подставленными переменными. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

   Если необходимо восстановить текст шаблона сообщения, нажмите на кнопку **Восстановить текст шаблона по умолчанию**.

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

Как изменить шаблон сообщения в Консоли администрирования

1. В дереве Консоли администрирования в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.

2. В рабочей области выберите вкладку **Политики**.

3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>**.

   Вы также можете открыть окно свойств политики с помощью пункта **Свойства** контекстного меню политики или по ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

4. В окне политики выберите **Контроль безопасности** → **Веб-Контроль**.

5. В блоке **Шаблоны сообщений** нажмите на кнопку **Настроить**.

6. В открывшемся окне **Шаблоны сообщений** настройте шаблоны сообщений Веб-Контроля на следующих вкладках:

   - **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.

   - **Жалоба администратору**. Поле ввода содержит шаблон сообщения-жалобы для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно. После запроса пользователя предоставить доступ приложение Kaspersky Endpoint Security отправляет в Kaspersky Security Center событие *Сообщение администратору о запрете доступа к веб-странице*. Описание события содержит сообщение администратору с подставленными переменными. Вы можете посмотреть эти события в Консоли администрирования Kaspersky Security Center с помощью предустановленной выборки **Запросы пользователей**. Если в вашей организации не развернуто решение Kaspersky Security Center или связь с Сервером администрирования отсутствует, приложение отправит сообщение администратору на указанный адрес электронной почты.

На вкладках **Предупреждение** и **Сообщение о блокировке** вы можете добавлять переменные и ссылки в тексты сообщений для пользователя, используя кнопки **Переменная** и **Ссылка**.

Вы можете восстановить текст шаблона сообщения, нажав на кнопку **По умолчанию**.

7. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **Применить**.

Правила формирования масок адресов веб-ресурсов

Использование *маски адреса веб-ресурса* (далее также "маски адреса") может быть удобно в случаях, когда в процессе создания правила доступа к веб-ресурсам требуется ввести множество схожих адресов веб-ресурсов. Одна грамотно сформированная маска адреса может заменить множество адресов веб-ресурсов.

При формировании маски адреса следует использовать следующие правила:

1. Символ `*` заменяет любую последовательность из нуля или более символов.

   Например, при вводе маски адреса `*abc*` правило доступа к веб-ресурсам применяется ко всем адресам, содержащим последовательность `abc`. Пример: `http://www.example.com/page_0-9abcdef.html`.

2. Последовательность символов `*.` позволяет выбрать все домены адреса – *маска домена*. Маска домена `*.` трактуется как любое имя домена, имя поддомена или пустая строка.

   Пример: под действие маски `*.example.com` попадают следующие адреса:

   - `http://pictures.example.com` – маска домена `*.` применена для `pictures.`.
   - `http://user.pictures.example.com` – маска домена `*.` применена для `pictures.` и `user.`.
   - `http://example.com` – маска домена `*.` трактуется как пустая строка.

3. Последовательность символов `www.` в начале маски адреса трактуется как последовательность `*.`.

   Пример: маска адреса `www.example.com` трактуется как `*.example.com`. Под действие маски попадают адреса `www2.example.com` и `www.pictures.example.com`.

4. Если маска адреса начинается не с символа `*`, то содержание маски адреса эквивалентно тому же содержанию с префиксом `*.`.

5. Если маска адреса заканчивается символом, отличным от `/` или `*`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

   Пример: под действие маски адреса `http://www.example.com` попадают адреса вида `http://www.example.com/abc`, где `a`, `b`, `c` – любые символы.

6. Если маска адреса заканчивается символом `/`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

7. Последовательность символов `/*` в конце маски адреса трактуется как `/*` или пустая строка.

8. Проверка адресов веб-ресурсов по маске адреса осуществляется с учетом схемы (http или https):

   - Если сетевой протокол в маске адреса отсутствует, то под действие маски адреса попадает адрес с любым сетевым протоколом.

     Пример: под действие маски адреса `example.com` попадают адреса `http://example.com` и `https://example.com`.

   - Если сетевой протокол в маске адреса присутствует, то под действие маски адреса попадают только адреса с таким же сетевым протоколом, как у маски адреса.

     Пример: под действие маски адреса `http://*.example.com` попадает адрес `http://www.example.com` и не попадает адрес `https://www.example.com`.

9. Маска адреса, заключенная в двойные кавычки, трактуется без учета каких-либо дополнительных подстановок, за исключением символа `*`, если он изначально включен в состав маски адреса. Для масок адреса, заключенных в двойные кавычки, не выполняются правила 5 и 7 (см. примеры 14 – 18 в таблице ниже).

10. При сравнении с маской адреса веб-ресурса не учитываются имя пользователя и пароль, порт соединения и регистр символов.

Примеры применения правил формирования масок адресов

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
1	*.example.com	http://www.123example.com	Нет	См. правило 1.
2	*.example.com	http://www.123.example.com	Да	См. правило 2.
3	*example.com	http://www.123example.com	Да	См. правило 1.
4	*example.com	http://www.123.example.com	Да	См. правило 1.
5	http://www.*.example.com	http://www.123example.com	Нет	См. правило 1.
6	www.example.com	http://www.example.com	Да	См. правила 3, 2, 1.
7	www.example.com	https://www.example.com	Да	См. правила 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Да	См. правила 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Да	См. правила 3, 5, 1.
10	example.com	http://www.example.com	Да	См. правила 3, 1.
11	http://example.com/	http://example.com/abc	Да	См. правила 6.
12	http://example.com/*	http://example.com	Да	См. правило 7.
13	http://example.com	https://example.com	Нет	См. правило 8.
14	"example.com"	http://www.example.com	Нет	См. правило 9.
15	"http://www.example.com"	http://www.example.com/abc	Нет	См. правило 9.
16	"*.example.com"	http://www.example.com	Да	См. правила 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Да	См. правила 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Да	См. правила 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Нет	Маска адреса содержит больше информации, чем адрес веб-ресурса.

Контроль приложений

Контроль приложений управляет запуском сторонних приложений на устройствах пользователей. Это позволяет снизить риск заражения защищенного устройства вредоносным ПО.

Для использования компонента требуется лицензия, которая включает эту функцию.

Как работает Контроль приложений

1. **Пользователь пытается запустить стороннее приложение**

2. **Контроль приложений применяет правила**

   Контроль приложений последовательно применяет правила к запускаемому приложению. В зависимости от выбранного режима правил компонент *контролирует* запуск приложений или *тестирует* правила. При этом приоритет запрещающего правила выше приоритета разрешающего правила.

3. **Завершение проверки**

   Если правила запрещают запуск стороннего приложения, компонент блокирует запуск этого приложения и формирует событие *Запуск приложения запрещен*. В тестовом режиме компонент не блокирует запуск этого приложения и формирует событие *Запуск приложения запрещен в тестовом режиме*.

Настройка Контроля приложений

1. **Проведите инвентаризацию приложений**

   С помощью задачи Инвентаризация получите список приложений, установленных на защищаемых устройствах. На основе полученной информации сформируйте список приложений, запуск которых вы хотите запретить.

2. **Выберите режим работы Контроля приложений**

   Компонент Контроль приложений может работать в одном из двух режимов:

   - *Разрешать все, не указанное в списке правил*. Контроль приложений разрешает пользователям запуск любых сторонних приложений, кроме тех, которые запрещены правилами.

   - *Блокировать все, не указанное в списке правил*. Контроль приложений запрещает пользователям запуск любых сторонних приложений, кроме тех, которые разрешены и не запрещены правилами.

   Выбор режима Контроля приложений зависит от политики безопасности вашей организации, а также количества приложений, запуск которых нужно контролировать.

3. **Создайте категории приложений**

Определите категории запрещенных или разрешенных приложений. Категории приложений предназначены для всех устройств организации независимо от групп администрирования. Категории приложений позволяют настраивать правила для группы приложений, а не на основе включающих и исключающих условий.

Рекомендуем создать категорию "приложения для работы", которая включает в себя стандартный набор приложений, используемых в организации. Если различные группы пользователей используют различные наборы приложений для работы, вы можете создать отдельную категорию приложений для работы каждой группы пользователей.

> Рекомендуем настраивать категории приложений в Kaspersky Security Center.

4. **Настройте правила контроля приложений**

   Компонент контролирует запуск приложений на основе *правил контроля приложений* – условий, при выполнении которых Контроль приложений разрешает или запрещает запуск стороннего приложения выбранной группе пользователей.

5. **Протестируйте правила контроля приложений**

   По умолчанию Контроль приложений выключен. Рекомендуем включить Контроль приложений в тестовом режиме и проверить работу созданных правил контроля приложений. Приложение не будет блокировать запуск сторонних приложений, но будет отправлять уведомления об их запуске на Сервер администрирования.

6. **Изучите работу правил контроля приложений**

   Ознакомьтесь с отчетом о работе Контроля приложений в тестовом режиме. После анализа полученной информации скорректируйте правила контроля приложений.

7. **Включите использование правил контроля приложений**

   В этом режиме Kaspersky Endpoint Security запрещает запуск сторонних приложений, если их запуск не разрешен правилами.

   Как включить использование правил контроля приложений в Web Console

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

      Откроется окно свойств политики.
   3. Выберите вкладку **Параметры приложения**.
   4. Перейдите в раздел **Контроль безопасности** → **Контроль приложений**.
   5. Убедитесь, что переключатель работы компонента находится в положении **Контроль приложений ВКЛЮЧЕН**.
   6. В блоке **Действие при запуске приложений** выберите действие Контроля приложений **Применять правила**.
   7. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

   Как включить использование правил контроля приложений в командной строке

Для включения тестового режима работы Контроля приложений выполните команду:

```
kesl-control --set-settings 21 AppControlRulesAction=ApplyRules
```

Администратор Kaspersky Security Center или локальный пользователь с назначенной в приложении ролью admin может запрещать или разрешать запуск процессов под учетной записью root, используя Контроль приложений.

Особенности и ограничения

- Контроль приложений не поддерживает управление запуском приложений Snap, Flatpak и AppImage.
- Контроль приложений не контролирует запуск скриптов из интерпретаторов, не поддерживаемых приложением Kaspersky Endpoint Security и запуск скриптов, передаваемых интерпретатору не через командную строку. Kaspersky Endpoint Security поддерживает следующие интерпретаторы: python, perl, bash, ssh.
- Если запуск интерпретатора разрешен правилами контроля, то Контроль приложений не блокирует скрипт, запущенный из этого интерпретатора. Если запуск хотя бы одного из скриптов, указанных в командной строке интерпретатора, запрещен правилами контроля, то Kaspersky Endpoint Security блокирует все скрипты, указанные в командной строке интерпретатора. Исключение: cat script.py | python.

Инвентаризация приложений

Для создания оптимальных правил контроля приложений рекомендуется получить представление о приложениях, используемых на защищаемых устройствах локальной сети организации. Задача *Инвентаризация* позволяет получить следующую информацию:

- название и версия стороннего приложения;
- краткое описание.

Для использования задачи требуется лицензия, которая включает эту функцию.

В базе данных приложения Kaspersky Security Center может храниться информация о 150 000 обработанных файлов. При достижении этого лимита новые файлы не будут обработаны. Для возобновления работы инвентаризации требуется удалить с защищаемого устройства файлы, добавленные в базу данных Kaspersky Security Center при предыдущей инвентаризации.

Настройка и запуск задачи Инвентаризация

1. **Создайте задачу Инвентаризация**

Как создать задачу Инвентаризация в Web Console

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Linux 12.5**.

   b. В раскрывающемся списке **Тип задачи** выберите **Инвентаризация**.

   c. В поле **Название задачи** введите название задачи.

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

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи.

5. Завершите работу мастера.

Как создать задачу Инвентаризация в командной строке

Для создания задачи выполните команду:

```
kesl-control --create-task <task name> --type InventoryScan
```

где `<task name>` – имя новой задачи.

В результате выполнения команды приложение отобразит ID созданной задачи.

Пример результата выполнения команды:

Задача создана (идентификатор задачи: 100)

2 **Настройте области инвентаризации**

Для запуска задачи должна быть указана хотя бы одна область инвентаризации. По умолчанию задана область *Executable commands (Исполняемые команды)* – `/usr/bin`.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в каком эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Как задать область инвентаризации в Web Console

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

   Откроется список задач.

2. Нажмите на созданную задачу инвентаризации.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Области инвентаризации**.

5. Нажмите на кнопку **Добавить**.

   Откроется окно добавления областей инвентаризации.

6. В поле **Название области** укажите имя области инвентаризации, например, *Файлы на рабочем столе*.

7. В поле **Путь** укажите путь к отдельному файлу или к директории, например, `/path/to/folder`. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

8. Если необходимо, укажите маски имен объектов в формате командной оболочки, например, `*.txt`, `file?.*`. Добавляйте маски по одной.

9. Сохраните внесенные изменения.

Как задать область инвентаризации в командной строке

1. Выполните команду:

```
kesl-control --set-settings <task name | task ID> ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. Для проверки текущих настроек задачи выполните следующую команду:

```
kesl-control --get-settings <task name | task ID>
```

Условные обозначения

Параметры задачи Инвентаризация

Параметр	Описание
`UseScanArea=Yes`	Включение области инвентаризации с идентификатором `#`. Вы можете временно отключить проверку области инвентаризации для приложения, а не удалять область. Для этого задайте значение `ScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Описание области инвентаризации. Максимальная длина строки, задаваемой этим параметром: 4096 символов.
`AreaMask.item_#`	Ограничение области инвентаризации. В области инвентаризации приложение проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `ScanScope.item_#.AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Например, `ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Путь к директории с проверяемыми объектами. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски. Значение по умолчанию: `/usr/bin`

3. **Если необходимо, измените настройки задачи**

Как настроить задачу Инвентаризация в Web Console

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

   Откроется список задач.

2. Нажмите на созданную задачу инвентаризации.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Настройки инвентаризации**.

5. Выберите действие с категорией приложений "Золотой образ":

   - **Оставить без изменений** – не изменять категорию приложений "Золотой образ" после выполнения инвентаризации. По умолчанию выбрано это значение. Этот вариант используется, когда вы хотите получить список сторонних приложений, используемых на устройстве, но не записывать их в категорию "Золотой образ".

   - **Обновить или создать (если не создана)** – добавлять приложения, обнаруженные на устройстве при инвентаризации, в категорию "Золотой образ". Если категория отсутствует, она будет создана. Если категория существует, список приложений в ней будет обновлен.

   - **Удалить** – очистить категорию приложений "Золотой образ" (Golden Image). Приложение очищает категорию сразу после запуска задачи без инвентаризации файлов на устройстве.

6. Если необходимо, установите флажки:

   - **Инвентаризация файлов скриптов**. Проверка на наличие скриптов в области инвентаризации. Приложение отправляет эту информацию в Kaspersky Security Center.

   - **Проверять все исполняемые файлы**.

   - **Проверять двоичные файлы**. Проверка двоичных файлов (с расширениями .elf, .java и .pyc).

7. Сохраните внесенные изменения.

Как настроить задачу Инвентаризация в командной строке

Выполните команду:

```
kesl-control --set-settings <task name | task ID> ScanScripts=<Yes|No> ScanBinaries=<Yes|No>
ScanAllExecutable=<Yes|No> GoldenImageAction=<DoNothing|Create|Remove>
```

Условные обозначения

Параметры задачи *Инвентаризация*

Параметр	Описание
`ScanScripts`	Проверка скриптов в области инвентаризации: `Yes` (значение по умолчанию) – проверять скрипты. `No` – не проверять скрипты.
`ScanBinaries`	Проверка двоичных файлов (с расширениями elf, java и pyc): `Yes` (значение по умолчанию) – проверять бинарные файлы. `No` – не проверять бинарные файлы.
`ScanAllExecutable`	Проверка исполняемых файлов: `Yes` (значение по умолчанию) – проверять файлы с исполняемым битом. `No` – не проверять файлы с исполняемым битом.

Параметр	Описание
`GoldenImageAction`	Действие, которое Kaspersky Endpoint Security выполняет с категорией приложений "Золотой образ" по завершении задачи Инвентаризация: `DoNothing` (значение по умолчанию) – не изменять категорию приложений "Золотой образ". `Create` – добавлять обнаруженные приложения в категорию приложений "Золотой образ". Если категория отсутствует, она будет создана. Если категория существует, список приложений в ней будет обновлен. `Remove` – очистить категорию приложений "Золотой образ" (Golden Image). Приложение очищает категорию сразу после запуска задачи без инвентаризации файлов на устройстве.

4 Настройте области исключения

Исключение имеет более высокий приоритет, чем область инвентаризации. Исключенный объект не проверяется, даже если находится в области инвентаризации. Если область инвентаризации задана на более низком уровне, чем директория, указанная в исключении, то приложение не отслеживает эту область инвентаризации во время выполнения задачи.

Как задать область исключения в Web Console

1. В главном окне Web Console выберите **Задачи**.
2. Откроется список задач.
3. Нажмите на созданную задачу инвентаризации.

   Откроется окно свойств задачи.
4. Выберите вкладку **Параметры приложения**.
5. Перейдите в раздел **Области исключения**.
6. Нажмите на кнопку **Добавить**.

   Откроется окно добавления областей исключения.
7. В поле **Название области** укажите имя области исключения, например, *Системные файлы*.
8. В поле **Путь** укажите путь к отдельному файлу или к директории (например, `/path/to/folder`). Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.
9. Укажите маски имен объектов в формате командной оболочки (например, `*.txt` или `file?.*`). Добавляйте маски по одной.
10. Сохраните внесенные изменения.

Как задать область исключения в командной строке

1. Выполните команду:

```
kesl-control --set-settings <task name | task ID>       ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. Для проверки текущих настроек задачи выполните следующую команду:

```
kesl-control --get-settings <task name | task ID>
```

Условные обозначения

Параметры задачи Инвентаризация

Параметр	Описание
`UseScanArea`	Исключение указанной области из инвентаризации. Вы можете временно отключить область исключения для приложения, а не удалять область. Для этого задайте значение `ExcludedFromScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Описание области исключения из инвентаризации.
`AreaMask.item_#`	Ограничение области исключения. В области исключения приложение не проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `ExcludedFromScanScope.item_#.AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Например, `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Путь к директории, которую необходимо исключить из инвентаризации. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

Пример исключения из инвентаризации директории `/tmp`:

```
kesl-control --set-settings 100 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

5 **Запустите задачу**

Как запустить задачу Инвентаризация в Web Console

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

   Откроется список задач.

2. Установите флажок напротив созданной задачи.

3. Нажмите на кнопку **Запустить**.

Как запустить задачу Инвентаризация в командной строке

Для запуска задачи выполните команду:

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `[-W]` – включение вывода текущих событий, связанных с этой задачей.
- `[--progress]` – включение отображения хода выполнения задачи.

Просмотр списка обнаруженных приложений

Чтобы просмотреть список приложений, обнаруженных на устройствах, в Web Console:

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

   Откроется список задач.

2. Нажмите на созданную задачу инвентаризации.

   Откроется окно свойств задачи.

3. Выберите вкладку **Результаты**.

```
Просмотреть список приложений, обнаруженных на устройстве

kesl-control --get-app-list [--json]
```

Kaspersky Endpoint Security отобразит следующую информацию об обнаруженных приложениях:

- Дата и время инвентаризации
- Количество приложений
- Список приложений, содержащий следующую информацию:
  - Путь к приложению
  - Хеш-сумма приложения
  - Тип приложения. Например: `Script`, `Executable`.
  - Категории, к которым принадлежит приложение (если они были созданы ранее). Вы можете просмотреть список созданных категорий приложений с помощью команды:

    ```
    kesl-control --get-categories
    ```

> При добавлении новой категории информация о ней в списке приложений не обновляется автоматически. Чтобы обновить список приложений, требуется запустить задачу Инвентаризация еще раз.

Как настроить режим работы Контроля приложений

Компонент Контроль приложений может работать в одном из двух режимов:

- *Разрешать все, не указанное в списке правил.* Контроль приложений разрешает пользователям запуск любых сторонних приложений, кроме тех, которые запрещены правилами.
- *Блокировать все, не указанное в списке правил.* Контроль приложений запрещает пользователям запуск любых сторонних приложений, кроме тех, которые разрешены и не запрещены правилами.

Выбор режима Контроля приложений зависит от политики безопасности вашей организации, а также количества приложений, запуск которых нужно контролировать.

Как настроить режим работы Контроля приложений в Web Console

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

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

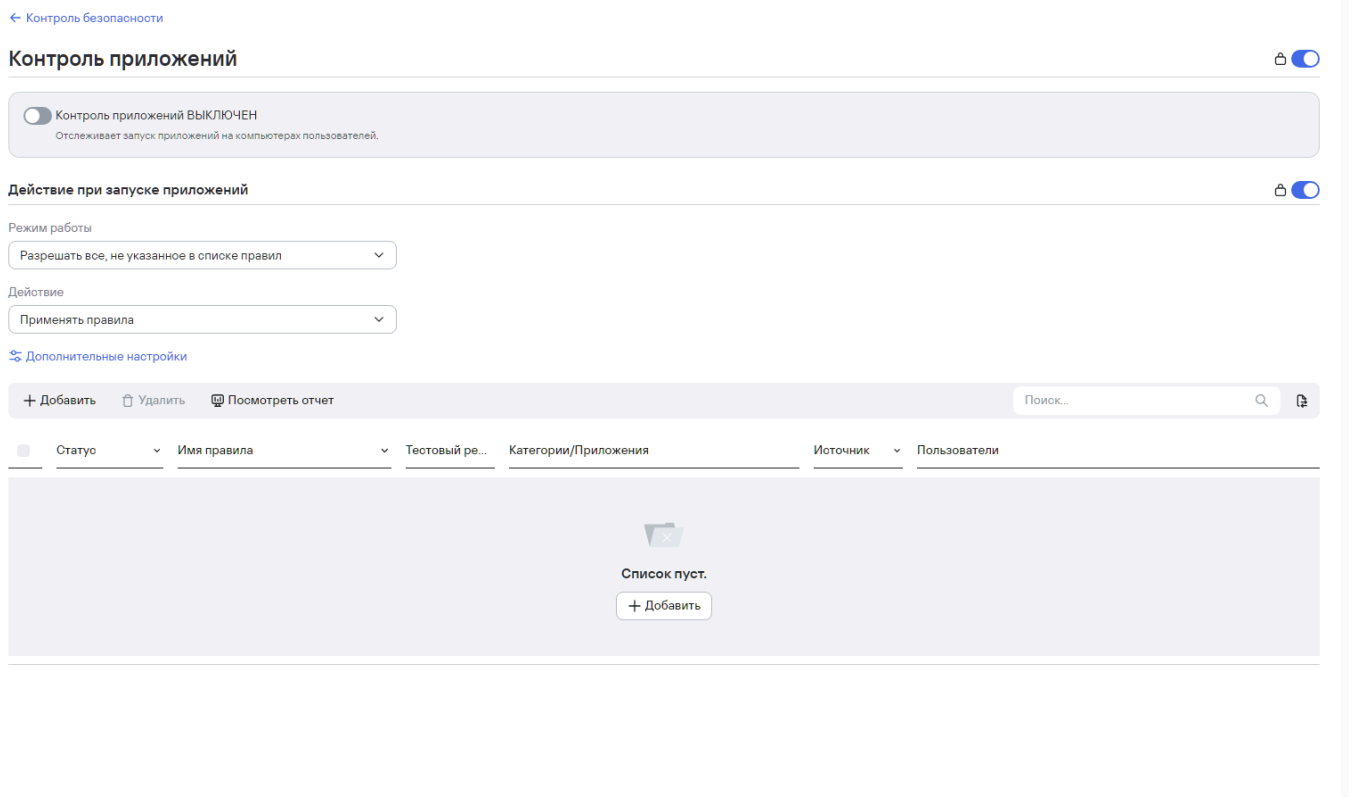
4. Перейдите в раздел **Контроль безопасности** → **Контроль приложений**.

5. Убедитесь, что переключатель работы компонента находится в положении **Контроль приложений ВКЛЮЧЕН**.

6. В блоке **Действие при запуске приложений** выберите режим работы Контроля приложений:

   - **Разрешать все, не указанное в списке правил**
   - **Блокировать все, не указанное в списке правил**

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



Контроль приложений

Как настроить режим работы Контроля приложений в командной строке

Выполните команду:

```
kesl-control --set-settings 21 AppControlMode=<AllowList|DenyList>
```

Условные обозначения

Параметры команды

Параметр	Описание
`AppControlMode`	`AllowList` – Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. `DenyList` (значение по умолчанию) – Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.

Создание категории приложений

Для удобства формирования правил Контроля приложений вы можете создать *категории приложений*.

Kaspersky Endpoint Security определяет категорию приложения с помощью следующих технологий:

- Антивирусные базы
- Облачные службы Kaspersky Security Network
- Эвристический анализ – технология позволяет выявлять угрозы, которые еще не внесены в базы данных "Лаборатории Касперского".

Для Kaspersky Endpoint Security для Linux категории могут быть созданы на основе следующих параметров:

- имя исполняемого файла приложения;
- имя директории с исполняемым файлом приложения;
- хеш исполняемого файла приложения. Допускается использование только SHA256.

  Для указания имен файлов и директорий вы можете использовать маски.

  Правила задания масок

  Вы можете использовать символ * (любая последовательность символов) или символ ? (один любой символ) для формирования маски имени файла или директории.

  Вы можете указать символ * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/*/file*/` или `/dir/file*/`.

  Вы можете указать символ ? вместо любого одного символа (включая символ `/`) в имени файла или директории.

Рекомендуется создать категорию "приложения для работы", которая включает в себя стандартный набор приложений, используемых в организации. Если различные группы пользователей используют различные наборы приложений для работы, вы можете создать отдельную категорию приложений для работы каждой группы пользователей.

> Kaspersky Endpoint Security для Linux не поддерживает KL-категории.

Чтобы создать категорию приложений в Kaspersky Security Center, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Сторонние приложения** → **Категории приложений**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания пользовательской категории.
3. Следуйте указаниям мастера создания пользовательской категории.

Шаг 1. Ввод названия и выбор типа категории

На этом шаге укажите название категории приложений и выберите один из следующих типов категорий приложений:

- *Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную*. Если вы выбрали этот тип категории, то на шаге *Условия* и шаге *Исключения* вы сможете задать критерии, по которым исполняемые файлы будут попадать в категорию.

- *Категория, в которую входят исполняемые файлы из указанной папки. Исполняемые файлы приложений, копируемых в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию*. Если вы выбрали этот тип категории, то следующем шаге вы сможете указать папку, исполняемые файлы из которой будут автоматически попадать в категорию.

- *Категория, в которую входят исполняемые файлы с выбранных устройств. Исполняемые файлы обрабатываются автоматически, их метрики заносятся в категорию*. Если вы выбрали этот тип категории, то на следующем шаге вы сможете указать компьютер, исполняемые файлы с которого будут автоматически попадать в категорию.

Шаг 2. Настройка условий для включения приложений в категорию

Этот шаг доступен, если вы выбрали тип категории **Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную**.

На этом шаге выберите критерии для включения приложений в категорию:

- **Из KL-категории**

  Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать категорию приложений "Лаборатории Касперского". *KL-категория* – сформированный специалистами "Лаборатории Касперского" список приложений, обладающих общими тематическими признаками. Например, KL-категория "Офисные приложения" включает в себя приложения из пакетов Microsoft Office, Adobe Acrobat и другие.

  Вы можете выбрать все KL-категории, чтобы сформировать расширенный список доверенных приложений.

- **Выберите сертификат из хранилища сертификатов**

  Если выбран этот вариант, можно указать сертификаты из хранилища. Условие категории соответствует только исполняемым файлам, которые подписаны указанным сертификатом.

  Если в качестве условия срабатывания правила вы выбрали сертификат, убедитесь, что этот сертификат добавлен в доверенное системное хранилище на компьютере, и проверьте параметры использования доверенного системного хранилища в приложении.

- **Задайте путь к приложению (поддерживаются маски)**

  Если выбран этот вариант, можно указать файл или папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию приложений. Вы можете использовать регулярные выражения, такие как `C:\path_to_exe\*`, например: `C:\Program Files\Internet Explorer\*`.

- **Съемный диск**

  Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск приложения. Приложения, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию приложений.

- **Хеши файлов папки, метаданные файлов папки или сертификаты из папки**:

  - **Выберите из списка исполняемых файлов**

    Если выбран этот вариант, приложения для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

  - **Выберите из реестра приложений**

    Если выбран этот параметр, отображается реестр приложений. После того как вы выберете приложение из реестра, откроется окно с параметрами, заполненными метаданными из выбранного вами приложения:

    - Имя файла.
    - Версия файла. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
    - Название приложения.
    - Версия приложения. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
    - Производитель.

    Обратите внимание, что блокируется только запуск исполняемых файлов, соответствующих указанным параметрам, но не запуск выбранного вами приложения. Если выбранные метаданные программы совпадают с метаданными исполняемого файла, который запускается при запуске программы, вы можете перейти к следующему шагу. Иначе вам нужно будет изменить значения вручную, чтобы они совпадали с метаданными исполняемого файла.

  - **Задайте вручную**

    Если выбран этот вариант, вам нужно указать хеш файла, метаданные или сертификат в качестве условия добавления приложений в пользовательскую категорию.

    Хеш файла

    В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Endpoint Security для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 и выше поддерживают вычисление хеш-функции SHA256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10.

Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Endpoint Security для файлов категории:

- Если все экземпляры приложений безопасности, установленных в вашей сети, являются версиями приложения Kaspersky Endpoint Security 10 и выше, установите флажок **SHA256**. Не рекомендуется добавлять категорию, созданную по критерию SHA256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10. Это может привести к сбою приложения безопасности. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.

- Если в вашей сети установлены более ранние версии, чем Kaspersky Endpoint Security 10, установите флажок **MD5-хеш**. Добавить категорию, созданную по критерию контрольной суммы MD5 исполняемого файла, для Kaspersky Endpoint Security 10 и выше, невозможно. В этом случае вы можете использовать криптографическую хеш-функцию SHA256 для файлов категории.

- Если разные устройства в вашей сети используют как более ранние, так и более поздние версии Kaspersky Endpoint Security 10, установите флажок **SHA256** и флажок **MD5-хеш**.

Метаданные

Если этот параметр выбран, вы можете указать метаданные файла такие как имя файла, версию файла и поставщика. Условие категории соответствует только исполняемым файлам с одинаковыми метаданными.

Сертификат

Если выбран этот вариант, можно указать сертификаты из хранилища. Условие категории соответствует только исполняемым файлам, которые подписаны указанным сертификатом.

- **Из файла MSI-пакета/архивной папки**

  Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать файл установщика MSI. Метаданные установщика приложения будут передаваться на Сервер администрирования. Приложения, у которых метаданные установщика совпадают с указанным установщиком MSI, будут добавлены в пользовательскую категорию приложений.

Шаг 3. Настройка условий для исключения приложений из категории

Этот шаг доступен, если вы выбрали тип категории **Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную**.

Приложения, указанные на этом шаге, исключаются из категории, даже если эти приложения были указаны на шаге "Настройка условий для включения приложений в категорию".

На этом шаге выберите критерии для исключения приложений из категории:

- **Из KL-категории**

  Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать категорию приложений "Лаборатории Касперского". *KL-категория* – сформированный специалистами "Лаборатории Касперского" список приложений, обладающих общими тематическими признаками. Например, KL-категория "Офисные приложения" включает в себя приложения из пакетов Microsoft Office, Adobe Acrobat и другие.

  Вы можете выбрать все KL-категории, чтобы сформировать расширенный список доверенных приложений.

- **Выберите сертификат из хранилища сертификатов**

  Если выбран этот вариант, можно указать сертификаты из хранилища. Условие категории соответствует только исполняемым файлам, которые подписаны указанным сертификатом.

  > Если в качестве условия срабатывания правила вы выбрали сертификат, убедитесь, что этот сертификат добавлен в доверенное системное хранилище на компьютере, и проверьте параметры использования доверенного системного хранилища в приложении.

- **Задайте путь к приложению (поддерживаются маски)**

  Если выбран этот вариант, можно указать файл или папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию приложений. Вы можете использовать регулярные выражения, такие как `C:\path_to_exe\*`, например: `C:\Program Files\Internet Explorer\*`.

- **Съемный диск**

  Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск приложения. Приложения, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию приложений.

- **Хеши файлов папки, метаданные файлов папки или сертификаты из папки**:

  - **Выберите из списка исполняемых файлов**

    Если выбран этот вариант, приложения для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

  - **Выберите из реестра приложений**

    Если выбран этот параметр, отображается реестр приложений. После того как вы выберете приложение из реестра, откроется окно с параметрами, заполненными метаданными из выбранного вами приложения:

    - Имя файла.
    - Версия файла. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
    - Название приложения.

- Версия приложения. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".

- Производитель.

Обратите внимание, что блокируется только запуск исполняемых файлов, соответствующих указанным параметрам, но не запуск выбранного вами приложения. Если выбранные метаданные программы совпадают с метаданными исполняемого файла, который запускается при запуске программы, вы можете перейти к следующему шагу. Иначе вам нужно будет изменить значения вручную, чтобы они совпадали с метаданными исполняемого файла.

- **Задайте вручную**

  Если выбран этот вариант, вам нужно указать хеш файла, метаданные или сертификат в качестве условия добавления приложений в пользовательскую категорию.

  Хеш файла

  В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Endpoint Security для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

  SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 и выше поддерживают вычисление хеш-функции SHA256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10.

  Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Endpoint Security для файлов категории:

  - Если все экземпляры приложений безопасности, установленных в вашей сети, являются версиями приложения Kaspersky Endpoint Security 10 и выше, установите флажок **SHA256**. Не рекомендуется добавлять категорию, созданную по критерию SHA256 исполняемого файла, для версий приложений ниже Kaspersky Endpoint Security 10. Это может привести к сбою приложения безопасности. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.

  - Если в вашей сети установлены более ранние версии, чем Kaspersky Endpoint Security 10, установите флажок **MD5-хеш**. Добавить категорию, созданную по критерию контрольной суммы MD5 исполняемого файла, для Kaspersky Endpoint Security 10 и выше, невозможно. В этом случае вы можете использовать криптографическую хеш-функцию SHA256 для файлов категории.

  - Если разные устройства в вашей сети используют как более ранние, так и более поздние версии Kaspersky Endpoint Security 10, установите флажок **SHA256** и флажок **MD5-хеш**.

  Метаданные

  Если этот параметр выбран, вы можете указать метаданные файла такие как имя файла, версию файла и поставщика. Условие категории соответствует только исполняемым файлам с одинаковыми метаданными.

  Сертификат

  Если выбран этот вариант, можно указать сертификаты из хранилища. Условие категории соответствует только исполняемым файлам, которые подписаны указанным сертификатом.

- **Из файла MSI-пакета/архивной папки**

  Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать файл установщика MSI. Метаданные установщика приложения будут передаваться на Сервер администрирования. Приложения, у которых метаданные установщика совпадают с указанным установщиком MSI, будут добавлены в пользовательскую категорию приложений.

Шаг 4. Параметры

Этот шаг доступен, если вы выбрали тип категории **Категория, в которую входят исполняемые файлы с выбранных устройств. Исполняемые файлы обрабатываются автоматически, их метрики заносятся в категорию**.

На этом шаге нажмите на кнопку **Добавить** и укажите компьютеры, исполняемые файлы с которых Kaspersky Security Center добавит в категорию приложений.

Также на этом шаге задайте следующие параметры:

- **Алгоритм вычисления хеш-функции**

  В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

  SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security для Linux поддерживает вычисление SHA256.

  Выберите один из вариантов вычисления хеш-функции для файлов категории:

  - Если вы используете Kaspersky Endpoint Security для Linux на защищаемых устройствах, установите флажок **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**.

  - Если вы используете Kaspersky Endpoint Security для Windows на защищаемых устройствах, установите флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**.

  Если в вашей сети используют как приложения для Windows, так и приложения для Linux, установите оба флажка.

- **Синхронизировать данные с хранилищем Сервера администрирования**

  Выберите этот параметр, если вы хотите, чтобы Сервер администрирования периодически выполнял проверку изменений в указанной папке (или папках).

  По умолчанию параметр выключен.

  Если вы включите этот параметр, укажите период (в часах), чтобы проверять изменения в указанной папке (папках). По умолчанию период проверки равен 24 часам.

- **Тип файла**

  В этом разделе вы можете указать тип файла, который используется для создания категории приложений.

  Все файлы. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.

  Только файлы вне категорий приложений. Для создаваемой категории учитываются только файлы вне категорий приложений.

- **Папки**

  В этом разделе вы можете указать папки выбранных устройств, содержащие файлы, которые используются для создания категории приложений.

  Все папки. Для создаваемой категории учитываются все папки. По умолчанию выбран этот вариант.

  Указанная папка. Для создаваемой категории учитывается только указанная папка. Если вы выбирали этот параметр, вам нужно указать путь к папке.

Шаг 5. Выбор папки

> Этот шаг доступен, если вы выбрали тип категории **Категория, в которую входят исполняемые файлы из указанной папки. Исполняемые файлы приложений, копируемых в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию**.

На этом шаге укажите папку, исполняемые файлы которой будут использоваться для создания категории.

Настройте следующие параметры:

- **Включать в категорию динамически подключаемые библиотеки (DLL)**

  В категорию приложений включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль приложений регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky Security Center.

  По умолчанию флажок снят.

- **Включать в категорию данные о скриптах**

  В категорию приложений включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky Security Center.

  По умолчанию флажок снят.

- **Алгоритм вычисления хеш-функции**

  В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky Security Center для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security для Linux поддерживает вычисление SHA256.

Выберите один из вариантов вычисления хеш-функции для файлов категории:

- Если вы используете Kaspersky Endpoint Security для Linux на защищаемых устройствах, установите флажок **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**.

- Если вы используете Kaspersky Endpoint Security для Windows на защищаемых устройствах, установите флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**.

Если в вашей сети используют как приложения для Windows, так и приложения для Linux, установите оба флажка.

- **Принудительно проверять папку на наличие изменений**

  Если этот параметр включен, приложение периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

  Если этот параметр выключен, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

  По умолчанию флажок снят.

Шаг 6. Создание пользовательской категории

Завершите работу мастера. В результате работы мастера будет создана новая категория приложений, запуск которых вы можете контролировать с помощью правил контроля приложений.

"Золотой образ"

При помощи задачи Инвентаризация вы можете добавить категорию приложений "Золотой образ" (Golden Image). По умолчанию категория пуста. В категорию "Золотой образ" добавляются приложения, которые поставляются на устройство вместе с операционной системой. Приложения из этой категории можно считать доверенными. При необходимости вы можете дополнить категорию сторонними приложениями.

По завершении задачи Инвентаризация приложение может изменять категорию "Золотой образ" следующим образом:

- **Оставить без изменений** – не изменять категорию приложений "Золотой образ" после выполнения инвентаризации. По умолчанию выбрано это значение. Этот вариант используется, когда вы хотите получить список сторонних приложений, используемых на устройстве, но не записывать их в категорию "Золотой образ".

- **Обновить или создать (если не создана)** – добавлять приложения, обнаруженные на устройстве при инвентаризации, в категорию "Золотой образ". Если категория отсутствует, она будет создана. Если категория существует, список приложений в ней будет обновлен.

- **Удалить** – очистить категорию приложений "Золотой образ" (Golden Image). Приложение очищает категорию сразу после запуска задачи без инвентаризации файлов на устройстве.

  Этот вариант может использоваться в следующих сценариях:

  - Если вам необходимо запретить запуск приложений из категории "Золотой образ" на устройстве, но отключить правило контроля приложений при этом невозможно.
  - Если вы применяете к устройству новую политику, содержащую отличные от текущей политики правила контроля приложений, а также при переносе устройства на дочернюю политику. В таком случае рекомендуется очистить категорию "Золотой образ", чтобы избежать ошибочной блокировки разрешенных приложений.

Настройка категории "Золотой образ" на основе эталонного компьютера

Вы можете использовать эталонный компьютер для создания категории "Золотой образ" с набором необходимых приложений. Далее вы можете использовать эту категорию для создания разрешающих правил Контроля приложений.

Настройка категории "Золотой образ" на основе эталонного компьютера состоит из следующих этапов:

1. **Настройте эталонный компьютер**

   Установите и настройте программное обеспечение, необходимое для работы устройств в сети организации, в том числе Kaspersky Endpoint Security для Linux и Агент администрирования.

2. **Создайте задачу Инвентаризации**

   Создайте задачу в Web Console или в командной строке и настройте следующие параметры:

   - Действие с категорией приложений "Золотой образ" – **Обновить или создать (если не создана)**;

     ```
     GoldenImageAction=Create
     ```

   - Область инвентаризации – эталонный компьютер.

3. **Запустите задачу инвентаризации и дождитесь ее выполнения**

   В результате выполнения задачи Kaspersky Endpoint Security сформирует категорию приложений "Золотой образ".

4. **Экспортируйте список категорий в файл**

   > Экспортировать список категорий в Web Console невозможно.

   Выполните команду:

   ```
   kesl-control [-A] --get-categories --file <path to file> --json
   ```

   где `<path to file>` – путь к конфигурационный файлу, в который будут экспортированы настройки.

5. **Если необходимо, скорректируйте категорию "Золотой образ"**

   Проверьте конфигурационный файл со списком категорий приложений. Если необходимо, скорректируйте список приложений в категории "Золотой образ".

6. **Импортируйте настройки из конфигурационного файла**

   Если вы изменяли конфигурационный файл со списком категорий приложений, импортируйте его в приложение:

```
kesl-control [-A] --set-categories --names GoldenImage [<category name 1> <category name 2> ... <name of category N>] --file <path to file>
```

   где `<category name 1> <category name 2> ... <category name N>` – названия категорий помимо категории "Золотой образ", информацию о которых вы хотите изменить.

   `<path to file>` – путь к конфигурационный файлу, в который будут экспортированы настройки.

В результате настроек вы сможете использовать категорию "Золотой образ" для создания правил контроля приложений.

О правилах контроля приложений

Правило контроля приложений – набор условий, при которых Контроль приложений разрешает или запрещает запуск стороннего приложения выбранной группе пользователей.

Правила ограничивают запуск сторонних приложений по следующим критериям:

- **Категории приложений**. Принадлежность приложения к категории приложений.

  Вы можете использовать одну и ту же категорию только в одном правиле.

- **Пользователи и группы пользователей**. Контроль приложений позволяет ограничить доступ к сторонним приложениям для отдельных пользователей или групп пользователей. Например, вы можете ограничить доступ к приложениям для удаленного администрирования для всех пользователей организации, кроме IT-отдела.

Правила контроля приложений могут иметь один из следующих *статусов работы*:

- **Включено**. Контроль приложений применяет это правило.
- **Выключено**. Контроль приложений не применяет это правило.
- **Тест**. Контроль приложений не запрещает запуск сторонних приложений, но отправляет уведомления об их запуске на Сервер администрирования.

Как добавить правило контроля приложений в Web Console

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

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль безопасности** → **Контроль приложений**.

5. Убедитесь, что переключатель работы компонента находится в положении **Контроль приложений ВКЛЮЧЕН**.

6. В блоке **Действие при запуске приложений** нажмите на кнопку **Добавить**.

   Откроется форма добавления правила контроля приложений.

7. В поле **Статус** задайте статус правила.

8. Если вы хотите протестировать работу правила, установите переключатель в положение **Включено** и установите флажок **Тестовый режим**.

9. В поле **Имя правила** введите имя правила. Имя правила должно быть уникальным.

10. Выберите категорию приложений, к которым применится правило. Если категория не указана, вы не сможете сохранить правило.

11. Выберите пользователей или группу пользователей и права запуска для них.

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

Как добавить правило контроля приложений в командной строке

1. Выведите список правил контроля приложений в файл:

```
kesl-control --get-settings 21 --file <path to file> [--json]
```

2. Откройте конфигурационный файл и добавьте секцию для правила с идентификатором `#` в зависимости от режима работы Контроля приложений:

   a. Если выбран режим `AppControlMode=AllowList`:

```
[AllowListRules.item_#]
Description=<rule name>
AppControlRuleStatus=<On|Off|Test>
Category=<category name>
[AllowListRules.item_#.ACL.item_#]
Access=<Allow|Block>
Principal=<user>
```

   b. Если выбран режим `AppControlMode=DenyList`:

```
[DenyListRules.item_#]
Description=<rule name>
AppControlRuleStatus=<On|Off|Test>
Category=<category name>
[DenyListRules.item_#.ACL.item_#]
Access=<Allow|Block>
Principal=<user>
```

3. Импортируйте настройки конфигурационного файла в приложение:

```
kesl-control --set-settings 21 --file <path to file> [--json]
```

Условные обозначения

Параметры команды

Параметр	Описание
[AllowListRules.item_#] [DenyListRules.item_#]	Правило контроля приложений с идентификатором #.
[AllowListRules.item_#.ACL.item_#] [DenyListRules.item_#.ACL.item_#]	Список пользователей, на которых распространяется правило контроля приложений с идентификатором #.
Description	Описание правила контроля приложений.
AppControlRuleStatus	Статус работы правила контроля приложений: On (значение по умолчанию) – правило включено, Kaspersky Endpoint Security применяет это правило для контроля приложений. Off – правило не используется для контроля приложений. Test – Kaspersky Endpoint Security разрешает запуск приложений, на которые распространяется действие правила, но фиксирует информацию о запуске этих приложений в отчете.
Category	Название категории приложений, для которой применяется правило. Вы можете указать категорию "Золотой образ" (Golden Image).
Access	Тип доступа, назначаемый пользователю или группе пользователей: Allow (значение по умолчанию) – разрешать запуск приложений. Block – запрещать запуск приложений.
Principal	Пользователь или группа пользователей, на которых распространяется правило контроля приложений: \Everyone (значение по умолчанию) – правило применяется для всех пользователей. <user> – имя пользователя, для которого применяется правило. @<group name> – название группы пользователей, для которых применяется правило.

Режим тестирования правил контроля приложений

Чтобы убедиться, что Контроль приложений не блокирует необходимые для работы приложения, рекомендуется протестировать правила контроля приложений. В тестовом режиме Kaspersky Endpoint Security не блокирует запуск сторонних приложений и отправляет уведомления об их запуске на Сервер администрирования.

По умолчанию Контроль приложений разрешает запуск всех сторонних приложений, кроме запрещенных правилами.

Тестирование правил Контроля приложений

1. **Сформируйте правила Контроля приложений**

   Настройте и включите правила контроля приложений, которые вы хотите протестировать. Например, вы можете составить правила, запрещающие запуск любых сторонних приложений, кроме приложений из категорий "Золотой образ" и "Приложения для работы".

2. **Включите Контроль приложений в тестовом режиме**

Как включить тестовый режим Контроля приложений в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль приложений**.
5. Убедитесь, что переключатель работы компонента находится в положении **Контроль приложений ВКЛЮЧЕН**.
6. В блоке **Действие при запуске приложений** выберите действие Контроля приложений **Информировать**.
7. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Как включить тестовый режим Контроля приложений в командной строке

Для включения тестового режима работы Контроля приложений выполните команду:

```
kesl-control --set-settings 21 AppControlRulesAction=TestRules
```

3 Ознакомьтесь с результатами тестирования

Изучите отчет Контроля приложений и события по результатам работы компонента, приходящие в Kaspersky Security Center.

Как посмотреть отчет Контроля приложений в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль приложений**.
5. Убедитесь, что переключатель работы компонента находится в положении **Контроль приложений ВКЛЮЧЕН**.
6. В таблице правил контроля приложений нажмите на кнопку **Посмотреть отчет**.
7. Откроется окно **Отчет о запрещенных приложениях в тестовом режиме**.
8. Ознакомьтесь с информацией о запусках запрещенных приложений в тестовом режиме.

Как посмотреть события по результатом тестовой работы Контроля приложений

1. В главном окне Web Console выберите **Мониторинг** → **Выборки событий**.
2. Нажмите на кнопку **Добавить**.

3. В открывшемся окне **Новая выборка событий** укажите имя выборки. Например, "Тестирование правил Контроля приложений".

4. Перейдите в раздел **События** и задайте следующие параметры:

   - **Название приложения** – Kaspersky Endpoint Security для Linux.
   - **Уровень критичности** – **Информационное сообщение**.
   - Выберите опцию **Включить выбранные общие события**.
   - Установите флажки напротив событий **Запуск приложения запрещен в тестовом режиме** и **Запуск приложения разрешен в тестовом режиме**.

5. Если необходимо, настройте остальные параметры.

6. Сохраните внесенные изменения.

7. Нажмите на имя выборки, чтобы посмотреть результат выборки событий.

4 **Скорректируйте правила**

Если для всех приложений, которые необходимы для работы пользователю компьютера, отсутствуют события о запрете запуска в тестовом режиме, то созданы верные правила.

В противном случае скорректируйте параметры созданных вами правил, создать дополнительные или удалить существующие правила.

Контроль целостности системы

Контроль целостности системы отслеживает изменения в операционной системе, которые могут указывать на нарушения безопасности компьютера. Обнаружив такие изменения, Kaspersky Endpoint Security формирует соответствующие события и предупреждает администратора.

Как работает Контроль целостности системы

Контроль целостности системы может работать в режиме реального времени и по запросу:

- Компонент *Контроль целостности системы* позволяет *в реальном времени* отслеживать изменения в файлах и директориях, которые вы включили в область мониторинга.
- Задача *Проверка целостности системы* позволяет *по расписанию или в ручном режиме* сравнивать текущее состояние объектов, включенных в область мониторинга, с зафиксированным состоянием.

Компонент Контроль целостности системы не передает данные о том, какие именно изменения внесены. Задача *Проверка целостности системы* передает данные об измененных атрибутах и перемещенных файлах и директориях.

Особенности и ограничения

- Технологические ограничения операционной системы Linux не позволяют приложению определять, какой пользователь или процесс внес изменение в файл.
- При добавлении директории в область мониторинга или в область исключения приложение не проверяет, существует ли такая директория.

Контроль целостности системы в реальном времени

Контроль целостности системы позволяет в режиме реального времени определять изменения объекта, включенного в область мониторинга.

Как работает Контроль целостности системы

1. **Приложение перехватывает события файловых операций**

   Приложение использует специальный механизм перехвата, который работает в режиме "только для чтения" при обращении к проверяемому файлу.

2. **Приложение проверяет изменения в файле**

   Контроль целостности системы отслеживает изменения в следующих свойствах файла:

   - содержимое (`write ()`, `truncate ()` и другие изменения);
   - метаданные (изменение прав доступа командами `chmod`/`chown`);
   - отметки времени (`utimensat`);
   - расширенные атрибуты (`setxattr`) и другие.

3. **Завершение проверки**

   Приложение формирует событие *Нарушена целостность системы*, если файл был изменен.

Настройка Контроля целостности системы

1. **Включите Контроль целостности системы**

   По умолчанию Контроль целостности системы выключен. Определите устройства, для которых вы хотите отслеживать изменения файлов в режиме реального времени, и включите компонент Контроль целостности системы на этих устройствах.

2. **Настройте область мониторинга**

   Для работы компонента должна быть указана хотя бы одна область мониторинга. По умолчанию задана область мониторинга *Внутренние объекты "Лаборатории Касперского"* (`/opt/kaspersky/kesl/`).

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в каком эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

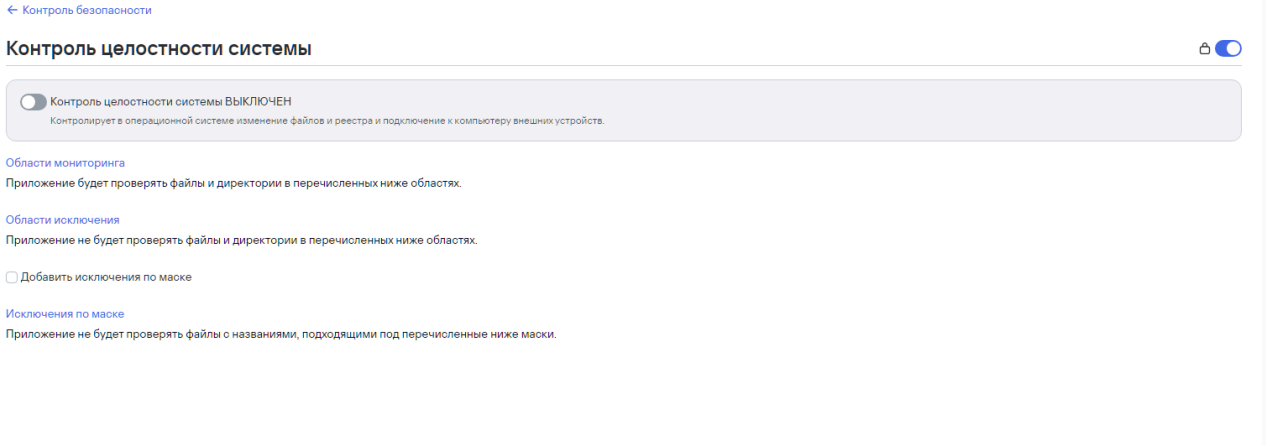
Как задать область мониторинга в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль целостности системы**.
5. Нажмите на ссылку **Области мониторинга**.

   Откроется окно с таблицей областей проверки.
6. Нажмите на кнопку **Добавить**.

   Откроется окно добавления областей проверки.
7. В поле **Имя** укажите имя области мониторинга, например, *Критические объекты*.
8. В поле **Путь** укажите путь к отдельному файлу или к директории (например, `/path/to/folder`). Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.
9. Если необходимо, укажите маски имен объектов в формате командной оболочки (например, `*.txt` или `file?.*`). Добавляйте маски по одной.
10. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.



Контроль целостности системы

Как задать область мониторинга в командной строке

1. Выполните команду:

```
kesl-control --set-settings 11  ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 11
```

Условные обозначения

Параметры команды

Параметр	Описание
`UseScanArea=Yes`	Включение области мониторинга с идентификатором `#`. Вы можете временно отключить проверку области мониторинга для приложения, а не удалять область. Для этого задайте значение `ScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Описание области мониторинга, содержит дополнительную информацию об области мониторинга.
`AreaMask.item_#`	Ограничение области мониторинга. В области мониторинга приложение проверяет только объекты, указанные с помощью масок в формате shell. Например, `ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Путь к директории для мониторинга. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

Пример

Область мониторинга, которая включает в себя только директорию `/etc` :

```
kesl-control --set-settings 11 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

3. **Настройте области исключения**

Исключение имеет более высокий приоритет, чем область мониторинга. Исключенный объект не проверяется, даже если находится в области мониторинга. Если область мониторинга задана на более низком уровне, чем директория, указанная в исключении, то приложение не отслеживает эту область мониторинга во время контроля целостности системы.

Как задать область исключения в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль безопасности** → **Контроль целостности системы**.

Исключения можно задать по пути или по маске имени файла. Приложение будет исключать из проверки директорию целиком (или отдельный файл), либо исключать из проверки файлы с подходящей маской имени в областях мониторинга.

Чтобы добавить исключения по пути:

1. Нажмите на ссылку **Области исключения**.

   Откроется окно с таблицей областей исключения.

2. Нажмите на кнопку **Добавить**.

   Откроется окно добавления областей исключения.

3. В поле **Имя** укажите имя области исключения, например, *Системные файлы*.

4. В поле **Путь** укажите путь к отдельному файлу или к директории (например, `/path/to/folder`). Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

5. Укажите маски имен объектов в формате командной оболочки (например, `*.txt` или `file?.*`). Добавляйте маски по одной.

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

Чтобы добавить исключения по маске имени файла:

1. Установите флажок **Добавить исключения по маске**.

2. Нажмите на ссылку **Исключения по маске**.

   Откроется таблица с областями исключений по маске.

3. Нажмите на кнопку **Добавить**.

   Откроется окно добавления областей исключения по маске.

4. Укажите маску имени файла в формате командной оболочки (например, `*.txt` или `file?.*`). Добавляйте маски по одной.

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

Как задать область исключения в командной строке

1. Выполните команду:

```
kesl-control --set-settings 11  ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 11
```

Условные обозначения

Параметры команды

Параметр	Описание
`UseScanArea=Yes`	Исключение указанной области из мониторинга. с идентификатором `#`. Вы можете временно отключить область исключения для приложения, а не удалять область. Для этого задайте значение `ExcludedFromScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Описание области исключения из мониторинга, содержит дополнительную информацию об области исключения из мониторинга.

Параметр	Описание
`AreaMask.item_#`	Ограничение области исключения. В области исключения приложение не проверяет только объекты, указанные с помощью масок в формате shell. Например, `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Путь к директории, которую необходимо исключить из проверки. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

Пример

Область исключения, которая включает в себя только директорию `/tmp`:

```
kesl-control --set-settings 11 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

Проверка целостности системы

Во время выполнения задачи *Проверка целостности системы* приложение сравнивает текущее состояние каждого объекта с исходным состоянием – *снимком состояния системы*. Снимок состояния системы содержит пути к контролируемым объектам и их метаданные. Это позволяет отслеживать изменения в файлах и директориях, включенных в область мониторинга.

Снимок состояния системы может содержать персональные данные.

В отличие от компонента Контроль целостности системы, задача *Проверка целостности системы* позволяет уменьшить количество событий и сформировать общий отчет об изменениях в операционной системе.

Как работает Проверка целостности системы

1. **Приложение создает снимок состояния системы**

   Снимок состояния системы создается во время первого выполнения задачи. Если вы создали несколько задач проверки целостности системы, для каждой задачи создается отдельный снимок состояния системы. Снимок состояния системы обновляется при изменении настроек задачи (например, при добавлении новой области мониторинга), а также при запуске задачи с включенной настройкой **Обновлять снимок состояния системы при каждом запуске задачи**.

   Снимки состояния системы хранятся в базе данных `/var/opt/kaspersky/kesl/private/fim.db`. Для доступа к базе данных, в которой хранятся снимки состояния системы, требуются root-права. Снимок состояния системы удаляется вместе с соответствующей задачей проверки целостности системы.

2. **Приложение проверяет изменения в состоянии системы**

Приложение сравнивает информацию об объектах, которые входят в область мониторинга, по следующим критериям:

- SHA256-хеш файла (для полной проверки);
- время изменения файла;
- размер файла.

3. **Завершение проверки**

   Если текущее состояние системы отличается от снимка состояния системы, Kaspersky Endpoint Security формирует событие о нарушении целостности системы *Нарушена целостность системы*.

Настройка и запуск задачи Проверка целостности системы

1. **Создайте задачу Проверка целостности системы**

   Как создать задачу Проверка целостности системы в Web Console

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

      Откроется список задач.

   2. Нажмите на кнопку **Добавить**.

      Запустится мастер создания задачи.

   3. Настройте параметры задачи:

      a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Linux 12.5**.

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

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

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

   4. Выберите устройства в соответствии с выбранным вариантом области действия задачи.

   5. Завершите работу мастера.

   Как создать задачу Проверка целостности системы в командной строке

   Для создания задачи выполните команду:

   ```
   kesl-control --create-task <task name> --type ODFIM
   ```

   где `<task name>` – имя новой задачи.

   В результате выполнения команды приложение отобразит ID созданной задачи.

   Пример результата выполнения команды:

   Задача создана (идентификатор задачи: 115)

2 **Если необходимо, измените настройки задачи**

Как настроить задачу Проверка целостности системы в Web Console

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

   Откроется список задач.

2. Нажмите на созданную задачу проверки целостности системы.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. Выберите тип проверки:

   - **Полная проверка**. Приложение будет сравнивать SHA256-хеш файла в текущем состоянии и в снимке состояния системы.

   - **Быстрая проверка**. Приложение будет сравнивать только размер файла. Если размер файла не изменился, время изменения не считается критическим параметром.

5. В разделе **Настройки проверки целостности системы** установите флажки:

   - **Обновлять снимок состояния системы при каждом запуске задачи**. Если флажок установлен, приложение обновляет снимок состояния системы при каждом запуске задачи.

   - **Проверять директории в областях мониторинга**. Если флажок установлен, приложение проверяет директории, заданные пользователем. Если флажок снят, приложение проверяет только область по умолчанию *Внутренние объекты "Лаборатории Касперского"* (`/opt/kaspersky/kesl/`).

   - **Отслеживать время последнего доступа к файлу при каждом запуске задачи**. Если флажок установлен, приложение проверяет время последнего обращения к файлу (параметр `noatime`) при каждом запуске задачи.

6. Сохраните внесенные изменения.

Как настроить задачу Проверка целостности системы в командной строке

Выполните команду:

```
kesl-control --set-settings <task ID|name> RebuildBaseline=<Yes|No> [CheckFileHash=<Yes|No>]
[TrackDirectoryChanges=<Yes|No>] [TrackLastAccessTime=<Yes|No>] [UseExcludeMasks=<Yes|No>]
[ExcludeMasks.item_#=<object mask>]
```

Условные обозначения

Параметры задачи *Проверка целостности системы*

Параметр	Описание
`RebuildBaseline`	Обновления снимка состояния системы при каждом запуске задачи.
`CheckFileHash`	Проверка SHA256-хеш файла. Если проверка выключена, приложение сравнивает только размер файла (если размер файла не изменился, время изменения не считается критическим параметром).
`TrackDirectoryChanges`	Проверка директорий, заданных пользователем. Если параметр выключен, приложение проверяет только область по умолчанию (`/opt/kaspersky/kesl/`).
`TrackLastAccessTime`	Проверка времени последнего обращения к файлу (параметр `noatime`).

Параметр	Описание
`UseExcludeMasks`	Исключения из области мониторинга. В параметры задачи будет добавлена новая секция `[ExcludeMasks.item_#]`. Приложение не будет проверять объекты, указанные в этой секции. Этот параметр работает, только если задано значение параметра `ExcludeMasks.item_#`.
`ExcludeMasks.item_#= <object mask>`	Исключение объектов из области мониторинга. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате командной оболочки. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски. Значение параметра можно задать только если включен параметр `UseExcludeMasks`. Вы можете указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом. Пример: `ExcludeMasks.item_0000=<eicar1.*>`

3 Настройте область мониторинга

Для запуска задачи должна быть указана хотя бы одна область мониторинга. По умолчанию задана область мониторинга *Внутренние объекты "Лаборатории Касперского"* (`/opt/kaspersky/kesl/`).

Задача выполняется, только если снимок состояния системы содержит информацию об объектах, которые входят в область мониторинга задачи.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в каком эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Как задать область мониторинга в Web Console

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

   Откроется список задач.

2. Нажмите на созданную задачу проверки целостности системы.

   Откроется окно свойств задачи.

3. Выберите вкладку **Параметры приложения**.

4. Убедитесь, что установлен флажок **Проверять директории в областях мониторинга**.

5. В блоке **Области проверки и исключения** нажмите на ссылку **Области мониторинга**.

   Откроется окно с таблицей областей проверки.

6. Нажмите на кнопку **Добавить**.

   Откроется окно добавления областей проверки.

7. В поле **Имя** укажите имя области мониторинга, например, *Файлы на рабочем столе*.

8. В поле **Путь** укажите путь к отдельному файлу или к директории (например, `/path/to/folder`). Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

9. Если необходимо, укажите маски имен объектов в формате командной оболочки (например, `*.txt`, `file?.*`). Добавляйте маски по одной.

10. Сохраните внесенные изменения.

Как задать область мониторинга в командной строке

1. Выполните команду:

```
kesl-control --set-settings <task ID|name> TrackDirectoryChanges=Yes ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. Для проверки текущих настроек задачи выполните следующую команду:

```
kesl-control --get-settings <task ID|name>
```

Условные обозначения

Параметры задачи *Проверка целостности системы*

Параметр	Описание
`UseScanArea=Yes`	Включение области мониторинга с идентификатором `#`. Вы можете временно отключить проверку области мониторинга для приложения, а не удалять область. Для этого задайте значение `ScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Описание области мониторинга, содержит дополнительную информацию об области мониторинга.
`AreaMask.item_#`	Ограничение области мониторинга. В области мониторинга приложение проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `ScanScope.item_#.AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Например, `ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Путь к директории для мониторинга. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

Пример

Область мониторинга, которая включает в себя только директорию `/etc` :

```
kesl-control --set-settings 115 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

4 Настройте области исключения

Исключение имеет более высокий приоритет, чем область мониторинга. Исключенный объект не проверяется, даже если находится в области мониторинга. Если область мониторинга задана на более низком уровне, чем директория, указанная в исключении, то приложение не отслеживает эту область мониторинга во время контроля целостности системы.

Как задать область исключения в Web Console

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

2. Откроется список задач.

3. Нажмите на созданную задачу проверки целостности системы.

   Откроется окно свойств задачи.

4. Выберите вкладку **Параметры приложения**.

Исключения можно задать по пути или по маске имени файла. Приложение будет исключать из проверки директорию целиком (или отдельный файл), либо исключать из проверки файлы с подходящей маской имени в областях мониторинга.

Чтобы добавить исключения по пути:

1. В блоке **Области проверки и исключения** нажмите на ссылку **Области исключения**.

   Откроется окно с таблицей областей исключения.

2. Нажмите на кнопку **Добавить**.

   Откроется окно добавления областей исключения.

3. В поле **Имя** укажите имя области исключения, например, *Системные файлы*.

4. В поле **Путь** укажите путь к отдельному файлу или к директории (например, `/path/to/folder`). Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

5. Укажите маски имен объектов в формате командной оболочки (например, `*.txt` или `file?.*`). Добавляйте маски по одной.

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

Чтобы добавить исключения по маске имени файла:

1. В блоке **Области проверки и исключения** нажмите на ссылку **Исключения по маске**.

   Откроется таблица с областями исключений по маске.

2. Нажмите на кнопку **Добавить**.

   Откроется окно добавления областей исключения по маске.

3. Укажите маску имени файла в формате командной оболочки (например, `*.txt` или `file?.*`). Добавляйте маски по одной.

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

Как задать область исключения в командной строке

1. Выполните команду:

```
kesl-control --set-settings <task ID|name>      ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. Для проверки текущих настроек задачи выполните следующую команду:

```
kesl-control --get-settings <task ID|name>
```

Условные обозначения

Параметры задачи *Проверка целостности системы*

Параметр	Описание
`UseScanArea=Yes`	Исключение указанной области из мониторинга с идентификатором `#`. Вы можете временно отключить область исключения для приложения, а не удалять область. Для этого задайте значение `ExcludedFromScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Описание области исключения из мониторинга, содержит дополнительную информацию об области исключения из мониторинга.
`AreaMask.item_#`	Ограничение области исключения. В области исключения приложение не проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `ExcludedFromScanScope.item_#.AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Например, `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Путь к директории, которую необходимо исключить из проверки. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

Пример

Область исключения, которая включает в себя только директорию `/tmp`:

```
kesl-control --set-settings 115 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

5 **Запустите задачу**

Как запустить задачу Проверка целостности системы в Web Console

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

   Откроется список задач.

2. Установите флажок напротив созданной задачи.

3. Нажмите на кнопку **Запустить**.

Как запустить задачу Проверка целостности системы в командной строке

Для запуска задачи выполните команду:

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

где:

- `<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `[-W]` – включение вывода текущих событий, связанных с этой задачей.
- `[--progress]` – включение отображения хода выполнения задачи.

Доверенная зона

Доверенная зона – это сформированный администратором системы список объектов и приложений, которые Kaspersky Endpoint Security не контролирует в процессе работы.

Доверенную зону администратор системы формирует самостоятельно в зависимости от особенностей объектов, с которыми требуется работать, а также от приложений, установленных на компьютере. Включение объектов и приложений в доверенную зону может потребоваться, например, если Kaspersky Endpoint Security блокирует доступ к какому-либо объекту или приложению, в то время как вы уверены, что этот объект или приложение безвредны.

Настройки Доверенной зоны

Настройка	Описание
Веб-адреса	Веб-адреса, которые компонент Защита от веб-угроз будет считать доверенными. Компонент не будет проверять входящий и исходящий трафик с этих адресов на наличие угроз. Список доверенных адресов может быть использован, например, если компонент препятствует загрузке файла с известного вам веб-сайта. Подробнее см. в статье Как добавить доверенные веб-адреса
IP-адреса	IP-адреса доверенных устройств. Компонент Защита от сетевых угроз не блокирует сетевую активность с этих адресов. Приложение также не заносит в отчет информацию о сетевых атаках с IP-адресов, входящих в список исключений. Подробнее см. в статье Как добавить доверенный IP-адрес компьютера
Сетевые порты	Список сетевых портов, которые компонент Защита от сетевых угроз исключает из проверки. Подробнее см. в статье Как выбрать контролируемые сетевые порты
Корневые сертификаты	Корневые сертификаты, которые приложение Kaspersky Endpoint Security будет считать доверенными. Список доверенных корневых сертификатов используется при проверке зашифрованных соединений (соединения по протоколу HTTPS) компонентами Защита от веб-угроз, Защита от почтовых угроз и Веб-Контроль. Подробнее см. в статье Как добавить сертификат в список доверенных корневых сертификатов
Домены	Список доверенных доменов. Компоненты Защита от веб-угроз и Веб-Контроль не контролируют зашифрованные соединения с этими доменами. Подробнее см. в статье Как добавить доверенный домен
Точки монтирования	Список доверенных точек монтирования. Компоненты Защита от файловых угроз, Защита от шифрования, Проверка контейнеров исключают указанные точки монтирования из проверки. Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды `mount`. Подробнее см. в статье Как исключить точки монтирования
Приложения	Приложения, у которых Kaspersky Endpoint Security не контролирует файловую и сетевую активности, а также обращения этих приложений к системному реестру. Компоненты защиты, например, Защита от файловых угроз или Анализ поведения, не будут контролировать активность указанных приложений. Подробнее см. в статье Как добавить доверенные приложения
Исключения из Поиска вредоносного ПО	Файлы или папки, а также типы объектов (согласно Вирусной энциклопедии), которые будут исключены из проверки всеми или некоторыми компонентами приложения. Подробнее см. в статье Как добавить исключения из защиты
Устройства	Устройства, к которым компонент Контроль устройств всегда разрешает полный доступ для выбранных пользователей или групп. Подробнее см. в статье Как добавить доверенные устройства

Как добавить исключения из защиты

Исключение из защиты – это совокупность условий, при выполнении которых приложение Kaspersky Endpoint Security не проверяет объекты на наличие вирусов и других вредоносных приложений.

Вы можете исключать из проверки объекты следующими способами:

- **Исключения**. Путь к директории. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски. Пример: `/.snapshots/*/snapshot/`.

  Для указания путей в контейнерах или образах используйте теги.

Правила использования тегов

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Где:

`<id>` – идентификатор контейнера.

`<name>` – имя контейнера.

`<path to local directory>` – путь к локальной директории.

Также вы можете использовать уникальные комбинации из тегов `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` и `[image-name:<name>]/path to local directory>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

- **Исключения по маске**. Имя файла, указанное с помощью маски. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски. Пример: маска `*.txt` – все текстовые файлы.

Используйте маски:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и директорий в путях к файлам и директориям). Например, маска `/dir/*/*.txt` будет включать все пути к файлам с расширением txt, расположенным в директориях внутри директории dir, но не в поддиректориях.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или директории, включая символы `\` и `/` (разделители имен файлов и директорий в путях к файлам и директориям). Например, маска `/dir/**/*.txt` будет включать все пути к файлам с расширением txt в директориях, вложенных в директорию dir, кроме самой директории dir.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и директорий в путях к файлам и директориям). Например, маска `/dir/???.txt` будет включать пути ко всем расположенным в директории dir файлам с расширением txt и именем, состоящим из трех символов.

- **Исключения по названию угрозы**. Название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`). Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, приложение исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

- **Исключения по процессам**. Путь к процессу.

Kaspersky Endpoint Security также позволяет исключать файлы определенных форматов: архивы, почтовые базы, текстовые файлы, файлы журналов баз данных.

Как добавить исключения из защиты в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Защита устройств от угроз** → **Защита от файловых угроз**.

5. Перейдите по ссылке **Исключения из проверки**.

6. В открывшемся окне нажмите на кнопку **Добавить**.

7. Установите флажок критериев, по которым вы хотите добавить исключение из защиты:

   - **Путь к файлу или папке**. Укажите путь к файлу, папке или маску имени файла. Для указания путей в контейнерах или образах используйте теги.

     Для локальной файловой системы укажите путь к директории (например, `/path/to/folder/`). Для смонтированной или всех удаленных смонтированных файловых систем укажите маску имени файла. Для смонтированной файловой системы также укажите протокол доступа (NFS, Samba или пользовательский).

   - **Тип объекта**. Укажите название угрозы.

   - **Хеш объекта**. Укажите SHA256 хеш объекта. Также вы можете добавить файл или указать событие, из которого будет сформирован SHA256 хеш исключения.

8. Выберите, к каким компонентам защиты применять исключение:

   - **Все компоненты защиты**. Исключение применится ко всем компонентам защиты, на которые влияют **Исключения из Поиска вредоносного ПО**.

   - **Выбранные компоненты защиты**. Выберите компоненты, к которым необходимо применить исключение: Защита от файловых угроз, Защита от шифрования, Защита от эксплойтов.

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

Как добавить исключения из защиты в командной строке

1. Для добавления исключения по пути выполните команду:

```
kesl-control --set-settings 1 --add-exclusion <path>
```

2. Для добавления исключения по маске выполните следующие действия:

   a. Включите исключение файлов по маске:

```
kesl-control --set-settings 1 UseExcludeMasks=Yes
```

   b. Добавьте маску файла:

```
kesl-control --set-settings 1 ExcludeMasks.item_#=<file mask>
```

3. Для добавления исключений по названию угрозы выполните следующие действия:

   a. Включите исключение файлов по названию угрозы:

```
kesl-control --set-settings 1 UseExcludeThreats=Yes
```

   b. Добавьте название угрозы:

```
kesl-control --set-settings 1 ExcludeThreats.item_#=<threat name>
```

4. Для проверки текущих значений параметров компонента выполните команду:

```
kesl-control --get-settings 1
```

Условные обозначения

Параметры команды

Параметр	Описание
`--add-exclusion`	Исключение из проверки директории. В параметры задачи будет добавлена новая секция `[ExcludedFromScanScope.item_#]`. Приложение будет исключать из проверки объекты в директории, указанной параметром `path`.
`ExcludeMasks.item_#`	Исключение из проверки объектов по именам или маскам. Используйте маски в формате shell для ввода имени файла. Пример: `ExcludeMasks.item_0000=*_my_file_??.html`.
`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных угроз. Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным. Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки. Пример: `ExcludeThreats.item_0000=EICAR-Test-*`.

Как добавить доверенные веб-адреса

Защита от веб-угроз, кроме вредоносных и фишинговых веб-сайтов, может заблокировать и другие веб-сайты. Например, Защита от веб-угроз блокирует HTTP-трафик, который не соответствует стандартам RFC. Вы можете сформировать список веб-адресов, содержанию которых вы доверяете. Компонент Защита от веб-угроз не анализирует информацию, поступающую с доверенных веб-адресов, на присутствие вирусов и других приложений, представляющих угрозу. Такая возможность может быть использована, например, в том случае, если компонент Защита от веб-угроз препятствует загрузке файла с известного вам веб-сайта.

Как добавить доверенный веб-адрес в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона**.
5. В открывшемся окне перейдите по ссылке **Веб-адреса**.

   Откроется окно со списком доверенных веб-адресов.
6. Сформируйте список адресов веб-сайтов / веб-страниц, содержимому которых вы доверяете.

   Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

   Вы также можете импортировать список доверенных веб-адресов из JSON-файла.
7. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Как добавить доверенный веб-адрес в командной строке

1. Для включения использования списка доверенных веб-адресов выполните команду:

```
kesl-control --set-settings 14 UseTrustedAddresses=Yes
```

2. Для добавления доверенного веб-адреса выполните команду:

```
kesl-control --set-settings 14 TrustedAddresses.item_#=<trusted web address>
```

3. Для проверки текущих значений параметров компонента выполните следующую команду:

```
kesl-control --get-settings 14
```

Пример

```
kesl-control --set-settings 14 TrustedAddresses.item_001=https://example.com/
```

Как добавить доверенный IP-адрес компьютера

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. Доверенные веб-адреса влияют на работу компонента Защита от сетевых угроз.

Как настроить адреса исключений из блокирования в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона**.
5. В открывшемся окне перейдите по ссылке **IP-адреса**.

   Откроется окно со списком доверенных IP-адресов.
6. В открывшемся окне нажмите на кнопку **Добавить**.
7. Введите IP-адрес компьютера, сетевые атаки с которого не должны блокироваться.

   Если требуется, укажите подсеть.
8. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Как настроить адреса исключений из блокирования в командной строке

1. Для применения доверенных IP-адресов выполните следующую команду:

```
kesl-control --set-settings 17 UseExcludeIPs=Yes
```

2. Для добавления доверенного IP-адреса выполните команду:

```
kesl-control --set-settings 17 ExcludeIPs.item_#=<IP address>
```

3. Для проверки списка доверенных IP-адресов выполните команду:

```
kesl-control --get-settings 17 TrustedIPAddresses
```

Пример

```
kesl-control --set-settings 17 ExcludeIPs.item_0000="192.168.2.0/24"
```

Как выбрать контролируемые сетевые порты

Во время работы Kaspersky Endpoint Security контролирует потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP-порты компьютера пользователя. По умолчанию приложение контролирует известные и зарегистрированные порты, например, 443 порт для HTTPS-соединений, 143 порт для работы почтового протокола IMAP и другие.

Доверенные сетевые порты – это сетевые порты, которые компонент Защита от сетевых угроз исключает из проверки. Это нужно, чтобы настроить совместимость Kaspersky Endpoint Security с доверенными сторонними сервисами и приложениями, а также для оптимизации производительности. Например, вы можете указать сетевые порты внутренних сервисов резервного копирования, чтобы приложение не препятствовало скачиванию или загрузке резервных копий.

Важно помнить, что исключение сетевых портов из проверки снижает защиту устройств. Используйте минимально необходимый набор исключений.

Как исключить сетевые порты из проверки в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона** → **Сетевые порты**.

   Откроется окно со списком контролируемых сетевых портов.
5. Выключите переключатель напротив портов, которые нужно исключить из проверки.

   Если нужного порта нет в списке, приложение не проверяет этот порт.
6. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Как исключить сетевые порты из проверки в командной строке

1. Получите список контролируемых портов, выполнив команду:

```
kesl-control --get-net-setting
```

2. Если включен режим контроля всех портов (`MonitorNetworkPorts=All`), выполните команду:

```
kesl-control --set-net-settings MonitorNetworkPorts=Selected
```

   Приложение добавит секцию `[NetworkPorts.item_#]`, содержащую контролируемые сетевые порты.

3. Если секция содержит порт, который нужно исключить из проверки, выполните следующие действия:

   a. Для вывода параметров проверки сетевого трафика в файл выполните команду:

   ```
   kesl-control --get-net-setting --file <path to file>
   ```

   b. Удалите в файле секции `[NetworkPorts.item_#]`, содержащие сетевые порты, которые не нужно контролировать.

   c. Для применения настроек выполните команду:

   ```
   kesl-control --set-net-settings --file <path to file>
   ```

   Измененные параметры будут импортированы в приложение.

Как добавить сертификат в список доверенных корневых сертификатов

Kaspersky Endpoint Security позволяет устанавливать доверенные корневые сертификаты на компьютеры пользователей, если, например, вам нужно развернуть новый центр сертификации. Приложение позволяет добавить сертификат в специальное хранилище сертификатов Kaspersky Endpoint Security. При этом сертификат будет доверенным только для приложения Kaspersky Endpoint Security. То есть пользователь будет иметь доступ к веб-сайту с новым сертификатом в браузере. Если другое приложение попытается получить доступ к веб-сайту, вы можете получить ошибку соединения из-за проблем с сертификатом.

Доверенные корневые сертификаты используется при работе следующих компонентов:

- Защита от веб-угроз
- Защита от почтовых угроз
- Веб-Контроль

Поддерживаются доверенные сертификаты в форматах CER, CRT, PEM и DER. Максимальный размер файла доверенного сертификата — 2 МБ.

Как установить доверенный корневой сертификат в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона** → **Корневые сертификаты**.
   Откроется окно со списком доверенных корневых сертификатов.
5. Нажмите на кнопку **Добавить**.
   Откроется форма добавления сертификата.
6. Загрузите сертификат.
7. Если необходимо, укажите описание сертификата в поле **Комментарий**.
8. Сохраните внесенные изменения.

В списке доверенных сертификатов в качестве названия сертификата используется его серийный номер.

Как установить доверенный корневой сертификат в командной строке

1. Для добавления сертификата выполните команду:

   ```
   kesl-control --add-certificate <path to certificate>
   ```

2. Для просмотра списка доверенных корневых сертификатов выполните команду:

   ```
   kesl-control --list-certificates
   ```

   Для каждого сертификата отображается следующая информация:

   - субъект сертификата;
   - серийный номер;
   - издатель сертификата;
   - дата начала срока действия сертификата;
   - дата окончания срока действия сертификата;
   - отпечаток сертификата SHA256.

3. Для удаления сертификата из списка выполните команду:

   ```
   kesl-control --remove-certificate <certificate subject>
   ```

Как добавить доверенный домен

Доверенные домены – это список доменных имен, для которых Kaspersky Endpoint Security не проверяет защищенные соединения. Доверенные домены влияют на работу компонентов Защита от веб-угроз и Веб-контроль. Исключение доменов из проверки позволяет избежать блокировок трафика от известных вам источников.

> Указывайте доменное имя. Веб-адреса, например `example.com/*` или `https://example.com`, учитываться не будут.

Как указать доверенные домены в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона** → **Доверенные домены**.

   Откроется окно со списком доверенных доменов.
5. Нажмите на кнопку **Добавить**.

   Откроется форма добавления домена
6. Укажите доменное имя или маску домена. Например, `*example.com`.
7. Сохраните внесенные изменения.

Как указать доверенные домены в командной строке

1. Для добавления домена выполните команду:

   ```
   kesl-control --set-net-settings ManageExclusions=Yes Exclusions.item_#.DomainName=<domain name>
   ```
2. Для проверки настроек выполните команду:

   ```
   kesl-control --get-net-settings
   ```

   Доверенные домены будут указаны в секции `[Exclusions.item_#]`.

Пример

```
kesl-control --set-net-settings Exclusions.item_0000.DomainName=example.com
```

Как исключить точки монтирования

Чтобы исключить файлы определенной директории не только из проверки, но и из перехвата, нужно исключить точку монтирования целиком. Такие исключения называются *глобальными исключениями*. Приложение исключает из проверки и перехвата файловых операций доверенные локальные или удаленные директории, смонтированные на устройстве. Например, вы можете исключить точки монтирования, которые содержат временные файлы, чтобы снизить нагрузку на систему и ускорить проверку.

Исключения из точек монтирования влияют на работу следующих компонентов:

- Защита от файловых угроз
- Защита от шифрования
- Проверка контейнеров

Также доверенные точки монтирования исключаются из проверки задачами:

- Поиск вредоносного ПО
- Проверка важных областей
- Проверка контейнеров
- Проверка съемных дисков

Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды `mount`.

Как указать доверенные точки монтирования в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона** → **Точки монтирования**.

   Откроется окно со списком доверенных точек монтирования.
5. Нажмите на кнопку **Добавить**.

   Откроется форма добавления точки монтирования.
6. В раскрывающемся списке файловых систем выберите тип файловой системы, на которой расположены директории для исключения: **Локальная**, **Смонтированная**, **Все удаленные смонтированные**.

   Kaspersky Endpoint Security поддерживает протоколы Samba или NFS для удаленных директорий.

Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды `mount`.

7. Введите название файловой системы, на которой расположены директории для исключения.

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

Как указать доверенные точки монтирования в командной строке

1. Если директория не является точкой монтирования, создайте из нее точку монтирования, выполнив следующую команду:

```
mount --bind <path to dir> <path to dir>
```

2. Чтобы точка монтирования сохранилась после перезагрузки сервера, добавьте в файл `/etc/fstab` следующую строку:

```
<path to dir> <path to dir> none defaults,bind 0 0
```

3. Перезапустите Kaspersky Endpoint Security:

```
systemctl restart kesl
```

4. Для добавления доверенной точки монтирования выполните команду:

```
kesl-control --set-app-settings ExcludedMountPoint.item_#=<path to mount point>
```

5. Перезапустите приложение, чтобы применить глобальные исключения:

```
systemctl restart kesl
```

Пример

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/tmp"
```

Как добавить доверенные приложения

Список доверенных приложений – это список приложений, у которых Kaspersky Endpoint Security не контролирует файловую активность и активность процессов (в том числе и вредоносную), а также память процессов. По умолчанию Kaspersky Endpoint Security контролирует объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех приложений.

Доверенные приложения влияют на работу следующих компонентов:

- Защита от файловых угроз
- Анализ поведения

А также на исключения памяти процессов из проверки.

Как указать доверенные приложения в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Доверенная зона** → **Доверенные приложения**.

   Откроется окно со списком доверенных приложений.
5. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных приложений для всех компьютеров организации. Списки доверенных приложений родительских и дочерних политик будут объединены. Приложения из родительской политики отображаются в дочерних только для просмотра, изменить или удалить их нельзя.

   > Для объединения списков должно быть включено наследование параметров родительской политики.
6. Нажмите на кнопку **Добавить**.

   Откроется форма добавления приложения.
7. Укажите путь или маску пути к приложению.
8. Настройте параметры доверенного приложения:

   - **Не проверять открываемые файлы**. Kaspersky Endpoint Security исключает из проверки все файлы, открываемые с помощью приложения.
   - **Не контролировать активность приложений**. Kaspersky Endpoint Security не контролирует файловую и сетевую активности доверенного приложения в операционной системе.

     Вы также можете настроить контроль активности приложения отдельно для компонентов MDR и EDR (KATA), установив флажок **Не контролировать для Managed Detection and Response и Endpoint Detection and Response**.
   - **Не контролировать активность дочерних приложений**. Kaspersky Endpoint Security не контролирует файловую и сетевую активности приложений, которые запускает доверенное приложение.
   - **Не проверять память указанного приложения**. Kaspersky Endpoint Security не проверяет память процессов, запускаемых доверенным приложением.

В Web Console параметр **Комментарий** недоступен для Kaspersky Endpoint Security для Linux.

9. Сохраните внесенные изменения.

Как указать доверенные приложения в командной строке

1. Для исключения из проверки файловой активности доверенного приложения выполните команду:

```
kesl-control --set-settings 1 ExcludedForProgram.item_#.UseExcludedForProgram=Yes
ExcludedForProgram.item_#.ProgramPath=<path to app> ExcludedForProgram.item_#.AreaDesc=<trusted app name>
[ExcludedForProgram.item_#.ApplyToDescendants=Yes]
```

2. Для исключения из проверки активности процессов доверенного приложения выполните команду:

```
kesl-control --set-set 20 UseTrustedPrograms=Yes TrustedPrograms.item_#.UseTrustedProgram=Yes
TrustedPrograms.item_#.ProgramPath=<path to app> TrustedPrograms.item_#.ProgramDesc=<trusted app name>
[TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes] [TrustedPrograms.item_#.ApplyToDescendants=Yes]
```

3. Для исключения из проверки памяти процессов доверенного приложения выполните команду:

```
kesl-control --set-app-settings MemScanExcludedProgramPath.item_#=<path to app>
```

Условные обозначения

Параметры команды

Параметр	Описание
`ExcludedForProgram.item_#.UseExcludedForProgram=Yes`	Исключать файловую активность доверенного приложения из проверки компонентом Защита от файловых угроз.
`ExcludedForProgram.item_#.ProgramPath`	Путь к доверенному приложению с идентификатором `#`. Компонент Защита от файловых угроз не будет проверять процессы указанного приложения. Если для перехвата системных событий используется обновляемый модуль ядра, указанный процесс исключается из перехвата во всех пространствах имен.
`ExcludedForProgram.item_#.AreaDesc`	Имя доверенного приложения с идентификатором `#`.
`ExcludedForProgram.item_#.ApplyToDescendants=Yes`	Исключать дочерние процессы доверенного приложения из проверки компонентом Защита от файловых угроз.
`UseTrustedPrograms=Yes`	Исключать активность процессов доверенных приложений из проверки компонентом Анализ поведения.
`TrustedPrograms.item_#.UseTrustedProgram=Yes`	Исключать из проверки активность доверенного приложения с идентификатором `#`.
`TrustedPrograms.item_#.ProgramPath`	Путь к доверенному приложению с идентификатором `#`. Компонент Анализ поведения не будет проверять процессы указанного приложения. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.
`TrustedPrograms.item_#.ProgramDesc`	Имя доверенного приложения с идентификатором `#`.
`TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes`	Исключать активность доверенного приложения из телеметрии, которую собирают компоненты Managed Detection and Response и Endpoint Detection and Response Expert (on-premises).

Параметр	Описание
`TrustedPrograms.item_#.ApplyToDescendants=Yes`	Исключать дочерние процессы доверенного приложения из проверки компонентом Анализ поведения.
`MemScanExcludedProgramPath.item_#`	Путь к доверенному приложению с идентификатором `#`. Приложение не будет проверять память процессов доверенного приложения.

Как добавить доверенные устройства

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.

Вы можете добавить доверенные устройства по следующим данным:

- **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.

- **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. Символ `?` заменяет один произвольный символ. Например, `WDC_C*`.

Как добавить доверенные устройства в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль устройств** → **Доверенные устройства**.

   Откроется окно со списком доверенных устройств.

5. Нажмите на кнопку **Добавить**.

   Откроется форма добавления устройства

6. В блоке **Пользователь или группа** укажите пользователя или группу пользователей, для которых устройство будет считаться доверенным.

   Вы можете выбрать пользователей из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   По умолчанию доступ к доверенным устройствам разрешен для группы "Все".

7. В блоке **Тип устройства** выберите тип устройства из раскрывающегося списка (например, **Съемные диски**).

8. Если вы хотите добавить устройство по маске идентификатора, установите флажок **Использовать маску**.

9. В поле **Поиск доверенных устройств** введите идентификатор или маску идентификатора устройства.

   В таблице отобразится список устройств, которые удовлетворяют заданным параметрам.

10. Установите флажки напротив названий устройств, которые вы хотите добавить в список доверенных.

11. Если необходимо, введите описание причины добавления устройств в список доверенных на вкладке **Комментарий**.

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

Как добавить доверенные устройства в командной строке

1. Для добавления доверенного устройства выполните команду:

```
kesl-control --trusted-devices --add <device ID>
```

2. Для проверки списка доверенных устройств компонента выполните команду:

```
kesl-control --trusted-devices --list
```

Пример

```
kesl-control --trusted-devices --add WDC_C*
```

Общие настройки

Настройки обнаружения

Обнаружение других типов объектов

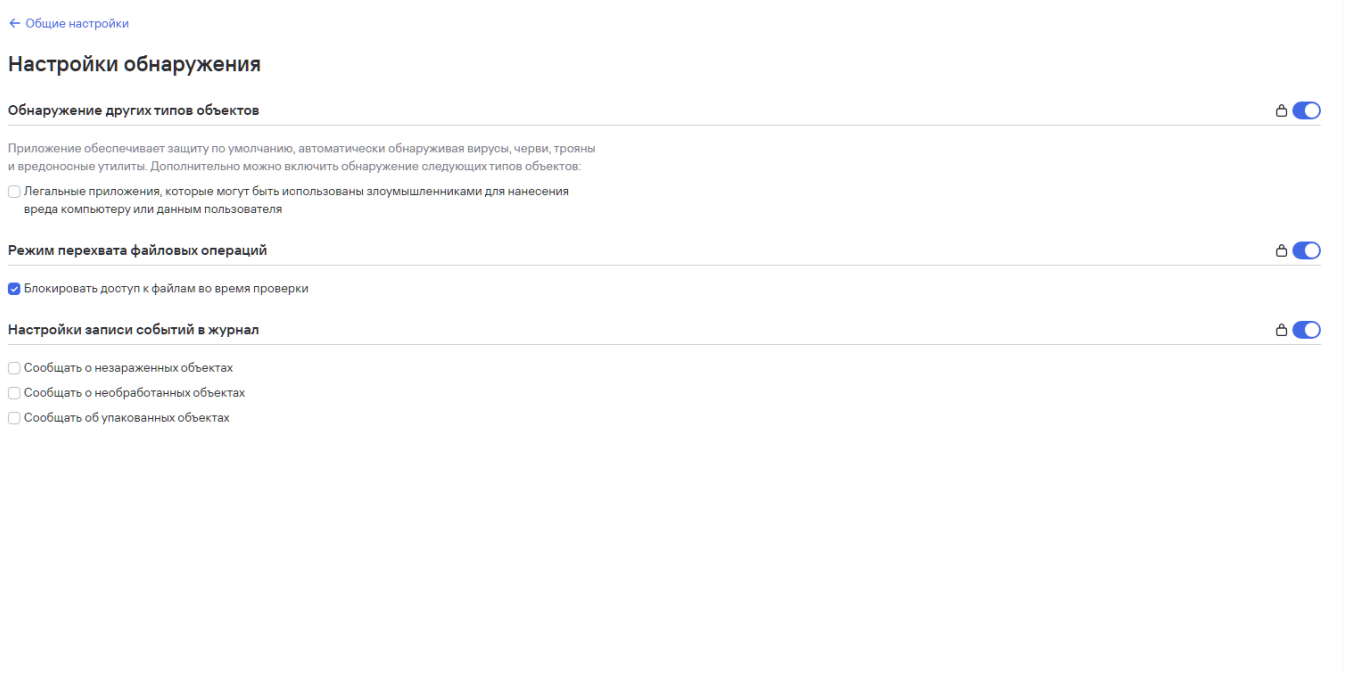
Вне зависимости от настроенных параметров приложения Kaspersky Endpoint Security всегда обнаруживает и блокирует вирусы, черви и троянские приложения. Эти приложения могут нанести значительный вред компьютеру.

Дополнительно можно включить обнаружение легальных приложений, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие приложения не имеют вредоносных функций, но могут быть использованы злоумышленниками. Подробную информацию о легальных приложениях, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского".

Как настроить обнаружение приложений, которые злоумышленники могут использовать для нанесения вреда, в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в **Общие настройки** → **Настройки обнаружения**.
5. В блоке **Обнаружение других типов объектов** установите флажок **Легальные приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя**.
6. Сохраните изменения.



Настройки обнаружения

Как настроить обнаружение приложений, которые злоумышленники могут использовать для нанесения вреда, в командной строке

1. Для настройки обнаружения приложений, которые злоумышленники могут использовать для нанесения вреда, для компонентов защиты приложения выполните команду:

```
kesl-control --set-app-settings DetectOtherObjects=<Yes|No>
```

2. Для проверки ссылок по базе веб-адресов, содержащих легальные приложения, которые злоумышленники могут использовать для нанесения вреда, в компоненте Защита от веб-угроз выполните команду:

```
kesl-control --set-settings 14 CheckOther=<Yes|No>
```

3. Для проверки текущих настроек приложения выполните команду:

```
kesl-control --get-app-settings
```

4. Для проверки текущих настроек Защиты от веб-угроз выполните команду:

```
kesl-control --get-settings 14
```

Настройки записи событий в журнал

По умолчанию приложение Kaspersky Endpoint Security не записывает в журнал события об обработке упакованных и незараженных объектов, а также события о необработанных объектах компонентом Защита от файловых угроз.

Вы можете включить запись таких событий, и приложение будет формировать события *Обнаружен упакованный объект*, *Объект не обработан*, *Объект обработан*. Такие события могут быть полезны при настройке компонента, а также при отладке или диагностике приложения. Это позволит убедиться, что объекты были проверены приложением, а не пропущены из-за ошибок.

Как включить запись событий об обработке объектов в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в **Общие настройки** → **Настройки обнаружения**.
5. В блоке **Настройки записи событий в журнал** установите флажки напротив нужных типов событий:
   - **Сообщать о незараженных объектах**
   - **Сообщать о необработанных объектах**
   - **Сообщать об упакованных объектах**
6. Сохраните изменения.

Как включить запись событий об обработке объектов в командной строке

1. Для записи в журнал событий о незараженных объектах выполните команду:

```
kesl-control --set-settings 1 ReportCleanObjects=Yes
```

2. Для записи в журнал событий о необработанных объектах выполните команду:

```
kesl-control --set-settings 1 ReportUnprocessedObjects=Yes
```

3. Для записи в журнал событий об упакованных объектах выполните команду:

```
kesl-control --set-settings 1 ReportPackedObjects=Yes
```

4. Для проверки текущих значений параметров Защиты от файловых угроз выполните команду:

```
kesl-control --get-settings 1
```

Kaspersky Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть Kaspersky Security Network.

Функциональность KSN может быть недоступна в приложении на территории США.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, приложение Kaspersky Endpoint Security получает от служб KSN сведения о репутации проверяемых веб-адресов, а также сведения о категории и репутации проверяемых файлов. Подробнее о настройке доступа к KSN см. в справке Kaspersky Security Center.

Использование Kaspersky Security Network является добровольным. Приложение предлагает использовать KSN во время первоначальной настройки приложения. Начать или прекратить использование KSN можно в любой момент.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского". Файл ksn_license.<language ID> с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения и доступен в директории /opt/kaspersky/kesl/doc/.

Инфраструктура репутационных баз "Лаборатории Касперского"

Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения для работы с репутационными базами "Лаборатории Касперского":

- *Kaspersky Security Network (KSN)* – это решение, которое используют большинство приложений "Лаборатории Касперского". Участники KSN получают информацию от "Лаборатории Касперского", а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.

- *Kaspersky Private Security Network (KPSN)* – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров. KPSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

  - отсутствие подключения локальных рабочих мест к сети Интернет;

  - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

После активации приложения по новой лицензии для использования KPSN требуется предоставить поставщику услуг информацию о новом лицензионном ключе. В противном случае обмен информацией с KPSN будет невозможен из-за ошибки аутентификации.

Ограничения работы с Kaspersky Private Security Network

Kaspersky Private Security Network позволяет использовать собственную базу данных репутаций объектов (файлов или веб-адресов) с помощью локальной репутационной базы. Репутация объекта, добавленного в локальную репутационную базу, имеет приоритет выше, чем в KSN / KPSN. То есть, если Kaspersky Endpoint Security при проверке компьютера запросит репутацию файла в KSN / KPSN, и в локальной репутационной базе файл имеет репутацию *Недоверенные*, а в KSN / KPSN объект имеет репутацию *Доверенные*, то Kaspersky Endpoint Security обнаружит файл как *Недоверенные* и выполнит действие, заданное для обнаруженных угроз.

Однако в некоторых случаях Kaspersky Endpoint Security может не запрашивать репутацию объекта в KSN / KPSN. В результате Kaspersky Endpoint Security не получит данные из локальной репутационной базы KPSN. Kaspersky Endpoint Security может не запрашивать репутацию объекта в KSN / KPSN, например, по следующим причинам:

- Приложения "Лаборатории Касперского" используют офлайн репутационные базы. Офлайн репутационные базы предназначены для оптимизации ресурсов при работе приложений "Лаборатории Касперского" и защите критически важных объектов компьютера. Офлайн репутационные базы формируют специалисты "Лаборатории Касперского" на основании данных Kaspersky Security Network. приложения "Лаборатории Касперского" обновляют офлайн репутационные базы с антивирусными базами приложения. Если информация о проверяемом объекте содержится в офлайн репутационных базах, приложение не запрашивает репутацию этого объекта в KSN / KPSN.

- В параметрах приложения настроены исключения из проверки (доверенная зона). В этом случае приложение не учитывает репутацию объекта в локальной репутационной базе.

- Приложение использует технологии оптимизации проверки, например, технологию iChecker или кеширование запросов репутации в KSN / KPSN. В этом случае приложение может не запрашивать репутацию ранее проверенных объектов.

- Для оптимизации нагрузки приложение проверяет файлы определенного формата и размера. Список форматов и ограничения по размеру определяют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами приложения. Также вы можете настроить параметры оптимизации проверки в интерфейсе приложения, например, для компонента Защита от файловых угроз.

- Kaspersky Endpoint Security в режиме Легкого агента взаимодействует с серверами KSN с помощью прокси-сервера KSN. Взаимодействие с KSN напрямую не поддерживается.

Как включить или выключить использование Kaspersky Security Network

По умолчанию Kaspersky Endpoint Security использует расширенный режим KSN. *Расширенный режим KSN* – режим работы приложения, при котором Kaspersky Endpoint Security передает в "Лабораторию Касперского" дополнительные данные.

Сбор, обработка и хранение персональных данных пользователя не производится. 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 сайте "Лаборатории Касперского". Файл с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения.

Как включить или выключить использование KSN в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

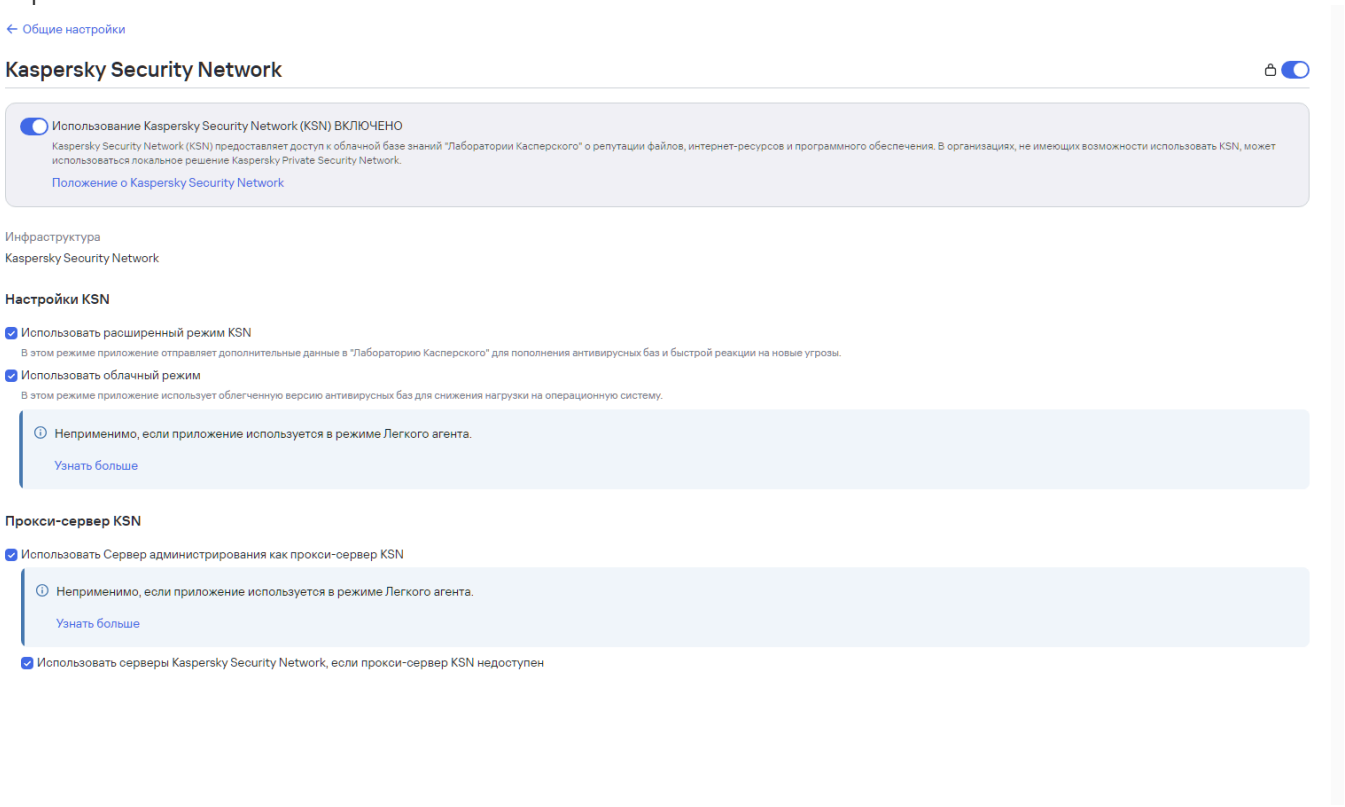
4. Перейдите в раздел **Общие настройки** → **Kaspersky Security Network**.

5. Используйте переключатель **Использование Kaspersky Security Network (KSN)**, чтобы включить или выключить компонент.

6. Если вы включили использование KSN, откроется окно **Положение о Kaspersky Security Network**. Если вы согласны, примите условия использования KSN.

7. Если требуется, установите или снимите флажок **Использовать расширенный режим KSN**.

8. Сохраните изменения.



Kaspersky Security Network

Как включить или выключить использование KSN в командной строке

1. Проверьте статус работы Kaspersky Security Network:

   ```
   kesl-control --app-info
   ```

   Приложение показывает статус работы KSN в строке **Использование Kaspersky Security Network**:

   - **Выключено**;
   - **Стандартный режим KSN**;
   - **Расширенный режим KSN**.

2. Для включения стандартного режима использования Kaspersky Security Network выполните следующую команду:

   ```
   kesl-control --set-app-settings UseKSN=Basic --accept-ksn
   ```

3. Для включения расширенного режима использования Kaspersky Security Network выполните следующую команду:

   ```
   kesl-control --set-app-settings UseKSN=Extended --accept-ksn
   ```

4. Для выключения использования Kaspersky Security Network выполните следующую команду:

```
kesl-control --set-app-settings UseKSN=No
```

Как включить или выключить использование KSN в интерфейсе приложения

1. Откройте главное окно приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Настройка**.
3. В открывшемся окне выберите один из следующих вариантов:
   - **Расширенный режим KSN**, если вы хотите использовать Kaspersky Security Network, получать информацию из базы знаний и отправлять анонимную статистику и данные о типах и источниках угроз.
   - **Стандартный режим KSN**, если вы хотите использовать Kaspersky Security Network, получать информацию из базы знаний, но не отправлять анонимную статистику и данные о типах и источниках угроз.
4. Нажмите на кнопку **Включить**.
5. В окне **Использование Kaspersky Security Network** внимательно прочитайте Положение о Kaspersky Security Network и выберите один их следующих вариантов:
   - **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**.
   - **Я не принимаю условия Положения о Kaspersky Security Network**.
6. Нажмите **OK**.

В результате, если использование KSN включено, Kaspersky Endpoint Security использует информацию о репутации файлов, веб-ресурсов и приложений, полученную из Kaspersky Security Network.

Приложение Kaspersky Endpoint Security использует следующие сетевые параметры для взаимодействия с внешними службами:

Адрес	Протокол	Порт
ds.kaspersky.com	HTTPS	443
ksn-a-stat-geo.kaspersky-labs.com	KSN	443, 1443
ksn-file-geo.kaspersky-labs.com	KSN	443, 1443
ksn-verdict-geo.kaspersky-labs.com	KSN	443, 1443
ksn-url-geo.kaspersky-labs.com	KSN	443, 1443
ksn-a-p2p-geo.kaspersky-labs.com	KSN	443, 1443
ksn-cinfo-geo.kaspersky-labs.com	KSN	443, 1443

Что такое облачный режим работы приложения

Облачный режим – режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию антивирусных баз, что позволяет снизить нагрузку на оперативную память компьютера примерно в два раза.

Облачный режим можно использовать только при включенном Kaspersky Security Network. Если вы не участвуете в Kaspersky Security Network или облачный режим выключен, Kaspersky Endpoint Security загружает полную версию антивирусных баз с серверов "Лаборатории Касперского". По умолчанию облачный режим включен.

> Если приложение работает в режиме Легкого агента, облачный режим недоступен.

Как включить или выключить облачный режим в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Kaspersky Security Network**.
5. Используйте переключатель **Использовать облачный режим**, чтобы включить или выключить компонент.
6. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Как включить или выключить облачный режим в командной строке

1. Выполните команду вывода общих параметров приложения, чтобы узнать текущий статус работы приложения:

   ```
   kesl-control --get-app-settings
   ```

   Приложение показывает статус работы приложения в строке `CloudMode`.
2. Для включения или выключения облачного режима выполните следующую команду:

   ```
   kesl-control --set-app-settings CloudMode=<Yes|No>
   ```

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.

Зачем нужен KSN Proxy

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN напрямую или при помощи службы KSN Proxy.

> Если приложение работает в режиме Легкого агента, взаимодействие с KSN напрямую не поддерживается. Kaspersky Endpoint Security взаимодействует с серверами KSN с помощью прокси-сервера KSN.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.
- Служба KSN Proxy кеширует обработанные данные, снижая тем самым нагрузку на канал связи с внешней сетью и ускоряя получение компьютером пользователя запрошенной информации.

По умолчанию после включения использования KSN и принятия Положения об использовании KSN приложение использует прокси-сервер для связи с Kaspersky Security Network. В качестве прокси-сервера приложение использует Сервер администрирования Kaspersky Security Center и TCP-порт 13111.

Вы можете настроить параметры прокси-сервера KSN в свойствах Сервера администрирования. Подробнее о прокси-сервере KSN см. в справке Kaspersky Security Center.

Настройка параметров подключения к прокси-серверу KSN с помощью командной строки недоступна.

Как настроить подключение к KSN через прокси-сервер в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Kaspersky Security Network**.
5. Используйте флажок **Использовать Сервер администрирования как прокси-сервер KSN**, чтобы включить или выключить использование KSN Proxy.
6. Если требуется, установите или снимите флажок **Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен**. По умолчанию флажок установлен.

   Если этот параметр включен, Kaspersky Endpoint Security использует серверы KSN напрямую, когда служба KSN Proxy недоступна. Этими серверами могут быть как расположенные в "Лаборатории Касперского", так и сторонние сервера, в случае использования Kaspersky Private Security Network.
7. Сохраните изменения.

Настройка отправки информации в хранилище Kaspersky Security Center

В Kaspersky Security Center вы можете включать и выключать отправку в хранилище Kaspersky Security Center информации о файлах в резервном хранилище, файлах на карантине, необработанных файлах и о подключенных устройствах.

Как посмотреть файлы, помещенные на карантин на клиентских устройствах

Общий список файлов, помещенных на карантин приложениями "Лаборатории Касперского" на клиентских устройствах, формируется в Kaspersky Security Center.

1. В главном окне Web Console выберите **Операции** → **Хранилища**.
2. Перейдите в папку **Карантин**.
3. Информация об объектах, помещенных на карантин, отобразится в правой панели консоли.

Как посмотреть файлы, помещенные в резервное хранилище на клиентских устройствах

Общий список файлов, помещенных в резервное хранилище приложениями "Лаборатории Касперского" на клиентских устройствах, формируется в Kaspersky Security Center.

1. В главном окне Web Console выберите **Операции** → **Хранилища**.
2. Перейдите в папку **Файлы резервных копий**.
3. Информация об объектах, помещенных в резервное хранилище, отобразится в правой панели консоли.

Как посмотреть информацию о необработанных файлах в списке активных угроз

1. В главном окне Web Console выберите **Операции** → **Хранилища**.
2. Перейдите в папку **Активные угрозы**.
3. Информация о необработанных файлах в списке активных угроз отобразится в правой панели консоли.

Как посмотреть информацию об оборудовании, подключенном к клиентским устройствам

1. В главном окне Web Console выберите **Операции** → **Хранилища**.
2. Перейдите в папку **Оборудование**.
3. Информация об устройствах отобразится в правой панели консоли.

Информация передается, если включен компонент Контроль устройств.

Как посмотреть информацию о приложениях на клиентских устройствах

1. В главном окне Web Console выберите **Операции** → **Сторонние приложения**.
2. Перейдите в папку **Реестр приложений**.
3. Информация о приложениях отобразится в правой панели консоли.

Информация передается, если включен компонент Контроль приложений.

Как настроить интеграцию с Сервером администрирования

Чтобы настроить интеграцию с Сервером администрирования в свойствах политики:

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

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

5. Нажмите на ссылку **Дополнительные настройки**.

6. Выберите категории событий на клиентских компьютерах, информация о которых должна передаваться на Сервер администрирования:

   - **О файлах карантина**. Флажок включает или выключает передачу на Сервер администрирования информации о файлах, помещенных на карантин.

   - **О файлах в резервном хранилище**. Флажок включает или выключает передачу на Сервер администрирования информации о файлах в резервном хранилище.

   - **О необработанных файлах**. Флажок включает или выключает отправку уведомлений о файлах, не обработанных во время проверки, на Сервер администрирования.

   - **Об установленных устройствах**. Флажок включает или выключает передачу на Сервер администрирования информации об устройствах, установленных на клиентском устройстве или подключенных к нему.

   - **О запускаемых приложениях**. Флажок включает или выключает передачу на Сервер администрирования списка приложений, обнаруженных на клиентском устройстве в результате работы задачи инвентаризации.

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

Чтобы настроить интеграцию с Сервером администрирования в свойствах управляемого устройства:

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)** → **Управляемые устройства**.

2. Нажмите на ссылку **<имя устройства>**.

3. Перейдите на вкладку **Приложения** и нажмите на ссылку **Kaspersky Endpoint Security**.

4. На вкладке **Параметры приложения** перейдите в раздел **Параметры хранилищ**.

5. В блоке **Параметры передачи данных на Сервер администрирования** нажмите на кнопку **Настроить**.

6. В окне **Параметры передачи данных** вы можете включать и выключать отправку информации на Сервер администрирования:

   - **Уведомлять о файлах резервного хранилища**. Флажок включает или выключает передачу на Сервер администрирования информации о файлах в резервном хранилище.

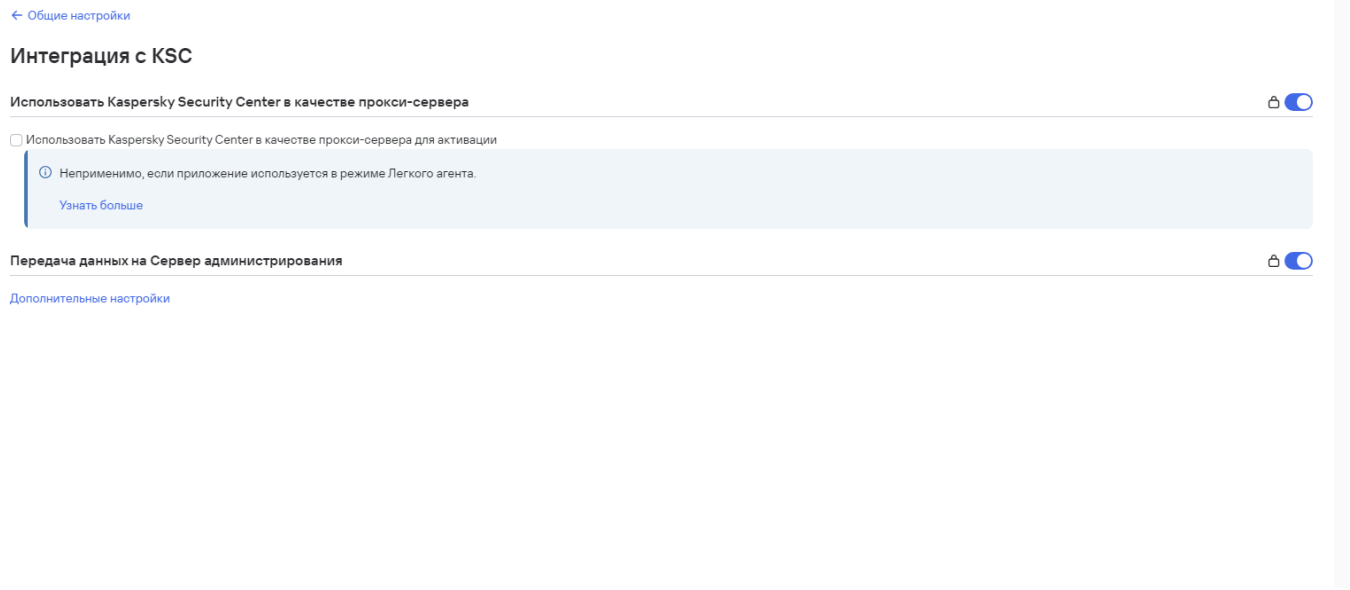
   - **Уведомлять о файлах карантина**. Флажок включает или выключает передачу на Сервер администрирования информации о файлах, помещенных на карантин.

- **Уведомлять о необработанных файлах**. Флажок включает или выключает отправку уведомлений о файлах, не обработанных во время проверки, на Сервер администрирования.

- **Уведомлять об установленных устройствах**. Флажок включает или выключает передачу на Сервер администрирования информации об устройствах, установленных на клиентском устройстве или подключенных к нему.

- **Уведомлять о приложениях, обнаруженных на устройстве**. Флажок включает или выключает передачу на Сервер администрирования списка приложений, обнаруженных на клиентском устройстве в результате работы задачи инвентаризации.

7. Сохраните изменения.



Интеграция с Kaspersky Security Center

Как настроить запуск приложения

Настройка запуска приложения

Вы можете настраивать максимальное количество неудачных попыток запуска и максимальное время ожидания запуска приложения Kaspersky Endpoint Security. Это позволит снизить нагрузку на систему, если приложение не запускается длительное время. По умолчанию максимальное количество неудачных последовательных попыток запуска приложения – 5, максимальное время ожидания запуска приложения – 3 минуты.

Как настроить запуск приложения в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

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

5. В блоке **Настройки запуска приложения** укажите значения в следующих полях:

   - **Максимальное количество неудачных последовательных попыток запуска приложения**. Значение по умолчанию: 5.

   - **Максимальное время ожидания запуска приложения (мин.)**. Значение по умолчанию: 3.

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

Как настроить запуск приложения в командной строке

В командной строке вы можете настраивать параметры запуска приложения с помощью параметров `MaxRestartCount` и `StartupTimeout` в конфигурационном файле kesl.ini.

Параметр `MaxRestartCount` позволяет задать максимальное количество неудачных последовательных попыток запуска приложения. Параметр может принимать значения от 1 до 10. Значение по умолчанию: 5.

Параметр `StartupTimeout` позволяет задать максимальное время ожидания запуска приложения (в минутах), после которого процесс kesl будет перезапущен. Параметр может принимать значения от 1 до 60. Значение по умолчанию: 3.

Применение критических обновлений

Вы можете настраивать автоматический перезапуск приложения при получении критически важных обновлений по истечении первых суток после установки приложения. В первые 24 часа после установки приложение автоматически перезапускается при получении критически важных обновлений, без дополнительной настройки.

Как настроить автоматический перезапуск приложения в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

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

5. В блоке **Применение критических обновлений** установите флажок **Автоматически перезапускать приложение при получении критических обновлений**.

   Приложение Kaspersky Endpoint Security будет перезапущено при получении критически важных обновлений по истечении первых суток после установки приложения.

6. Сохраните изменения.

Как настроить автоматический перезапуск приложения в командной строке

В командной строке вы можете настраивать автоматический перезапуск приложения при получении критически важных обновлений с помощью параметра `UrgentUpdateRestartEnabled` в общих параметрах приложения.

Для автоматического перезапуска приложения при получении критически важных обновлений выполните команду:

```
kesl-control --set-app-settings UrgentUpdateRestartEnabled=Yes
```

Настройка разрешений на управление задачами

В Kaspersky Security Center вы можете настраивать следующие разрешения для пользователей:

- Разрешение на использование локальных задач, созданных в приложении Kaspersky Endpoint Security. Если политика Kaspersky Security Center запрещает пользователям просматривать, изменять, создавать и удалять локальные задачи, информация о задачах Scan_My_Computer, Critical_Areas_Scan, Container_Scan, Inventory_Scan, Update (в стандартном режиме) и Rollback (в стандартном режиме) недоступна.

- Разрешение на просмотр и управление на клиентских устройствах задачами, которые созданы в Kaspersky Security Center.

Чтобы настроить разрешения на управление задачами в Web Console:

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

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

5. В блоке **Разрешенные действия** выберите действия, разрешенные пользователям на их устройствах:

   - **Доступ к локальным задачам**. Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователи, при отсутствии дополнительных ограничений политики, могут настраивать, запускать, создавать и удалять доступные локальные задачи в графическом интерфейсе приложения и в командной строке.

   - **Управление групповыми задачами**. Если флажок установлен, пользователи могут управлять групповыми задачами, заданными в Kaspersky Security Center, на клиентских устройствах. Возможен запуск задач в графическом интерфейсе приложения и в командной строке.

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

Защита паролем

Защита паролем позволяет ограничить доступ пользователей к изменению Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на просмотр отчетов приложения). Ограничение доступа к настройкам приложения снижает риск несанкционированных или непреднамеренных изменений в приложении.

Как работает Защита паролем

1. **Пользователь пытается выполнить действие, контролируемое компонентом**

   Например, выключить компоненты защиты или просмотреть отчеты Kaspersky Endpoint Security.

2. **Kaspersky Endpoint Security проверяет права пользователя**

   Если у пользователя есть соответствующее разрешение, то действие успешно выполняется. Если у пользователя нет соответствующего разрешения, то приложение запрещает выполнение действия и показывает ошибку.

   В графическом интерфейсе Kaspersky Endpoint Security запрещенные действия недоступны для просмотра и редактирования.

Настройка Защиты паролем

1. **Включите Защиту паролем**

   По умолчанию Защита паролем выключена. Включите компонент в Web Console или в Консоли администрирования или в командной строке с помощью следующей команды:

   ```
   kesl-control --set-permission-manager-settings Enabled=Yes
   ```

2. **Настройте разрешения пользователей**

   По умолчанию в приложении настроены пользовательские разрешения для предустановленных групп пользователей *kesladmin*, *kesluser*, *keslaudit*.

   Настройте пользовательские разрешения для этих групп или создайте нового пользователя или группу пользователей.

   > Для корректной работы приложения рекомендуем настроить разрешения хотя бы для одной группы пользователей.

   Как настроить пользовательские разрешения в Web Console

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

      Откроется окно свойств политики.
   3. Выберите вкладку **Параметры приложения**.
   4. Перейдите в раздел **Общие настройки** → **Самозащита**.
   5. Убедитесь, что переключатель работы компонента находится в положении **Защита паролем ВКЛЮЧЕНА**.
   6. Нажмите на ссылку **Пользовательские разрешения**.

      Откроется окно с пользователями и их разрешениями.

7. Если вы хотите изменить разрешения для предустановленных групп пользователей, нажмите на название группы.

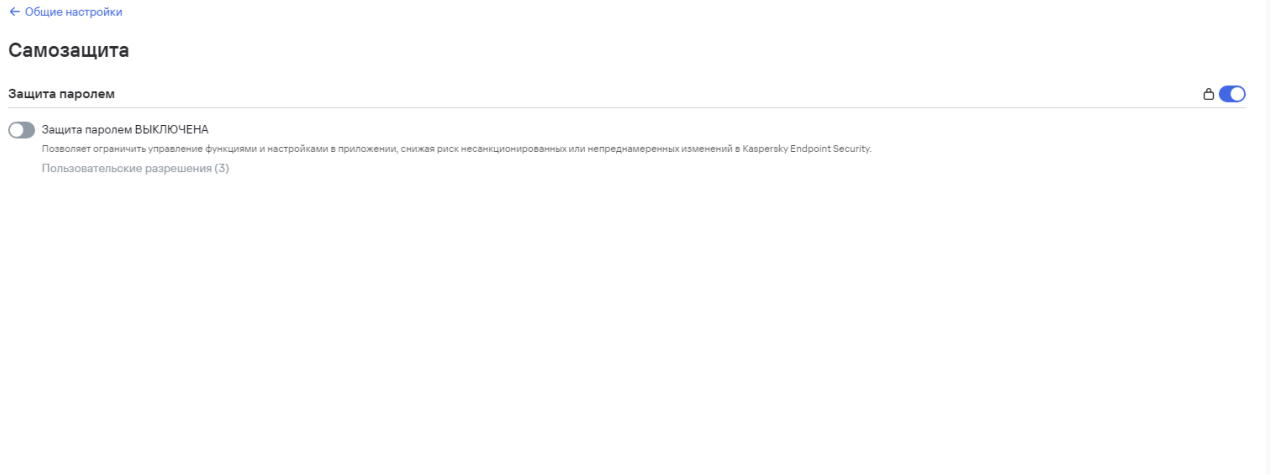
   Если вы хотите изменить разрешения для другого пользователя или группы пользователей:

   a. Нажмите на кнопку **Добавить**.

   b. Выберите пользователя / группу пользователей из Active Directory или задайте имя вручную.

8. Установите флажки напротив разрешений, которые будут доступны пользователю или группе.

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



Самозащита

Как настроить пользовательские разрешения в командной строке

1. Для просмотра списка текущих настроек Защиты паролем выполните команду:

```
kesl-control --get-permission-manager-settings
```

2. Для изменения разрешений пользователя или группы пользователей выполните команду:

```
kesl-control --set-permissions <principal> [--group] <permissions>=<Yes|No> [--file <file name>] [--
json]
```

3. Для удаления пользователя или группы пользователей, для которых настроены разрешения, выполните команду:

```
kesl-control --remove-permissions <principal> [--group]
```

Условные обозначения

Параметры команды

Параметр	Описание
`--group`	Параметр применяется к группе пользователей. Если ключ `--group` не указан, параметр применяется к отдельному пользователю.
`--file <file name>`	Вывод параметров в файл или импорт параметров из файла. Укажите имя файла вместо `<file name>`.
`--json`	Вывод параметров в JSON-файл или импорт параметров из JSON-файла. Этот параметр можно указать, только если указан параметр `--file <file name>`.

Параметр	Описание
`principal`	Имя пользователя или группы пользователей.
`permissions`	Пользовательские разрешения. Укажите значение `Yes`, чтобы разрешить пользователю выполнять действие, или `No`, чтобы запретить. • `StopProtection`. Выключение компонентов защиты. • `StopSecurityControl`. Выключение компонентов контроля. • `StartProtection`. Включение компонентов защиты • `StartSecurityControl`. Включение компонентов контроля. • `ApplicationSettings`. Настройка приложения. • `ViewReports`. Просмотр отчетов. • `RestoreFromBackup`. Восстановление из резервного хранилища. • `RemoveLicenseKey`. Удаление ключа. • `AddLicense`. Добавление ключа. • `DisablePolicy`. Выключение политики Kaspersky Security Center.

Примеры

Отозвать у группы пользователей *kesluser* разрешение на просмотр отчетов:

```
kesl-control --set-permissions kesluser --group ViewReports=No
```

Разрешить пользователю *new-user* управлять компонентами контроля:

```
kesl-control --set-permissions new-user startSecurityControl=Yes StopSecurityControl=Yes
```

Особенности работы Защиты паролем

- Если Защита паролем выключена, разрешения пользователей на управление приложением определяется ролями пользователей.
- Если для пользователя одновременно заданы разрешения группы и разрешения для отдельного пользователя, приоритет отдается индивидуальным разрешениям. Для пользователя применятся индивидуальные разрешения, даже если они ограничивают доступ сильнее, чем разрешения для группы.

  Например, если группе *kesluser* запрещена настройка приложения, вы можете разрешить настройку приложения отдельному пользователю, входящему в эту группу. Такой пользователь сможет настраивать приложение.
- Если Защита паролем включена и для пользователя не заданы разрешения группы и разрешения для отдельного пользователя, все действия запрещены.

О пользовательских разрешениях

Если Защита паролем включена, вы управляете доступом пользователей на управление Kaspersky Endpoint Security с помощью *пользовательских разрешений*. Пользовательские разрешения определяют права пользователя (см. таблицу ниже).

Разрешение	Права
Настройка приложения	Просмотр и изменение параметров приложения. Управление параметрами задач через графический интерфейс и командную строку приложения без использования команды `sudo`. Назначение ролей пользователям. Отзыв ролей у пользователей (администратор не имеет права отозвать роль admin у себя самого). Управление задачей *Откат обновления баз (Rollback)*. Управление компонентами: • Managed Detection and Response • Endpoint Detection and Response Optimum
Включение компонентов защиты	Управление компонентами: • Защита от файловых угроз • Проверка съемных дисков • Анализ поведения • Защита от шифрования • Защита от атак BadUSB • Защита от почтовых угроз • Защита от веб-угроз • Защита от сетевых угроз • Управление сетевым экраном • Контроль целостности системы • Запрет запуска объектов (EDR Optimum) (*EDRO_Prevention*) • Endpoint Detection and Response Expert (on-premises) • Endpoint Detection and Response Expert (cloud) • Network Detection and Response (KATA) • Sandbox • Интеграция с KUMA
Выключение компонентов защиты	
Включение компонентов контроля	Управление компонентами: • Контроль устройств • Контроль приложений • Веб-Контроль
Выключение компонентов контроля	
Просмотр отчетов	Просмотр отчетов задач. Просмотр событий.
Восстановление из резервного хранилища	Просмотр и управление хранилищами пользователей.
Удаление ключа	Управление лицензированием приложения.
Добавление ключа	
Выключение политики Kaspersky Security Center	Выключение или включение политики Kaspersky Security Center на устройстве.

Особенности пользовательских разрешений

- Пользовательские разрешения не влияют на просмотр списка задач, просмотр объектов в резервном хранилище, просмотр параметров и статуса приложения.

  Всем пользователям разрешено управление следующими задачами:

  - Задачи проверки (*Выборочная проверка*, *Проверка контейнеров*, *Выборочная проверка контейнеров*, *Проверка важных областей*, *Поиск вредоносного ПО*);
  - *Инвентаризация*,
  - *Обновление баз и модулей приложения*,

- *Проверка целостности системы*,
- *Поиск IOC*.

- В графическом интерфейсе недоступно добавление и удаление основного лицензионного ключа, если устройство управляется политикой Kaspersky Security Center. Пользователь с разрешениями *Добавление ключа* и *Удаление ключа* может добавить резервный ключ или лицензионный ключ для активации других решений "Лаборатории Касперского" (add-on).

  Если устройство не находится под управлением политики, пользователю доступны и удаление, и добавление основного лицензионного ключа.

Пользовательские разрешения по умолчанию

По умолчанию в приложении настроены пользовательские разрешения для предустановленных групп пользователей *kesladmin*, *kesluser*, *keslaudit*. Пользователям, не входящим в эти группы, запрещены все операции с приложением.

Пользовательские разрешения предустановленных групп пользователей

Разрешение	kesladmin	kesluser	keslaudit
Настройка приложения	✓	–	–
Включение компонентов защиты	✓	–	–
Выключение компонентов защиты	✓	–	–
Включение компонентов контроля	✓	–	–
Выключение компонентов контроля	✓	–	–
Просмотр отчетов	✓	–	✓
Восстановление из резервного хранилища	✓	–	–
Удаление ключа	✓	–	–
Добавление ключа	✓	–	–
Выключение политики Kaspersky Security Center	✓	–	–

Настройки производительности

Проверка компьютера с помощью приложения Kaspersky Endpoint Security может потребовать значительных системных ресурсов. Чтобы оптимизировать нагрузку на систему, вы можете:

- Откладывать или пропускать задачи по расписанию при работе от аккумулятора
- Ограничить использование ресурсов процессора для задач проверки
- Ограничить использование резидентной памяти приложением
- Исключить память некоторых процессов из проверки

Откладывать или пропускать задачи по расписанию при работе от аккумулятора

Если ваше устройство работает от аккумулятора и вы хотите снизить потребление ресурсов приложением Kaspersky Endpoint Security, вы можете отменить запуск запланированных задач:

- всех задач проверки (выборочная проверка, проверка контейнеров, выборочная проверка контейнеров, проверка важных областей, *Поиск вредоносного ПО*)
- *Инвентаризация*
- *Обновление баз и модулей приложения*
- *Проверка целостности приложения*
- *Поиск IOC*

Вы можете запускать нужные задачи вручную.

Как отменить запуск запланированных задач при работе от аккумулятора в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Производительность**.
5. Включите функцию **Откладывать или пропускать задачи по расписанию при работе от аккумулятора**.

   Приложение Kaspersky Endpoint Security *отменяет* выполнение задач, для которых задан запуск по расписанию.
6. Сохраните изменения.

Как отменить запуск запланированных задач при работе от аккумулятора в командной строке

В командной строке вы можете настраивать отмену запуска запланированных задач с помощью параметра `PowerSaveMode` в общих параметрах приложения.

Для отмены запуска задач по расписанию на устройстве, работающем от аккумулятора, выполните команду:

```
kesl-control --set-app-settings PowerSaveMode=Yes
```

Ограничить использование ресурсов процессора для задач проверки

Вы можете ограничить использование памяти и ресурсов процессора для задач проверки *Поиск вредоносного ПО*, *Проверка важных областей*, *Инвентаризация* и *Проверка контейнеров* (типа ODS, ContainerScan и InventoryScan). По умолчанию установлено ограничение на использование памяти в 8192 МБ. Для ресурсов процессора ограничение не установлено.

Рекомендуется указывать ограничение на использование памяти для задач проверки ниже ограничения на использование резидентной памяти, чтобы задачи проверки не занимали всю доступную оперативную память и не вызывали перезапуск приложения.

Обратите внимание, что ресурс всех ядер процессора суммарно принимается за 100%.

Утилита `top` выводит загрузку процессора, считая, что ресурс одного ядра равен 100%. Таким образом, значение 400% для процессора при наличии 10 ядер (суммарно 1000% в измерении утилиты `top`) означает, что весь процессор (все ядра в сумме) используется на 40%. Для того, чтобы значение в выводе утилиты `top` не превышало 150% на тех же 10 ядрах, установите ограничение на использование ресурсов процессора `15%`.

Ограничение на использование ресурсов процессора используется для задач *Поиск вредоносного ПО*, *Проверка важных областей*, *Инвентаризация* и *Проверка контейнеров*, поэтому загрузка процессора при ограничении может превышать желаемое значение.

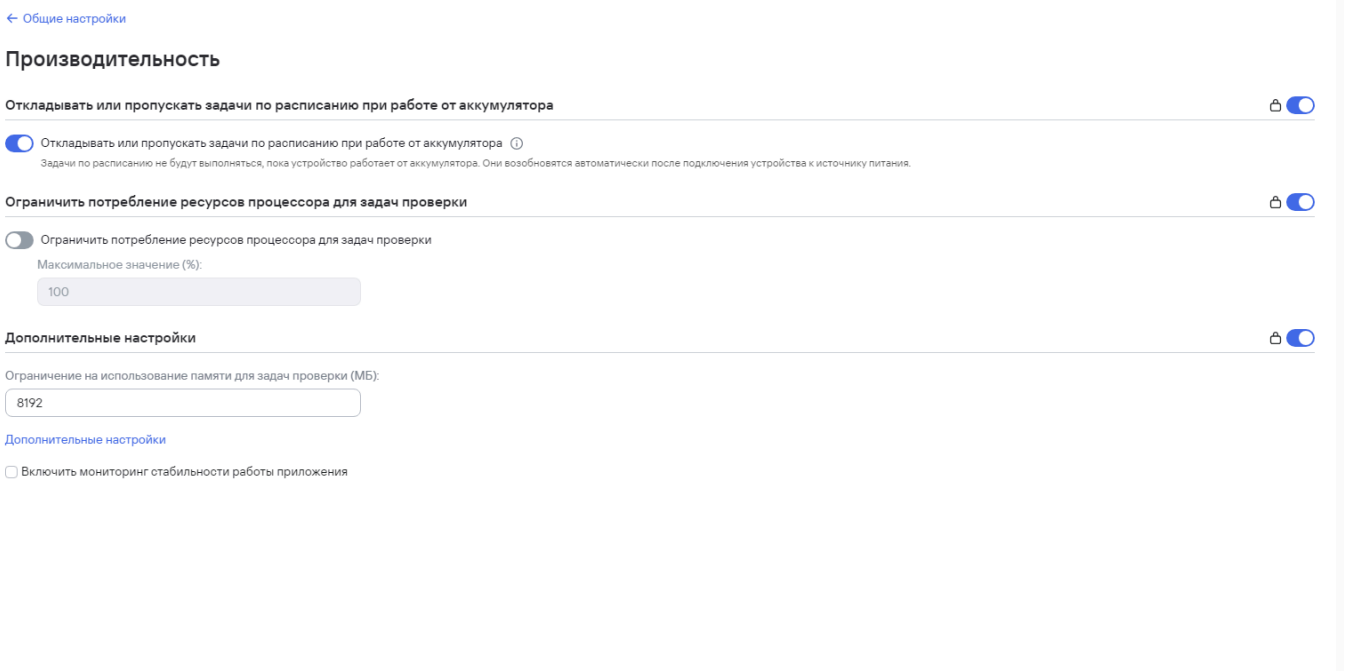
Ограничение на использование ресурсов процессора не работает на устройствах с операционными системами CentOS 5.2 и 5.4.

Как ограничить использование памяти и ресурсов процессора в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Производительность**.
5. Включите функцию **Ограничить потребление ресурсов процессора для задач проверки**.
6. Укажите максимальную нагрузку на все ядра процессора в поле **Максимальное значение (%)**. Значение должно быть целым числом и находиться в пределах от 10 до 100.
7. В блоке **Дополнительные настройки** укажите ограничение на использование памяти для задач проверки (МБ) в соответствующем поле ввода. Значение по умолчанию: 8192.

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



Производительность

Как ограничить использование памяти и ресурсов процессора в командной строке

В командной строке вы можете настраивать ограничение на использование ресурсов процессора для задач проверки с помощью параметров `UseOnDemandCPULimit` и `OnDemandCPULimit` в общих параметрах приложения.

1. Включите ограничение потребления ресурсов процессора для задач проверки, выполнив команду:

```
kesl-control --set-app-settings UseOnDemandCPULimit = Yes
```

2. Укажите ограничение потребления ресурсов процессора, выполнив команду:

```
kesl-control --set-app-settings OnDemandCPULimit =<value>
```

   Ограничение указывается в процентах, возможны целочисленные значения от 10 до 100.

3. Укажите ограничение на использование памяти для задач проверки с помощью параметра `ScanMemoryLimit` в конфигурационном файле kesl.ini.

Ограничить использование резидентной памяти приложением

Вы можете ограничить использование резидентной памяти приложением. По умолчанию установлено ограничение до 50% памяти, но не менее 2 ГБ и не более 16 ГБ.

Как ограничить использование резидентной памяти в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки** → **Производительность**.

5. В блоке **Дополнительные настройки** нажмите на ссылку **Дополнительные настройки** и в открывшемся окне установите флажок **Ограничить использование памяти приложением**.

   В раскрывающемся списке вы можете выбрать способ ограничения на использование резидентной памяти:

   - **Задать точное значение (%)**. При выборе этого элемента списка становится доступно поле **Точное значение (%)**, в котором вы можете указать нужное значение в процентах. Значение по умолчанию - 50%.

   - **Задать точное значение (МБ)**. При выборе этого элемента списка становится доступно поле **Точное значение (МБ)**, в котором вы можете указать нужное значение в мегабайтах. Значение по умолчанию - 2000 МБ.

   - **Использовать большее из двух значений (% или МБ)**. При выборе этого элемента списка становятся доступны поля **Точное значение (%)** и **Точное значение (МБ)**, в которых вы можете указать нужные значения.

   - **Использовать меньшее из двух значений (% или МБ)**. При выборе этого элемента списка становятся доступны поля **Точное значение (%)** и **Точное значение (МБ)**, в которых вы можете указать нужные значения.

   - **Ограничивать автоматически (рекомендуется)**. При выборе этого элемента списка использование резидентной памяти ограничивается автоматически (значение по умолчанию).

6. Сохраните изменения.

Чтобы измененные настройки вступили в силу, после применения политики на управляемом устройстве перезапустите приложение Kaspersky Endpoint Security.

Как ограничить использование резидентной памяти в командной строке

Настроить параметр `MaxMemory` в командной строке невозможно. Воспользуйтесь конфигурационным файлом kesl.ini, чтобы настроить ограничение на использование резидентной памяти приложением.

Рекомендуется изменять значение этого параметра только под руководством специалистов Службы технической поддержки по полученным от них инструкциям.

Параметр `MaxMemory` может принимать следующие значения:

- `off` – использование резидентной памяти не ограничено.

- `<value>%` – значение от 1 до 100 в процентах от объема памяти.

- `<value>MB` – значение в мегабайтах.

- `lowest/<value>%/<value>MB` – наименьшее значение между значением в процентах и значением в мегабайтах.

- highest/<value>%/<value>MB – наибольшее значение между значением в процентах и значением в мегабайтах.
- auto (значение по умолчанию) – автоматическое ограничение.

Исключение памяти процессов из проверки

Вы можете исключить из проверки память выбранных вами процессов.

Как исключить из проверки память процессов в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Производительность**.
5. В блоке **Дополнительные настройки** нажмите на ссылку **Настроить исключение памяти процессов из проверки**.
6. В открывшемся окне нажмите на кнопку **Добавить** и укажите путь к нужному процессу.

   Требования к пути:
7. Должен начинаться с символа `/` (абсолютный путь)

   a. Не должен содержать недопустимых символов:

   - `\0` (нулевой байт): запрещен операционной системой;
   - слеш (`/`) внутри имени файла или директории: используется как разделитель.
8. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Как исключить из проверки память процессов в командной строке

В командной строке вы можете настраивать исключение памяти процессов из проверки с помощью параметра `MemScanExcludedProgramPath.item_#` в общих параметрах приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `MemScanExcludedProgramPath.item_#` содержит полный путь к процессу в локальной директории. Для указания пути вы можете использовать маски.

Вы можете указать несколько процессов, память которых требуется исключить из проверки.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Оптимизация потребления ресурсов приложением

Настройки сети

Вы можете настроить параметры прокси-сервера для подключения к интернету, выбрать режим контроля сетевых портов и настроить проверку защищенных соединений.

Как настроить использование прокси-сервера

Вы можете настроить параметры прокси-сервера, если доступ пользователей с клиентских устройств в интернет осуществляется через прокси-сервер. Приложение Kaspersky Endpoint Security может использовать прокси-сервер для подключения к серверам активации "Лаборатории Касперского", к источникам обновлений баз и модулей приложения, к Kaspersky Security Network и при проверке сертификатов сайтов компонентом Защита от веб-угроз.

По умолчанию использование прокси-сервера выключено.

Если вы активируете устройства, которые находятся в изолированном сегменте сети без доступа в интернет, с помощью кода активации, вы можете использовать Сервер администрирования Kaspersky Security Center в качестве прокси-сервера для доступа к серверам активации "Лаборатории Касперского".

Как настроить использование Kaspersky Security Center в качестве прокси-сервера для активации приложения в Web Console

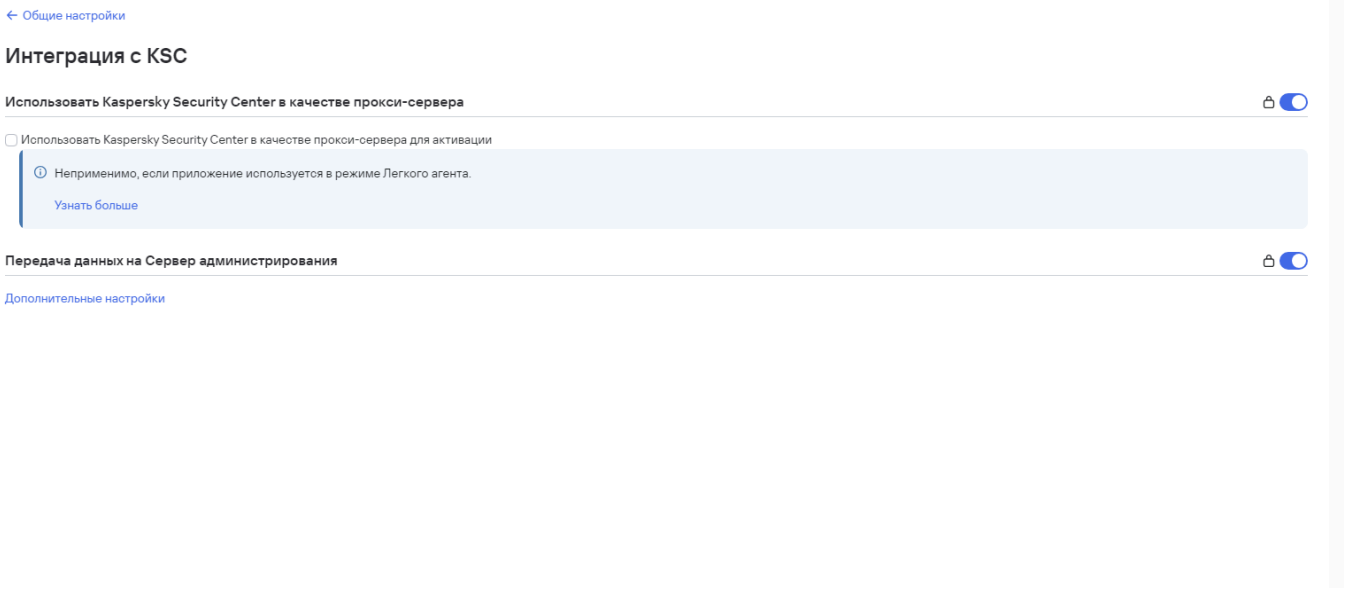
1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.

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

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

6. Нажмите на кнопку **Сохранить**.



Интеграция с Kaspersky Security Center

Если Kaspersky Endpoint Security используется в режиме Легкого агента, не поддерживается использование прокси-сервера для подключения к Kaspersky Security Network, к SVM и к Серверу интеграции. Также в режиме Легкого агента не поддерживается использование Сервера администрирования в качестве прокси-сервера для доступа к серверам активации "Лаборатории Касперского".

Как настроить использование прокси-сервера в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

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

5. Переведите переключатель в положение **Использование прокси-сервера ВКЛЮЧЕНО**.

6. В открывшемся окне заполните поля:

   - **Адрес прокси-сервера**.

   - **Порт прокси-сервера**.

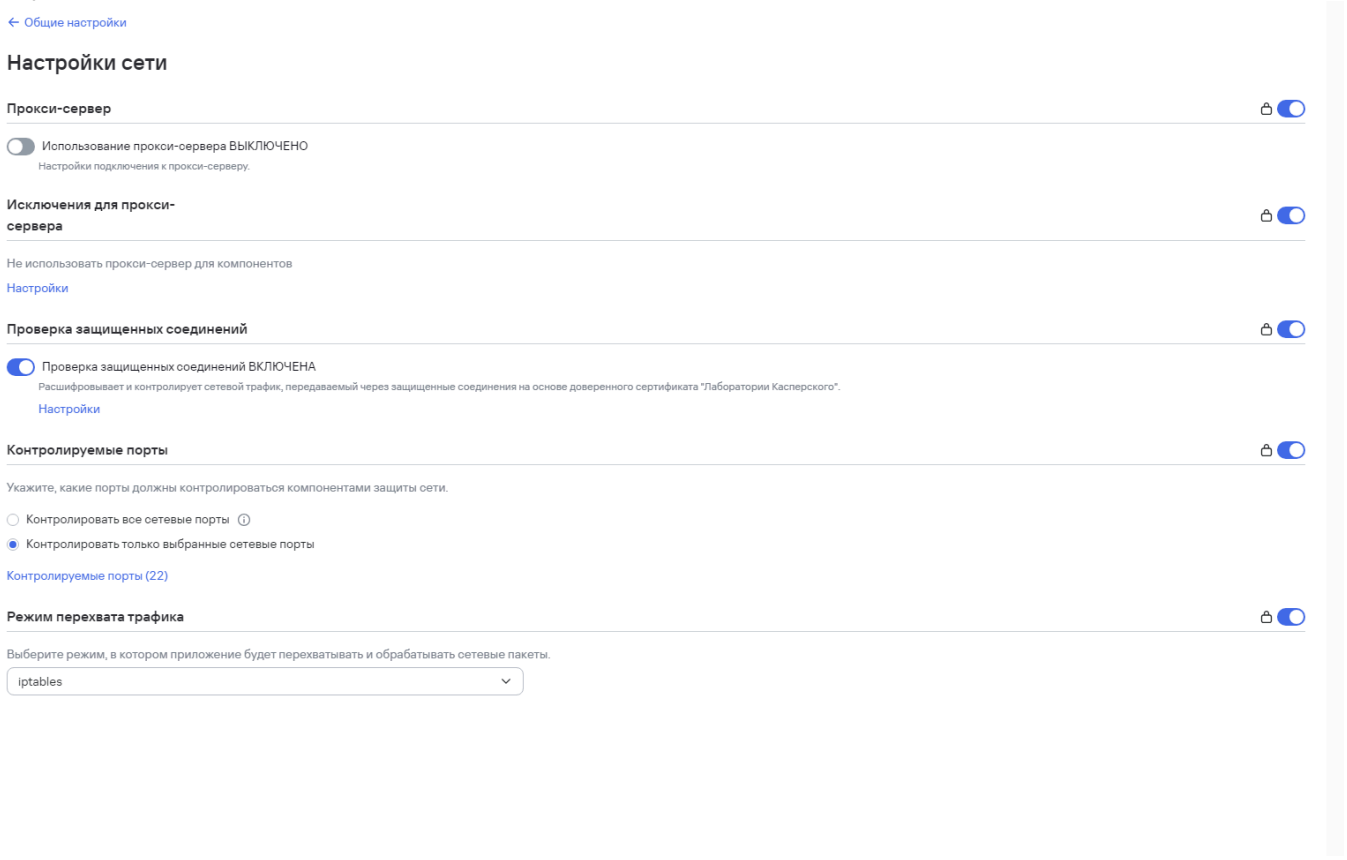
7. Если необходимо, включите аутентификацию на прокси-сервере:

   a. Установите флажок **Использовать аутентификацию на прокси-сервере**.

   b. Заполните поля:

   - **Имя пользователя**.
   - **Пароль**.

8. Сохраните внесенные изменения.



Настройки сети

Как настроить использование прокси-сервера в командной строке

1. Для включения использования прокси-сервера выполните команду:

```
kesl-control --set-net-settings UseProxy=Yes ProxyServer=<proxy server address>
```

2. Для проверки текущих значений параметров сети выполните команду:

```
kesl-control --get-net-settings
```

Условные обозначения

Параметры команды

Параметр	Описание
`ProxyServer`	Адрес прокси-сервера, используемого для подключения к интернету. Адрес прокси-сервера в одном из следующих форматов: • `[<connection protocol>://]<address of the proxy server>:<port>`, если для подключения к прокси-серверу не требуется аутентификация; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, если для подключения к прокси-серверу требуется аутентификация. Если вы указываете IP-адрес в формате IPv6, то вводите адрес в квадратных скобках. Подключение к прокси-серверу по протоколу HTTPS не поддерживается. Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.

Исключения прокси-сервера

Если для соединения с некоторыми адресами использовать прокси-сервер не требуется, вы можете добавить такие адреса в исключения.

Также вы можете отключить использование прокси-сервера для компонентов EDR Expert (on-premises), NDR (KATA) и Sandbox, которые обеспечивают интеграцию с решениями Detection and Response. При подключении к серверам взаимодействия с этими компонентами прокси-сервер не будет использоваться.

Как настроить исключения прокси-сервера в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки сети**.
5. В блоке **Исключения для прокси-сервера** нажмите на ссылку **Настройки**.

   Откроется окно исключений для прокси-сервера.
6. Установите флажки напротив компонентов, для которых не требуется использовать прокси-сервер:
   - **Endpoint Detection and Response Expert (on-premises)oint Detection and Response Expert (on-premises)**.
   - **KATA Sandbox**.
   - **Network Detection and Response (KATA)**.

7. Добавьте IP-адреса, для которых не требуется использовать прокси-сервер. Пример: `1.2.3.4/24`, `1234::cdef/96`.

8. Сохраните внесенные изменения.

Как настроить исключения прокси-сервера в командной строке

1. Для добавления адресов, для которых не нужно использовать прокси-сервер, выполните команду:

```
kesl-control --set-net-settings ProxyBypass=<address:port>
```

2. Для исключения использования прокси-сервера при интеграции с решениями Detection and Response от "Лаборатории Касперского" выполните команду:

```
kesl-control --set-net-settings [ProxyBypassEdr=<Yes|No>] [ProxyBypassNdr=<Yes|No>] [ProxyBypassSandbox=
<Yes|No>]
```

3. Для проверки текущих значений параметров сети выполните команду:

```
kesl-control --get-net-settings
```

Условные обозначения

Параметры команды

Параметр	Описание
`ProxyBypass`	Список адресов, для подключения к которым прокси-сервер не используется. Адрес задается в формате `<address>[:<port>]`. Для указания адресов вы можете использовать маски (символ `*`) и комментарии после символа `\`.
`ProxyBypassEdr`	Использование прокси-сервера при подключении к серверам, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises). По умолчанию использование прокси-сервера выключено (`No`).
`ProxyBypassNdr`	Использование прокси-сервера при подключении к серверам, обеспечивающим интеграцию с Kaspersky Network Detection and Response (KATA). По умолчанию использование прокси-сервера выключено (`No`).
`ProxyBypassSandbox`	Использование прокси-сервера при подключении к серверам, обеспечивающим взаимодействие с Sandbox. По умолчанию использование прокси-сервера выключено (`No`).

Как приложение перехватывает трафик

Приложение может использовать в своей работе один из двух режимов перехвата сетевого трафика: eBPF или iptables. Режим iptables выбран по умолчанию.

Параметр неприменим для устройств с процессором Эльбрус.

О перехвате сетевого трафика eBPF

В режиме eBPF приложение создает свое отдельное сетевое пространство имен (network linux namespace), куда перенаправляет сетевые пакеты с помощью eBPF-программ, привязанных к очередям `tc` (linux traffic control) локальных сетевых интерфейсов. Далее перенаправленный сетевой трафик проходит анализ в соответствии с активными сетевыми задачами и после этого возвращается на исходный сетевой интерфейс.

Для обмена данных между сетевыми пространствами имен используются пары виртуальных сетевых интерфейсов `veth` (каждый конец пары находится в своем сетевом пространстве имен):

- Пара `kesl_in - kesl_worm_in` передает сетевой трафик входящих соединений.
- Пара `kesl_out - kesl_worm_out` передает сетевой трафик исходящих соединений.

Через эти пары интерфейсов сетевой трафик передается на проверку из пространства имен по умолчанию в пространство имен, созданное приложением, и через них же возвращается обратно после анализа.

Сетевой трафик попадает на эти интерфейсы с других сетевых интерфейсов в системе, только если приложение запущено и включен сетевой перехват. Они не могут использоваться для передачи данных по сети между удаленными устройствами.

О перехвате сетевого трафика iptables

В режиме iptables перехват осуществляется с помощью механизма ядра tproxy.

В цепочке PREROUTING таблицы mangle создаются соответствующие правила, которые перенаправляют трафик на специальный порт, открытый приложением. Приложение также добавляет дополнительные правила в различные таблицы сетевого экрана операционной системы, предназначенные для перенаправления пакетов в tproxy. Сетевой перехватчик приложения встраивается между клиентом и сервером, устанавливая с каждым из них отдельное соединение, проверяет и передает трафик между ними.

Перехватываемые входящие и исходящие соединения маркируются отдельными метками, которые вы можете изменять в конфигурационном файле kesl.ini.

Для исходящих соединений вводятся дополнительные правила маршрутизации, которые перенаправляют исходящий трафик для перехватываемых портов на интерфейс loopback в tproxy.

Выбор режима перехвата сетевого трафика

Как выбрать режим перехвата сетевого трафика в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.

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

5. В блоке **Режим перехвата трафика** выберите режим, в котором приложение будет перехватывать сетевой трафик:

   - **iptables**. Выбран по умолчанию. Приложение использует для перехвата трафика утилиту iptables.

   - **eBPF**. Приложение использует для перехвата трафика технологию eBPF.

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

Как выбрать режим перехвата сетевого трафика в командной строке

1. Выполните команду:

```
kesl-control --set-net-settings NetInterceptorMode=<UseEBPF|UseIPTables>
```

2. Для проверки текущих значений параметров сети выполните команду:

```
kesl-control --get-net-setting
```

Особенности и ограничения

- Для изменения режима перехвата трафика требуется перезапустить приложение. Во время перезапуска происходит разрыв установленных сетевых соединений.

- Если приложение не смогло использовать режим eBPF для перехвата сетевого трафика, будет использован режим iptables.

Как настроить политику проверки сертификатов

Параметры проверки сетевого трафика используются в работе компонентов Защита от веб-угроз, Защита от сетевых угроз, Защита от почтовых угроз и Веб-Контроль.

Защита от веб-угроз по умолчанию расшифровывает и проверяет сетевой трафик, передаваемый по защищенным соединениям. Для этого приложение проверяет всю цепочку сертификатов.

Политика проверки сертификатов включает в себя следующие параметры:

- способ проверки (локально или через интернет);

- доступ к веб-сайтам с недоверенным сертификатом;

- доступ к веб-сайтам с ошибкой проверки сертификата.

Если устройство не имеет прямого выхода в интернет, вы можете выбрать локальный способ проверки сертификатов приложением.

По умолчанию приложение разрешает установку сетевого соединения с доменом с недоверенным сертификатом. При этом приложение отображает HTML-страницу с предупреждением и информацией о причине, по которой этот домен не рекомендован для посещения. По ссылке из HTML-страницы с предупреждением пользователь может получить доступ к запрошенному веб-ресурсу.

Если стороннее приложение или служба устанавливает соединение с доменом с недоверенным сертификатом, приложение создаст собственный сертификат для проверки трафика. Новый сертификат будет иметь статус *Недоверенный*. Это нужно, чтобы предупредить стороннее приложение о недоверенном соединении, так как показать HTML-страницу в этом случае невозможно и соединение может быть установлено в фоновом режиме.

Во время проверки сертификатов могу возникать ошибки. Например, при работе с облачными хранилищами или при проверке самоподписанных сертификатов. По умолчанию приложение добавляет доменные имена таких веб-сайтой в исключения и не контролирует зашифрованный сетевой трафик при переходе на этот домен. Также приложение формирует событие об ошибке проверки защищенного соединения.

Просмотреть список доменов с ошибками проверки защищенных соединений возможно только в локальном интерфейсе приложения.

Как настроить политику проверки сертификатов в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки сети**.
5. В блоке **Проверка защищенных соединений** убедитесь, что переключатель находится в положении **Проверка защищенных соединений ВКЛЮЧЕНА**.

   Если переключатель выключен, Kaspersky Endpoint Security не имеет доступ к содержанию сайтов, адрес которых начинается с `https://`.
6. Перейдите по ссылке **Настройки** и настройте политику проверки сертификатов:

   - **Переход на домен с недоверенным сертификатом**. Действие при обнаружении неподтвержденного сертификата:

     - **Разрешать соединение**. Приложение будет разрешать соединение с доменом с недоверенным сертификатом. При этом приложение 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.

     - **Блокировать соединение**. При переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security блокирует сетевое соединение и при этом отображает HTML-страницу с информацией о причине, по которой переход на этот домен заблокирован.

- **Переход на домен с ошибкой проверки защищенного соединения**. Действие при возникновении ошибки проверки зашифрованных соединений:
  - **Разрешать и добавлять домен в исключения**. При возникновении ошибки проверки защищенного соединения приложение добавляет домен, при переходе на который возникла ошибка, в список исключений и не контролирует зашифрованный сетевой трафик при переходе на этот домен.
  - **Блокировать соединение**. При возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security блокирует это сетевое соединение.
- **Политика проверки сертификатов**. Способ, которым приложение проверяет сертификаты:
  - **Полная проверка**. Приложение использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата.
  - **Локальная проверка**. Приложение проверяет сертификат на компьютере локально.

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

Как настроить политику проверки сертификатов в командной строке

1. Для включения проверки зашифрованных соединений выполните команду:

```
kesl-control --set-net-settings EncryptedConnectionsScan=Yes
```

2. Для выбора способа проверки сертификатов выполните команду:

```
kesl-control --set-net-settings CertificateVerificationPolicy=<FullCheck|LocalCheck>
```

3. Для выбора действия при обнаружении неподтвержденного сертификата выполните команду:

```
kesl-control --set-net-settings UntrustedCertificateAction=<Allow|Block>
```

4. Для выбора действия при возникновении ошибки проверки зашифрованных соединений выполните команду:

```
kesl-control --set-net-setting EncryptedConnectionsScanErrorAction=<AddToAutoExclusions|Disconnect>
```

5. Для проверки текущих значений параметров сети выполните команду:

```
kesl-control --get-net-setting
```

Условные обозначения

Параметры команды

Параметр	Описание
`EncryptedConnectionsScan`	Режим проверки защищенного соединения: `Yes` (по умолчанию). Проверка зашифрованных соединений включена. `No`. Проверка зашифрованных соединений выключена.

Параметр	Описание
`CertificateVerificationPolicy`	Способ проверки сертификатов: `FullCheck` (по умолчанию). Приложение использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата. `LocalCheck`. Приложение проверяет сертификат на компьютере локально.
`UntrustedCertificateAction`	Действие при обнаружении неподтвержденного сертификата: `Allow` (по умолчанию). Приложение будет разрешать соединение с доменом с недоверенным сертификатом. При этом приложение 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. `Block`. 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.
`EncryptedConnectionsScanErrorAction`	Действие при возникновении ошибки проверки зашифрованных соединений: `AddToAutoExclusions` (по умолчанию). При возникновении ошибки проверки защищенного соединения приложение добавляет домен, при переходе на который возникла ошибка, в список исключений и не контролирует зашифрованный сетевой трафик при переходе на этот домен. `Disconnect`. При возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security блокирует это сетевое соединение.

Как настроить контролируемые порты

Во время работы Kaspersky Endpoint Security компонент Защита от сетевых угроз контролирует данные, передаваемые через некоторые сетевые порты. Список сетевых портов, которые контролирует приложение, настроен в соответствии с рекомендациями специалистов "Лаборатории Касперского".

Анализ поведения и Защита от эксплойтов дополнительно контролируют сетевые порты для процессов приложений, которые могут представлять угрозу безопасности компьютера. Приложение получает данные о таких процессах с антивирусными базами.

Вы можете настроить какие порты будет контролировать приложение:

- **Контролировать все сетевые порты**. Режим контроля сетевых портов, при котором приложение контролирует потоки данных, передаваемые через любые открытые сетевые порты компьютера.

  Выбор этого значения может значительно увеличить нагрузку на операционную систему.

- **Контролировать только выбранные сетевые порты**. Режим контроля сетевых портов, при котором компоненты защиты контролируют выбранные сетевые порты компьютера и сетевую активность выбранных приложений.

Если вы хотите перехватывать сетевые соединения к серверу NFS, требуется убедиться, что сервер NFS запущен с опцией `insecure` (чтобы он принимал соединения с портов не из диапазона 1–1024), иначе сервер NFS может отклонять такие соединения.

Как настроить контролируемые порты в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки сети**.
5. В блоке **Контролируемые порты** выберите режим контроля портов приложением:
   - **Контролировать все сетевые порты**.
   - **Контролировать только выбранные сетевые порты** (значение по умолчанию).
6. Если вы выбрали вариант **Контролировать только выбранные сетевые порты**, настройте список контролируемых портов:

   a. Нажмите на ссылку **Контролируемые порты**.

   b. Измените список контролируемых портов.

   > Для работы компонента Защита от почтовых угроз в параметрах сети должны контролироваться сетевые порты 25, 110, 143, 465, 587, 993 и 995. Эти сетевые порты добавлены в список контролируемых по умолчанию. Их удаление из списка может привести к нарушению работы компонента.
7. Сохраните внесенные изменения.

Как настроить контролируемые порты в командной строке

1. Для выбора режима контроля портов выполните команду:

   ```
   kesl-control --set-net-settings MonitorNetworkPorts=<All|Selected>
   ```
2. Если вы выбрали контроль только выбранных портов (`MonitorNetworkPorts=Selected`), задайте список контролируемых портов:

   ```
   kesl-control --set-net-settings NetworkPorts.item_#.PortName=<port name> NetworkPorts.item_#.Port=<port number>
   ```

   Для удаления порта из списка контролируемых измените список с помощью конфигурационного файла.
3. Для проверки текущих значений параметров сети выполните команду:

   ```
   kesl-control --get-net-settings
   ```

Условные обозначения

Параметры команды

Параметр	Описание
`MonitorNetworkPorts`	`Selected` (значение по умолчанию) – контролировать только сетевые порты, указанные в секции `[NetworkPorts.item_#]` (см. ниже). `All` – контролировать все сетевые порты. Выбор этого значения может значительно увеличить нагрузку на операционную систему.
`PortName`	Описание сетевого порта.
`Port`	Номера сетевых портов, контролируемые приложением. Доступные значения: `1 – 65535`. Для работы компонента Защита от почтовых угроз в параметрах сети должны контролироваться сетевые порты 25, 110, 143, 465, 587, 993 и 995. Эти сетевые порты добавлены в список контролируемых по умолчанию. Их удаление из списка может привести к нарушению работы компонента.

Исключения из перехвата трафика средствами операционной системы

В параметрах приложения Kaspersky Endpoint Security вы можете настраивать исключения из перехвата трафика по направлению трафика, IP-адресу и порту назначения. Если с помощью этих исключений не удается разрешить конфликт сетевого взаимодействия приложения Kaspersky Endpoint Security и клиентских приложений, вы можете использовать специальную разрешающую цепочку правил kesl_bypass.

Цепочка kesl_bypass – это специальный список правил, который приложение Kaspersky Endpoint Security создает в таблице mangle сетевого экрана операционной системы (iptables/ip6tables). Правила цепочки kesl_bypass позволяют исключать трафик из перехвата приложением Kaspersky Endpoint Security. Цепочка kesl_bypass добавляется первой в процесс обработки сетевых пакетов, таким образом правила kesl_bypass обрабатываются в первую очередь, до всех остальных правил iptables.

В отличие от исключений, которые вы можете настроить в параметрах Kaspersky Endpoint Security, цепочка kesl_bypass позволяет использовать для настройки исключений не только направление трафика, IP-адрес и порт назначения, но и другие параметры соединений.

Изменение правил в цепочке kesl_bypass выполняется средствами операционной системы.

Например, вы можете добавить в цепочку kesl_bypass правило, выполнив следующую команду:

```
iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT
```

Такое правило позволяет исключить из перехвата приложением Kaspersky Endpoint Security входящий и исходящий HTTP-трафик для порта 80 и любого IP-адреса. Это может помочь избежать потенциальных конфликтов с веб-сервисами, которым вы доверяете.

Если в цепочке настроены правила исключения трафика, они влияют на работу компонентов Защита от веб-угроз, Защита от сетевых угроз и Веб-Контроль.

При удалении приложения цепочка правил kesl_bypass в iptables и ip6tables удаляется, только если она была пустая.

Перехват файловых операций

Режим перехвата файловых операций влияет на работу компонентов Защита от файловых угроз и Контроль устройств, действия Запрет запуска объектов, задачи Проверка съемных дисков.

Если включен блокирующий режим перехвата файловых операций

- Приложение может блокировать во время проверки доступ к файлам, которые проверяет компонент Защита от файловых угроз. Если в результате проверки в файле не обнаружены угрозы, приложение разрешает доступ к файлу. При обнаружении зараженных объектов приложение выполняет действия, указанные в параметре **Действия при обнаружении угрозы** (`ActionOnThreat`) компонента Защита от файловых угроз.

- Приложение может блокировать доступ к файлам на устройстве на время, пока компонент Контроль устройств определяет возможность предоставления доступа к устройству. Приложение разрешает доступ к файлам, если в результате проверки Контроль устройств разрешает доступ к устройству с файлами.

- Приложение может блокировать файлы на устройстве на время, пока Запрет запуска объектов определяет возможность запуска этих файлов. Приложение разрешает запуск файлов, если в результате проверки Запрет запуска объектов разрешает запуск этих файлов.

- Приложение может во время проверки блокировать доступ к файлам на съемном диске. Если в результате проверки в файле не обнаружены угрозы, приложение разрешает доступ к файлу. При обнаружении зараженных объектов приложение выполняет действия, указанные в параметре **Действия при обнаружении угрозы** (`ActionOnThreat`) компонента Защита от файловых угроз.

Если выключен блокирующий режим перехвата файловых операций

- Компонент Защита от файловых угроз работает в режиме информирования, независимо от установленного режима работы, и разрешает доступ к файлам, проверку выполняет в асинхронном режиме.

- Компонент Контроль устройств работает в режиме информирования, независимо от установленного режима работы, и всегда разрешает доступ к устройствам.

- Действие Запрет запуска объектов работает в режиме информирования, независимо от установленного режима работы, и всегда разрешает запуск объектов.

- Приложение всегда разрешает доступ к файлам на съемном диске, проверку съемного диска выполняет в асинхронном режиме.

Такой режим перехвата файловых операций оказывает меньшее влияние на производительность системы во время работы, но есть риск, что угроза в файле не будет вылечена или удалена. Это возможно, если во время проверки процесс, связанный с этим файлом, успеет, например, изменить имя файла до принятия приложением решения о статусе этого файла.

По умолчанию блокирующий режим перехвата файловых операций включен.

Как настроить режим перехвата файловых операций в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в **Общие настройки** → **Настройки обнаружения**.
5. В блоке **Режим перехвата файловых операций** снимите или установите флажок **Блокировать доступ к файлам во время проверки**. По умолчанию флажок установлен.
6. Сохраните изменения.

Как настроить режим перехвата файловых операций в командной строке

В командной строке вы можете настраивать режим перехвата файловых операций с помощью параметра `FileBlockDuringScan` в общих параметрах приложения.

Для выбора режима перехвата файловых операций выполните команду:

```
kesl-control --set-app-settings FileBlockDuringScan=<Yes|No>
```

Условные обозначения

Параметры команды

Параметр	Описание
`FileBlockDuringScan`	`Yes` (значение по умолчанию) – блокировать доступ к файлам во время проверки компонентами Защита от файловых угроз и Контроль устройств, действия Запрет запуска объектов, задачи Проверка съемных дисков. `No` – не блокировать доступ к файлам во время проверки. Обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме.

Настройка перехвата системных событий

Вы можете выбирать используемый механизм перехвата системных событий в Web Console, в командной строке, а также в Консоли администрирования.

Изменить параметры перехвата системных событий возможно только на устройствах, где операционная система поддерживает технологию fanotify.

Настройка перехвата системных событий недоступна для устройств с процессором Эльбрус.

Как настроить механизм перехвата системных событий в Web Console

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

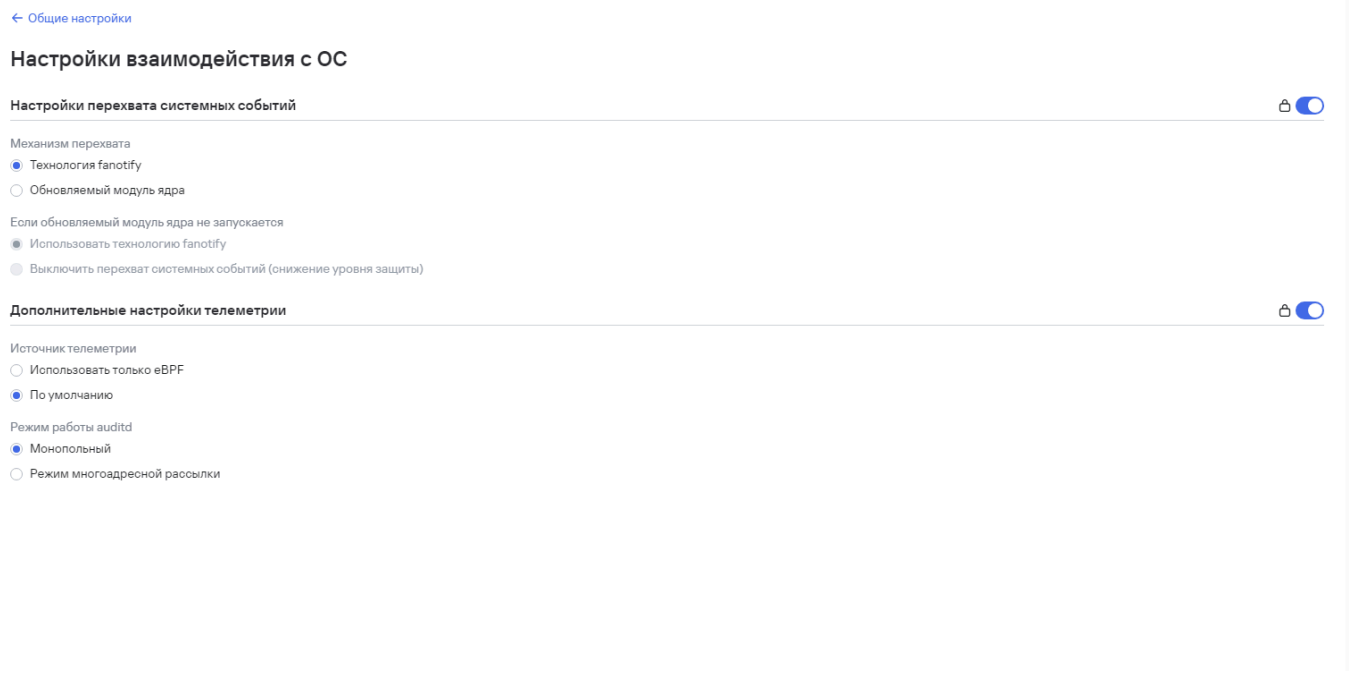
   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в **Общие настройки** → **Настройки взаимодействия с ОС**.

5. В блоке **Настройки перехвата системных событий** выберите механизм перехвата системных событий:

   - **Технология fanotify**.
   - **Обновляемый модуль ядра**. Если выбран этот вариант, выберите какое действие выполнит приложение, если обновляемый модуль ядра не запускается:
     - **Использовать технологию fanotify**.
     - **Выключить перехват системных событий (снижение уровня защиты)**.



Настройки взаимодействия с ОС

Как настроить механизм перехвата системных событий в командной строке

1. Для выбора механизма перехвата системных событий выполните команду:

```
kesl-control --set-app-settings InterceptorMode=<UseFanotify|UseUpdatableKernelModule>
```

2. Для выбора действия, которое приложение выполняет в случае ошибки запуска обновляемого модуля ядра, выполните команду:

```
kesl-control --set-app-settings InterceptorFallbackStrategy=<FallbackToFanotify|FallbackToLimitedMode>
```

3. Для настройки перезапуска приложения при выборе обновляемого модуля ядра выполните команду:

```
kesl-control --set-app-settings InterceptorApplyStrategy=<RestartServiceAutomatically|RestartServiceManually>
```

4. Для проверки текущих настроек приложения выполните команду:

```
kesl-control --get-app-settings [--json]
```

Условные обозначения

Параметры команды

Параметр	Описание
`InterceptorMode`	`UseFanotify` (значение по умолчанию) – использовать технологию fanotify для перехвата системных событий. `UseUpdatableKernelModule` – использовать обновляемый модуль ядра для перехвата системных событий.
`InterceptorFallbackStrategy`	`FallbackToFanotify` (значение по умолчанию) – перейти к использованию технологии fanotify для перехвата системных событий. `FallbackToLimitedMode` – не использовать перехват системных событий. Если приложение не использует перехват системных событий, проверка файлов в режиме реального времени не выполняется, уровень защиты устройства снижается.
`InterceptorApplyStrategy`	`RestartServiceAutomatically` – автоматически перезапускать приложение для запуска обновляемого модуля ядра. Рекомендуется использовать этот параметр. `RestartServiceManually` (значение по умолчанию) – запускать обновляемый модуль ядра после перезапуска приложения, выполненного пользователем вручную.

Приложение может использовать механизм перехвата на основе обновляемого модуля ядра, если операционная система соответствует требованиям для установки обновляемого модуля ядра.

Если вы выбрали механизм перехвата на основе обновляемого модуля ядра, вы можете настроить поведение приложения в случае, если при запуске обновляемого модуля ядра происходит ошибка, и модуль не запускается. В этом случае приложение может перейти к использованию технологии fanotify для перехвата системных событий или выключить перехват системных событий.

Если в ходе установки приложения не удалось установить обновляемый модуль ядра, вы можете установить его позже, когда появилась поддержка вашей операционной системы. Для этого:

1. Выполните обновление баз и модулей приложения. Обновляемый модуль ядра устанавливается в результате получения обновлений.

2. Выберите механизм перехвата на основе обновляемого модуля ядра.

Приложение может перейти к использованию обновляемого модуля ядра в следующих ситуациях:

- Если вы изменили механизм перехвата системных событий в параметрах приложения на обновляемый модуль ядра.

- Если на устройстве, где обновляемый модуль ядра не запускался, в ходе обновления баз и модулей получены обновления, обеспечивающие поддержку обновляемого модуля ядра.

Информация о состоянии обновляемого модуля ядра

Информация о состоянии и доступности обновляемого модуля ядра отображается в виде статусов:

- **Запущен** – модуль установлен и работает.
- **Остановлен** – модуль установлен, но не работает.
- **Недоступен** – модуль не поддерживается на устройстве.
- **Ошибка в работе** – произошла ошибка при запуске модуля, модуль не работает.

Вы можете просматривать статус обновляемого модуля ядра на устройстве в Web Console и в командной строке.

Как просматривать статус обновляемого модуля ядра в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Чтобы выбрать вложенную группу, нажмите на кнопку **Показать иерархию** в верхней части окна.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. Нажмите на имя устройства.
4. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.
5. В списке приложений, установленных на устройстве, нажмите на название приложения Kaspersky Endpoint Security.
6. Просмотрите статус функционального компонента **Обновляемый модуль ядра**.

Как просматривать статус обновляемого модуля ядра в командной строке

Чтобы посмотреть статус обновляемого модуля ядра, выполните команду:

```
kesl-control --app-info [--json]
```

Где `--json` – выводить данные в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в консоль.

"Безопасный" режим при использовании обновляемого модуля ядра

Если при использовании обновляемого модуля ядра приложение работает нестабильно, после достижения заданного максимального количества нештатных остановок приложения автоматически включается "безопасный" режим работы (в конфигурационном файле kesl.ini устанавливается значение параметра `SafeMode=yes`). По умолчанию приложение переходит в "безопасный" режим работы после трех нештатных остановок. Максимальное количество нештатных остановок приложения задается параметром `PanicThreshold` в конфигурационном файле kesl.ini.

Если приложение работает в "безопасном" режиме, обновляемый модуль ядра не запускается, приложение переходит к использованию технологии fanotify для перехвата системных событий. Приложение передает в Kaspersky Security Center тег `UpdatableKernelModule=Error`.

Чтобы продолжить использование обновляемого модуля ядра после устранения проблем в работе приложения, вам нужно выключить "безопасный" режим работы.

Как выключить "безопасный" режим работы приложения в командной строке

1. Откройте файл /var/opt/kaspersky/kesl/common/kesl.ini на редактирование.
2. В секции `[General]` установите значение параметра `SafeMode=no`.
3. Перезапустите Kaspersky Endpoint Security:

```
systemctl restart kesl
```

Безопасный режим будет выключен.

Настройка дополнительных параметров телеметрии

Вы можете настраивать следующие дополнительные параметры сбора телеметрии, отправляемой решениям Detection and Response при интеграции с ними:

- Источник телеметрии. Для сбора телеметрии можно использовать технологию eBPF и службу auditd или только технологию eBPF.
- Режим использования службы auditd. Приложение Kaspersky Endpoint Security может использовать службу auditd в монопольном режиме или в режиме многоадресной рассылки.

Как настроить дополнительные параметры телеметрии в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки взаимодействия с ОС**.
5. В блоке **Настройки телеметрии** укажите источник, который использует приложение Kaspersky Endpoint Security для сбора телеметрии:

   - **Использовать только eBPF** – использовать для сбора телеметрии только технологию eBPF.

     Если выбран параметр **Использовать только eBPF**, телеметрия для решений Detection and Response может иметь ограничения.

   - **По умолчанию** – использовать для сбора телеметрии технологию eBPF и службу auditd.

6. Также укажите режим работы службы auditd:

- **Монопольный** – приложение Kaspersky Endpoint Security использует службу auditd в монопольном режиме.
- **Режим многоадресной рассылки** – служба auditd используется в режиме многоадресной рассылки.

> Параметр применяется, только если для параметра **Источник телеметрии** выбран вариант **По умолчанию**.

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

Как настроить дополнительные параметры телеметрии в командной строке

В командной строке вы можете настраивать дополнительные параметры сбора телеметрии с помощью параметров `TelemetrySource` и `UseTelemetryMonopolyMode` предустановленной задачи Анализ поведения (*Behavior_Detection*).

1. Для выбора источника телеметрии выполните команду:

```
kesl-control --set-settings 20 TelemetrySource=<Default|OnlyEBPF>
```

2. Для выбора режима использования службы auditd выполните команду

```
kesl-control --set-settings 20 UseTelemetryMonopolyMode=<True|False>
```

Условные обозначения

Параметры команды

Параметр	Описание
`TelemetrySource`	`Default` (значение по умолчанию) – использовать для сбора телеметрии технологию eBPF и службу auditd. `OnlyEBPF` – использовать для сбора телеметрии только технологию eBPF.
`UseTelemetryMonopolyMode`	`True` (значение по умолчанию) – приложение Kaspersky Endpoint Security использует службу auditd в монопольном режиме. `False` – служба auditd используется в режиме многоадресной рассылки. Параметр `UseTelemetryMonopolyMode` применяется, только если для параметра `TelemetrySource` установлено значение `Default`.

Резервное хранилище

Если во время проверки защищенного устройства приложение Kaspersky Endpoint Security обнаруживает в файле вредоносный код, приложение может заблокировать этот файл, присвоить ему статус *Заражен*, поместить его копию в резервное хранилище и попытаться провести лечение файла.

Резервное хранилище – это хранилище резервных копий файлов, которые были удалены или изменены в процессе лечения. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

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.

Восстановление зараженных объектов может привести к заражению устройства.

Резервные копии файлов в резервном хранилище могут содержать персональные данные. Для доступа к объектам резервного хранилища требуются root-права.

Настройка параметров резервного хранилища

Вы можете настраивать параметры резервного хранилища на устройстве в Web Console, в Консоли администрирования или с помощью командной строки. Вы можете настраивать следующие параметры резервного хранилища:

- **Время хранения объектов в резервном хранилище**. По умолчанию объекты хранятся 30 суток. По истечении максимального срока хранения Kaspersky Endpoint Security удаляет наиболее старые файлы из резервного хранилища.
- **Максимальный размер резервного хранилища**. По умолчанию установлены следующие значения максимального размера резервного хранилища:
  - 0 МБ, если политика не применена;
  - 1024 МБ, если политика применена.

  После достижения максимального размера резервного хранилища приложение Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения.
- **Путь к директории, в которой хранятся объекты резервного хранилища и карантина** (этот параметр настраивается только с помощью командной строки). По умолчанию для хранения резервных копий файлов, а также файлов, помещенных на карантин, используется директория /var/opt/kaspersky/kesl/common/objects-backup/.

Как настроить параметры резервного хранилища в Web Console

Чтобы настроить параметры для резервного хранилища в свойствах политики:

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Отчеты и хранилище**.

5. В блоке **Резервное хранилище** настройте параметры:

   - **Удалять объекты через (дни)**. Если флажок установлен, то максимальный срок хранения файлов ограничен заданным интервалом времени. По умолчанию флажок установлен.

     Доступны значения от 0 до 10 000.

   - **Ограничить размер резервного хранилища до (МБ)**. Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. По умолчанию флажок установлен.

     Доступны значения от 1 до 4000.

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

Чтобы настроить параметры для резервного хранилища в свойствах управляемого устройства:

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Чтобы выбрать вложенную группу, нажмите на кнопку **Показать иерархию** в верхней части окна.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. Нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

5. Выберите приложение Kaspersky Endpoint Security

6. Перейдите в **Параметры приложения** → **Параметры хранилищ**.

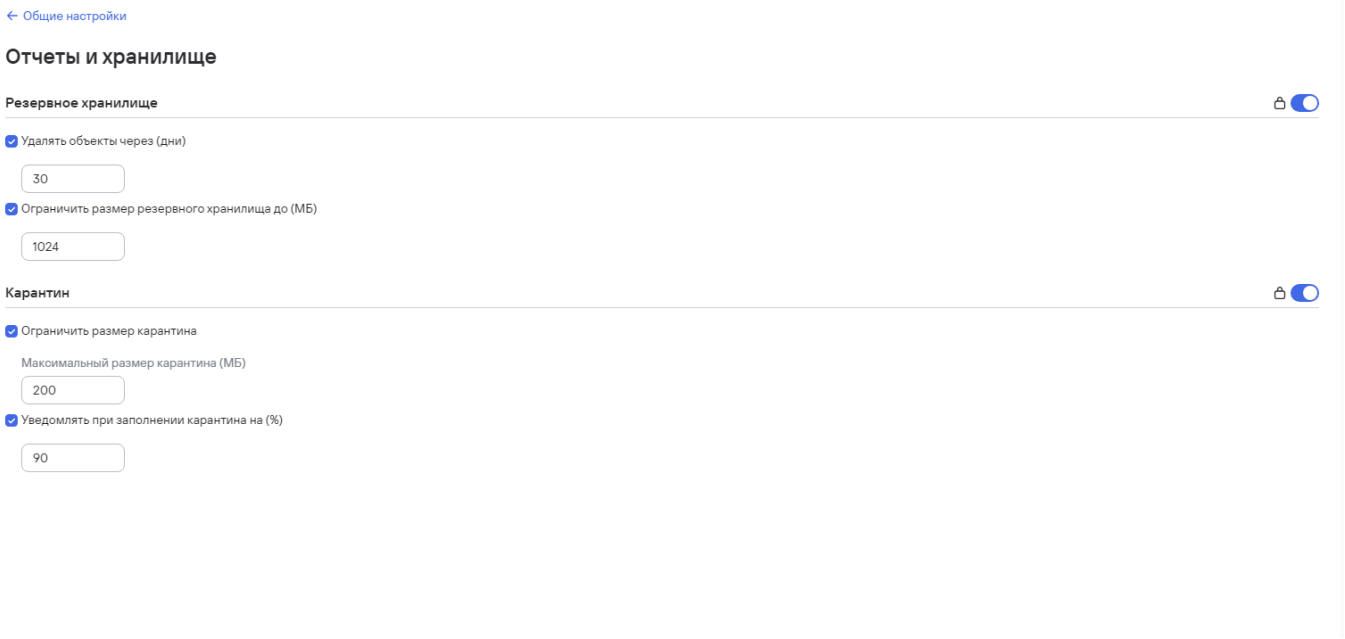
   - **Удалять объекты через (дни)**. Если флажок установлен, то максимальный срок хранения файлов ограничен заданным интервалом времени. По умолчанию флажок установлен.

     Доступны значения от 1 до 10 000.

   - **Ограничить размер резервного хранилища до (МБ)**. Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. По умолчанию флажок установлен.

     Доступны значения от 1 до 4000.

7. Сохраните изменения.



Отчеты и хранилище

Как настроить параметры резервного хранилища в командной строке

В командной строке вы можете настраивать параметры резервного хранилища с помощью параметров `BackupDaysToLive, BackupSizeLimit` и `QuarantineBackupFolder` в общих параметрах приложения.

1. Для настройки времени хранения объектов в резервном хранилище выполните команду:

```
kesl-control --set-app-settings BackupDaysToLive=<days>
```

2. Для настройки максимального размера резервного хранилища выполните команду:

```
kesl-control --set-app-settings BackupSizeLimit=<Backup size>
```

3. Для настройки директории, в которой хранятся объекты резервного хранилища и карантина, выполните команду:

```
kesl-control --set-app-settings QuarantineBackupFolder=<path to folder>
```

4. Для проверки текущих настроек приложения выполните команду:

```
kesl-control --get-app-settings
```

Параметры команды

Параметр	Описание
`BackupDaysToLive`	Интервал времени, в течение которого объекты хранятся в резервном хранилище (в сутках). По истечении заданного времени приложение удаляет самые старые резервные копии файлов. Чтобы снять ограничение на время хранения объектов в резервном хранилище, укажите значение 0.
`BackupSizeLimit`	Максимальный размер резервного хранилища (в мегабайтах). При достижении максимального размера резервного хранилища приложение удаляет самые старые резервные копии файлов. Чтобы снять ограничение на размер резервного хранилища, укажите значение 0.

Параметр	Описание
`QuarantineBackupFolder`	Путь к директории, в которой хранятся объекты резервного хранилища и карантина. Вы можете указать директорию, отличную от директории, заданной по умолчанию. В качестве директории для хранения объектов резервного хранилища и карантина можно использовать директории на любых устройствах. Не рекомендуется указывать директории, расположенные на удаленных устройствах, например смонтированных по протоколам Samba и NFS. Если указанной директории не существует или она недоступна, приложение использует директорию, заданную по умолчанию. Значение по умолчанию: `/var/opt/kaspersky/kesl/common/objects-backup/` Для доступа к заданной по умолчанию директории требуются root-права.

Просмотр объектов резервного хранилища

Общий список файлов, помещенных в резервное хранилище приложениями "Лаборатории Касперского" на клиентских устройствах, формируется в Kaspersky Security Center и доступен в Web Console и в Консоли администрирования (**Дополнительно** → **Хранилища** → **Резервное хранилище**).

Kaspersky Security Center не копирует файлы из резервных хранилищ на Сервер администрирования, все файлы размещаются в резервных хранилищах на защищенных устройствах.

Как просмотреть информацию об объектах в резервном хранилище в Web Console

1. В главном окне Web Console выберите **Хранилища** → **Файлы резервных копий**.

   Откроется список файлов, помещенных в резервное хранилище приложениями "Лаборатории Касперского" на клиентских устройствах. Kaspersky Security Center не копирует файлы из резервных хранилищ на Сервер администрирования, все файлы размещаются в резервных хранилищах на защищенных устройствах.

2. Просмотрите свойства файлов, находящихся в резервных хранилищах на защищенных устройствах:

   - **Имя файла**.
   - **Статус**:
     - *Warning*
     - *Probably infected*
     - *Added by user*
     - *False positive*
     - *Disinfected*
     - *Not infected*
     - *Password-protected*
     - *Deleted*
     - *Must be sent to Kaspersky*

- **Имя устройства**.
- **Выполняемое действие**:
  - *Удаляется*
  - *Лечение*
  - *Проверяется*
  - *Восстанавливается*
- **Объект**.
- **Дата помещения в хранилище**.
- **Запись добавлена**.
- **Размер (байт)**.
- **Папка восстановления**.
- **Пользователь**.
- **Описание**.
- **Имя виртуального Сервера администрирования**.

Как просмотреть информацию об объектах в резервном хранилище в командной строке

Чтобы просмотреть информацию об объектах резервного хранилища, выполните команду:

```
kesl-control -B --query ["<filter conditions>"] [-n <objects number>] [--json]
```

Где:

- `<filter conditions>` – одно или несколько логических выражений в формате `<field> <comparison operator> '<value>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса. Если вы не укажете условия фильтра, приложение выведет информацию обо всех объектах резервного хранилища.
- `<objects number>` – количество последних объектов из хранилища, информация о которых будет выведена. Если вы не укажете ключ `-n`, приложение отобразит информацию о последних 30 объектах. Если вы хотите, чтобы отображалась информация обо всех объектах, укажите значение `0`.
- `--json` – выводить данные в формате JSON.

В строке `ObjectId` отобразится числовой идентификатор, который приложение присвоило объекту при помещении в резервное хранилище. Этот идентификатор используется для выполнения действий над объектом, таких как восстановление или удаление объекта из резервного хранилища.

Как просмотреть информацию об объектах в резервном хранилище в графическом интерфейсе

1. Откройте главное окно графического интерфейса приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Резервное хранилище**.

   Откроется окно **Резервное хранилище**.

В окне отображается следующая информация об объектах резервного хранилища:

- название объекта;
- полный путь к объекту;
- дата добавления объекта в резервное хранилище;
- дата удаления объекта из резервного хранилища (это поле отображается, если задано ограничение на время хранения объектов в резервном хранилище);
- размер объекта.

Восстановление объектов из резервного хранилища

Файл, помещенный в резервное хранилище, восстанавливается в исходное местоположение согласно заданным параметрам. Мандатная метка (только на устройствах под управлением операционных систем Astra Linux) и атрибуты исходного файла (кроме атрибутов immutable и append-only) сохраняются при восстановлении.

На устройствах под управлением операционных систем Astra Linux восстановление файла из резервного хранилища завершается с ошибкой, если:

- Мандатная метка файла выше мандатной метки директории, в которую восстанавливается файл.
- Мандатная метка файла ниже мандатной метки директории, в которую восстанавливается файл, и для директории не установлен флаг ccnr.
- На устройствах с операционной системой Astra Linux в режиме замкнутой программной среды можно восстановить файл только под той учетной записью, под которой он был помещен в резервное хранилище. При восстановлении файла приложение создает директорию с мандатной меткой 3 (флаг cnnr).

Для выполнения действий с файлами в резервном хранилище в Kaspersky Security Center вам нужно включить передачу данных на Сервер администрирования о файлах резервного хранилища.

Восстановление зараженных объектов может привести к заражению устройства.

Как восстановить объекты из резервного хранилища в Web Console

1. В главном окне Web Console выберите **Хранилища** → **Файлы резервных копий**.

   Откроется список файлов, помещенных в резервное хранилище приложениями "Лаборатории Касперского" на клиентских устройствах. Kaspersky Security Center не копирует файлы из резервных хранилищ на Сервер администрирования, все файлы размещаются в резервных хранилищах на защищенных устройствах.

2. Установите флажки напротив файлов, которые хотите восстановить.

3. Нажмите на кнопку **Восстановить**.

Объекты резервного хранилища на клиентских устройствах будут восстановлены.

Как восстановить объекты из резервного хранилища в командной строке

Чтобы восстановить объект с исходным именем в исходное местоположение, выполните команду:

```
kesl-control -B --restore <object id>
```

Где `<object id>` – числовой идентификатор, который приложение присвоило объекту при помещении в резервное хранилище.

Чтобы восстановить объект с новым именем в указанную директорию, выполните команду:

```
kesl-control -B --restore <object id> --file <path to file>
```

Где `--file <path to file>` – новое имя файла и путь к директории, в которой вы хотите его сохранить. Если указанной директории не существует, приложение создает ее.

> На устройствах с операционной системой Astra Linux в режиме замкнутой программной среды можно восстановить файл только под той учетной записью, под которой он был помещен в резервное хранилище.

Как восстановить объекты из резервного хранилища в графическом интерфейсе

Чтобы восстанавливать объекты из резервного хранилища в их исходные директории:

1. Откройте главное окно графического интерфейса приложения.

2. В нижней части главного окна приложения нажмите на кнопку **Резервное хранилище**.

   Откроется окно **Резервное хранилище**.

3. Выберите объекты, которые хотите восстановить.

4. Нажмите на кнопку **Восстановить**.

Объекты из резервного хранилища будут восстановлены и доступны в исходной директории.

> Информация о восстановлении и удалении объектов записывается в журнал событий.

Удаление объектов из резервного хранилища

По истечении заданного времени или при достижении максимального размера резервного хранилища приложение автоматически удаляет из резервного хранилища самые старые резервные копии файлов с любым статусом.

Также вы можете самостоятельно удалить резервную копию как восстановленного, так и невосстановленного файла.

Как удалять объекты из резервного хранилища в Web Console

1. В главном окне Web Console выберите **Хранилища** → **Файлы резервных копий**.

   Откроется список файлов, помещенных в резервное хранилище приложениями "Лаборатории Касперского" на клиентских устройствах. Kaspersky Security Center не копирует файлы из резервных хранилищ на Сервер администрирования, все файлы размещаются в резервных хранилищах на защищенных устройствах.

2. Установите флажки напротив файлов, которые хотите удалить.

3. Нажмите на кнопку **Удалить**.

Объекты резервного хранилища на клиентских устройствах будут удалены.

Как удалять объекты из резервного хранилища в командной строке

Чтобы удалить выбранные объекты из резервного хранилища, выполните следующую команду:

```
kesl-control -B --mass-remove --query "<filter conditions>"
```

Где `<filter conditions>` – одно или несколько логических выражений в формате `<field> <comparison operator> '<value>'`, скомбинированных с помощью логического оператора `and` для ограничения результатов запроса.

Примеры:

```
Удалить объект с ID=15
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

```
Удалить объекты, в названии которых или в пути к которым содержится "test"
kesl-control -B --mass-remove --query "FileName like '%test%'"
```

Чтобы удалить все объекты из резервного хранилища, выполните следующую команду:

```
kesl-control -B --mass-remove
```

Как удалять объекты из резервного хранилища в графическом интерфейсе

1. Откройте главное окно графического интерфейса приложения.

2. В нижней части главного окна приложения нажмите на кнопку **Резервное хранилище**.

   Откроется окно **Резервное хранилище**.

3. Выберите объекты, которые хотите удалить.

4. Нажмите на кнопку **Удалить**.

Объекты резервного хранилища будут удалены. Удаленные объекты восстановить невозможно.

Информация о восстановлении и удалении объектов записывается в журнал событий.

Защита от сложных угроз и целевых атак

Решения Detection and Response от "Лаборатории Касперского" представляют собой системы безопасности, предназначенные для обнаружения сложных угроз и признаков атак на разных уровнях инфраструктуры организации. Решения Detection and Response предоставляют информацию об обнаруженных угрозах и позволяют управлять действиями по реагированию на обнаружения.

Приложение Kaspersky Endpoint Security может взаимодействовать со следующими решениями Detection and Response от "Лаборатории Касперского":

- Kaspersky Endpoint Detection and Response Expert (on-premises) на платформе Open Single Management Platform (OSMP). Интеграцию обеспечивает компонент приложения Kaspersky Endpoint Security – Endpoint Detection and Response Expert (on-premises) (далее также *EDR Expert (on-premises)*).

- Kaspersky Endpoint Detection and Response Expert (cloud) на платформе Open Single Management Platform (OSMP). Интеграцию обеспечивает компонент приложения Kaspersky Endpoint Security – Endpoint Detection and Response Expert (cloud) (далее также *EDR Expert (cloud)*).

- Компонентами Kaspersky Endpoint Detection and Response и Kaspersky Network Detection and Response на платформе Kaspersky Anti Targeted Attack Platform. Интеграцию обеспечивают следующие компоненты приложения Kaspersky Endpoint Security:

  - Endpoint Detection and Response Expert (on-premises) (далее также *EDR Expert (on-premises)*).

  - Network Detection and Response (KATA) (далее также *NDR (KATA)*).

- Sandbox на платформе Open Single Management Platform (OSMP) или на платформе Kaspersky Anti Targeted Attack Platform. Интеграцию обеспечивает компонент приложения Kaspersky Endpoint Security – *Sandbox*.

- Kaspersky Unified Monitoring and Analysis Platform.

- Kaspersky Endpoint Detection and Response Optimum. Интеграцию обеспечивает компонент приложения Kaspersky Endpoint Security – Endpoint Detection and Response Optimum (далее также *EDR Optimum*).

- Kaspersky Managed Detection and Response. Интеграцию обеспечивает компонент приложения Kaspersky Endpoint Security – Managed Detection and Response (далее также *MDR*).

Особенности интеграции с решениями Detection and Response

- Если вы используете приложение Kaspersky Endpoint Security в режиме EDR-агента, поддерживается интеграция только с Kaspersky Endpoint Detection and Response Expert (on-premises) на платформе Open Single Management Platform (OSMP) и с компонентами Kaspersky Endpoint Detection and Response и Kaspersky Network Detection and Response на платформе Kaspersky Anti Targeted Attack Platform.

- При интеграции приложения Kaspersky Endpoint Security с решениями Kaspersky Managed Detection and Response и Kaspersky Anti Targeted Attack Platform встроенный агент может записывать в журнал systemd-journald большое количество событий. Если вы хотите выключить запись событий аудита в systemd-journald, вам нужно отключить сокет systemd-journald-audit и перезагрузить операционную систему.

  Отключить сокет systemd-journald-audit

  ```
  systemctl stop systemd-journald-audit.socket
  systemctl disable systemd-journald-audit.socket
  systemctl mask systemd-journald-audit.socket
  ```

- В операционной системе СинтезМ-Клиент конфигурация службы auditd по умолчанию заблокирована против изменений, то есть находится в режиме работы `enabled 2`. Для корректной работы компонента Анализ поведения при интеграции Kaspersky Endpoint Security с решениями Kaspersky Managed Detection and Response и Kaspersky Anti Targeted Attack Platform требуется изменить режим работы auditd в конфигурационных файлах на режим без блокировки конфигурации `enabled 1` и перезагрузить операционную систему.

- Решения Detection and Response могут работать некорректно на виртуальных машинах, созданных из образа с установленным Kaspersky Endpoint Security для Linux. При интеграции с решениями Detection and Response используется уникальный идентификатор компьютера (Sensor ID). Приложение создает этот идентификатор при первой установке и сохраняет его даже после удаления. При клонировании образа виртуальная машина наследует Sensor ID, из-за чего решения Detection and Response могут определять несколько виртуальных машин как одно устройство.

  Рекомендации по созданию эталонного образа для корректной интеграции с MDR

  Как подготовить эталонный образ для корректной интеграции с EDR Expert (on-premises)

Действия по реагированию

При интеграции с решениями Detection and Response приложение Kaspersky Endpoint Security может выполнять действия по реагированию, направленные на обеспечение функций безопасности. Действия по реагированию могут формироваться на стороне решения Detection and Response и выполняться автоматически на устройствах с Kaspersky Endpoint Security, если такая функция включена в параметрах решения Detection and Response. Вы также можете настраивать и выполнять действия по реагированию вручную.

> Параметры действий по реагированию отличаются в зависимости от решения Detection and Response, с которым интегрируется приложение Kaspersky Endpoint Security.

Приложение Kaspersky Endpoint Security может выполнять следующие действия по реагированию:

- Сетевая изоляция устройства.

При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response Expert (cloud), с Kaspersky Endpoint Detection and Response (KATA) или с Kaspersky Managed Detection and Response включение и выключение сетевой изоляции выполняется на стороне соответствующего решения Detection and Response. Вы можете вручную выключать сетевую изоляцию устройства.

При интеграции с Kaspersky Endpoint Detection and Response Optimum устройство может быть изолировано от сети в автоматическом или ручном режиме. Вы можете настраивать параметры сетевой изоляции и вручную выключать сетевую изоляцию устройства.

- Помещение файла на карантин.

  Действие выполняется с помощью задачи помещения файла на карантин (*Quarantine file*).

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response Expert (cloud), с Kaspersky Endpoint Detection and Response (KATA) или с Kaspersky Managed Detection and Response задача создается и запускается на стороне соответствующего решения Detection and Response.

  При интеграции с Kaspersky Endpoint Detection and Response Optimum файл может быть помещен на карантин автоматически в результате обнаружения индикаторов компрометации.

  При интеграции с Kaspersky Endpoint Detection and Response Optimum или с Kaspersky Managed Detection and Response вы также можете помещать файлы на карантин вручную.

- Восстановление файла из карантина.

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response Expert (cloud), с Kaspersky Endpoint Detection and Response (KATA) или Kaspersky Managed Detection and Response действие по реагированию формируется на стороне соответствующего решения Detection and Response. Вы также можете выполнять действие вручную с помощью Kaspersky Security Center или командной строки.

  При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете выполнять действие вручную с помощью Kaspersky Security Center или командной строки.

- Удаление файла из карантина.

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response Expert (cloud), с Kaspersky Endpoint Detection and Response (KATA) или Kaspersky Managed Detection and Response действие по реагированию формируется на стороне соответствующего решения Detection and Response. Вы также можете выполнять действие вручную с помощью Kaspersky Security Center или командной строки.

  При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете выполнять действие вручную с помощью Kaspersky Security Center или командной строки.

- Получение файла из карантина.

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response Expert (cloud) или с Kaspersky Endpoint Detection and Response (KATA) действие по реагированию формируется на стороне соответствующего решения Detection and Response.

  При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете выполнять действие вручную с помощью Kaspersky Security Center.

- Получение файла с устройства.

  Действие выполняется с помощью задачи получения файла с устройства (*Get file*). Например, вы можете настроить получение файла журнала событий, который создает стороннее приложение.

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response Expert (cloud), с Kaspersky Endpoint Detection and Response (KATA) или Kaspersky Managed Detection and Response задача создается и запускается на стороне соответствующего решения Detection and Response.

При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете создавать задачи получения файлов с устройств в Web Console.

- Удаление файла с устройства.

  Действие выполняется с помощью задачи удаления файла с устройства (*Delete file*).

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response Expert (cloud) или с Kaspersky Endpoint Detection and Response (KATA) задача создается и запускается на стороне соответствующего решения Detection and Response.

  При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете создавать задачи удаления файлов с устройств в Web Console.

- Удаленный запуск процесса на устройстве.

  Действие выполняется с помощью задачи запуска процесса (*Run application*). Например, вы можете удаленно запустить утилиту, которая создает файл с конфигурацией устройства, а затем получить созданный файл с помощью задачи получения файла с устройства.

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response Expert (cloud), с Kaspersky Endpoint Detection and Response (KATA) или Kaspersky Managed Detection and Response задача создается и запускается на стороне соответствующего решения Detection and Response.

  При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете создавать и выполнять задачи запуска процесса в Web Console.

- Удаленное завершение процесса на устройстве.

  Действие выполняется с помощью задачи завершения процесса (*Kill process*). Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена с помощью задачи запуска процесса.

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response Expert (cloud), с Kaspersky Endpoint Detection and Response (KATA) или Kaspersky Managed Detection and Response задача создается и запускается на стороне соответствующего решения Detection and Response.

  При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете создавать и выполнять задачи завершения процессов в Web Console.

- Обнаружение индикаторов компрометации (IOC) на устройствах.

  Индикатор компрометации (Indicator of Compromise, IOC) – набор данных об объекте или активности, который указывает на несанкционированный доступ к устройству (компрометация данных). Например, индикатором компрометации может быть большое количество неудачных попыток входа в систему.

- Запуск *YARA-проверки*.

  YARA-проверка – процесс, в ходе выполнения которого Kaspersky Endpoint Security использует YARA-файлы для поиска сигнатур вредоносной активности на устройстве. *YARA-файлы* – это файлы с расширением .YARA или .YAR, которые содержат YARA-правила. *YARA-правила* представляют собой описание сигнатур целевых атак и вторжений в IT-инфраструктуру организации. По этим правилам Kaspersky Endpoint Security производит проверку объектов. Если правило выполняется, анализатор выносит заключение о заражении с соответствующими подробностями в журнале. Проверка выполняется рекурсивно на локальных дисках. Проверка сетевых, подключаемых и облачных ресурсов не поддерживается.

  Команда для YARA-проверки на устройстве с установленным Kaspersky Endpoint Security создается и запускается на стороне решений Kaspersky Endpoint Detection and Response Expert (on-premises) и Kaspersky Endpoint Detection and Response Expert (cloud).

- Запрет запуска объектов.

- Сбор форензики.

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) и Kaspersky Endpoint Detection and Response Expert (cloud) вы можете собрать цифровые данные, которые могут быть полезными при расследовании инцидентов, связанных с киберпреступлениями и утечками данных.

  Действие выполняется с помощью следующих задач:

  - задачи сбора форензики (*Get forensics*), которая собирает следующие типы информации:
    - список файлов;
    - список процессов;
    - список точек автозапуска;
  - задачи получения дампа памяти (*Get memory dump*);
  - задачи получения дампа памяти процесса (*Get process memory dump*);
  - задачи получения образа диска (*Get disk image*).

  Задачи создаются и запускаются на стороне решений Kaspersky Endpoint Detection and Response Expert (on-premises) и Kaspersky Endpoint Detection and Response Expert (cloud).

Поиск индикаторов компрометации

Индикатор компрометации (Indicator of Compromise, IOC) – набор данных об объекте или активности, который указывает на несанкционированный доступ к компьютеру (компрометация данных). Например, индикатором компрометации может быть большое количество неудачных попыток входа в систему. Задача *Поиск IOC* позволяет обнаруживать индикаторы компрометации на компьютере и выполнять действия по реагированию на угрозы.

Функциональность поиска IOC доступна в приложении Kaspersky Endpoint Security при выполнении одного из следующих условий:

- Включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Optimum и активирован компонент EDR Optimum.

  В этом случае поиск IOC выполняется с помощью задачи *Поиск IOC* (*IOC Scan*).

- Включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (on-premises) или с компонентом Kaspersky Endpoint Detection and Response (KATA) и активирован компонент EDR Expert (on-premises).

  В этом случае поиск IOC выполняется на стороне соответствующего решения.

При выполнении задачи поиска IOC проверка по IOC-терминам (свойствам IOC-объекта, например, хеш-сумме файла) выполняется только в основном пространстве имен операционной системы. Задача поиска IOC не вычисляет хеш-суммы файлов размером более 200 МБ.

Для поиска индикаторов компрометации Kaspersky Endpoint Security использует IOC-файлы, подготовленные пользователем. Если вы хотите добавить индикатор компрометации вручную, ознакомьтесь с требованиями к IOC-файлам. Если IOC-файл не соответствует требованиям, приложение не сможет его использовать.

Идентификаторы всех IOC-файлов, которые используются в одной задаче поиска IOC, должны быть уникальными. Если вы загружаете несколько IOC-файлов с одинаковыми идентификаторами, то приложение использует только один из этих IOC-файлов. Остальные IOC-файлы будут автоматически исключены.

Создание задачи Поиск IOC

Вы можете создавать задачи *Поиск IOC* вручную следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали алерта – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum и в справке Kaspersky Endpoint Detection and Response Expert.

- С помощью мастера создания задач.

- Локально в командной строке.

Как создать задачу Поиск IOC в Web Console

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Endpoint Security для Linux 12.5**.

   b. В раскрывающемся списке **Тип задачи** выберите **Поиск IOC**.

   c. В поле **Название задачи** введите название новой задачи.

   d. В блоке **Устройства, которым будет назначена задача** выберите способ определения области действия задачи.

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

5. Завершите работу мастера.

   В списке задач отобразится новая задача.

6. Нажмите на новую задачу.

   Откроется окно свойств задачи.

7. Выберите вкладку **Параметры приложения**.

8. Перейдите в раздел **Поиск угроз**.

9. Загрузите IOC-файлы для поиска индикаторов компрометации.

После загрузки IOC-файлов приложение покажет сводную информацию о файле, включая список индикаторов, которые не прошли проверку. После загрузки IOC-файлов вы можете вручную изменять содержание файлов во встроенном редакторе прямо в свойствах задачи. Kaspersky Endpoint Security поддерживает изменение содержания IOC-файлов, которые соответствуют стандарту OpenIOC версии 1.1. Изменить содержание IOC-файлов, соответствующих стандарту OpenIOC версии 1.0, невозможно.

Kaspersky Endpoint Security добавит IOC-файлы в IOC-коллекцию. Если требуется, вы можете временно выключить IOC-файлы из области действия задачи.

> Не рекомендуется добавлять или удалять IOC-файлы после запуска задачи. Это может привести к некорректному отображению результатов поиска IOC для предыдущих запусков задачи. Для поиска индикаторов компрометации по новым IOC-файлам рекомендуется добавлять новые задачи.

10. Перейдите в раздел **Настройки проверки**.

11. Если требуется, настройте ретроспективный поиск IOC.

    Ретроспективный поиск IOC – это режим работы задачи *Поиск IOC*, при котором Kaspersky Endpoint Security выполняет поиск индикаторов компрометации по данным, полученным за определенный интервал времени. Режим предназначен для поиска индикаторов компрометации по телеметрии защищаемого компьютера, такой как сетевая активность, процессы, файлы и другие. Kaspersky Endpoint Security анализирует данные в журналах операционной системы и браузеров на компьютере. Ретроспективный поиск IOC анализирует журналы следующих браузеров: Google Chrome, Mozilla Firefox, Microsoft Edge (версии 79 и выше).

    a. В блоке **Ретроспективный поиск IOC** перейдите в настройки поиска.

    b. Включите переключатель **Ретроспективный поиск IOC**.

    c. Задайте интервал времени для ретроспективного поиска IOC.

12. Выберите типы данных (IOC-документы), которые необходимо анализировать во время выполнения задачи.

    > Kaspersky Endpoint Security автоматически выбирает типы данных (IOC-документы) для задачи *Поиск IOC* в соответствии с содержанием загруженных IOC-файлов. Не рекомендуется самостоятельно отменять выбор типов данных.

    Дополнительно вы можете настроить области поиска для типа данных **Файлы - FileItem**. Задайте область поиска IOC на компьютере с помощью предустановленных областей.

13. Перейдите в раздел **Настройки реагирования**.

14. Выберите режим работы задачи: **Только обнаруживать** или **Обнаруживать и реагировать**.

15. Выберите действие по реагированию при обнаружении IOC:

    - **Запустить проверку важных областей**. Если выбран этот вариант действия, то Kaspersky Endpoint Security запускает задачу *Проверка важных областей*. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

Важные области, которые проверяет Kaspersky Endpoint Security

- /lib/systemd
- /lib/udev
- /lib/dbus-1.0
- /usr/local/lib/systemd/user
- /usr/share/dbus-1
- /usr/share/gdm/autostart
- /usr/share/gnome/autostart
- /var/spool/at
- /var/spool/at/spool
- /var/spool/anacron
- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession

- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

- **Копию поместить на карантин, объект удалить**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удаляет вредоносный объект, обнаруженный на компьютере. Перед удалением объекта Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин.

  Если флажок снят, вы можете поместить файл на карантин после выполнения задачи вручную. Если в результате выполнения задачи *Поиск IOC* обнаружен файл, который может вызывать компрометацию данных, то вы можете поместить этот файл на карантин прямо из результатов поиска IOC (**Параметры приложения** → **Результаты поиска IOC**). В результате Kaspersky Endpoint Security запустит мастер создания задач с предустановленными данными об обнаруженном файле. Вам нужно только настроить дополнительные параметры задачи, например, задать расписание запуска задачи.

- **Изолировать устройство от сети**. Если выбран этот вариант действия, то Kaspersky Endpoint Security изолирует компьютер от сети для предотвращения распространения угрозы. Вы можете настроить время изоляции в параметрах компонента Endpoint Detection and Response.

  Если флажок снят, вы можете изолировать компьютер от сети после выполнения задачи вручную. Если в результате выполнения задачи *Поиск IOC* обнаружен файл, который может вызывать компрометацию данных, то вы можете поместить этот файл на карантин прямо из результатов поиска IOC (**Параметры приложения** → **Результаты поиска IOC**). В результате Kaspersky Endpoint Security запустит мастер создания задач с предустановленными данными об обнаруженном файле. Вам нужно только настроить дополнительные параметры задачи, например, задать расписание запуска задачи.

16. В окне свойств задачи выберите вкладку **Расписание**.
17. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

18. Сохраните внесенные изменения.
19. Установите флажок напротив задачи.
20. Нажмите на кнопку **Запустить**.

Вы можете посмотреть результат выполнения задачи *Поиск IOC* в свойствах задачи в Web Console в разделе **Результаты поиска IOC**. Срок хранения результатов поиска IOC составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет старые записи.

Как создать задачу Поиск IOC в командной строке

Выполните команду:

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

Условные обозначения

Параметры расписания задачи Поиск вредоносного ПО

Параметр	Описание
`--path`	Путь к IOC-файлу или директории с IOC-файлами с расширением IOC или XML, с помощью которых требуется выполнить проверку. *IOC-файлы* – файлы, содержащие набор индикаторов, при совпадении с которыми приложение считает событие обнаружением. IOC-файлы должны соответствовать стандарту описания OpenIOC. Вы можете указать несколько путей, разделяя их пробелами. Вы также можете указать оба типа путей (к файлу и к директории).
`--process`	Анализ данных о процессах при поиске IOC (термин ProcessItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет запущенные на компьютере процессы при выполнении проверки. Если в IOC-файле указаны IOC-термины IOC-документа ProcessItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security проверяет данные о процессах, только если IOC-документ ProcessItem описан в переданном на проверку IOC-файле.
`--hint`	Анализ данных о файле при поиске IOC (термины ProcessItem и FileItem). Вы можете выбрать файл следующими способами: • `<full path to the executable file of the process>` – термин ProcessItem; • `<full path to the file>` – термин FileItem.
`--arpentry`	Анализ данных о записях в ARP-таблице при поиске IOC (термин ArpEntryItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет таблицу ARP. Если в IOC-файле указаны термины IOC-документа ArpEntryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security проверяет ARP-таблицу, только если IOC-документ ArpEntryItem описан в переданном на проверку IOC-файле.
`--ports`	Анализ данных о портах, открытых на прослушивание, при поиске IOC (термин PortItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не проверяет таблицу активных соединений на устройстве. Если в IOC-файле указаны термины IOC-документа PortItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security проверяет таблицу активных соединений, только если IOC-документ PortItem описан в переданном на проверку IOC-файле.
`--system`	Анализ данных об окружении при поиске IOC (термин SystemInfoItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не анализирует данные об окружении. Если в IOC-файле указаны термины IOC-документа SystemInfoItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security анализирует данные об окружении, только если IOC-документ SystemInfoItem описан в переданном на проверку IOC-файле.
`--files`	Анализ данных о файлах при поиске IOC (термин FileItem). Если параметр установлен со значением `off`, Kaspersky Endpoint Security не анализирует данные о файлах. Если в IOC-файле указаны термины IOC-документа FileItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не установлен, Kaspersky Endpoint Security анализирует данные о файлах, только если IOC-документ FileItem описан в переданном на проверку IOC-файле.
`--drives`	Область поиска IOC при анализе данных для IOC-документа FileItem. Доступны следующие значения области поиска: • `<all>` – все доступные файловые области. • `<system>` – файлы, расположенные в папках, в которых установлена ОС. • `<critical>` – временные файлы в пользовательских и системных папках. • `<custom>` – файлы в указанных пользователем областях (`/scope=<list of folders to scan>`). Если параметр не установлен, проверка выполняется в критических областях.
`--excludes`	Область исключений при анализе данных для IOC-документа FileItem. Вы можете указать несколько путей через пробел.
`--scope`	Пользовательская область поиска IOC при анализе данных для IOC-документа FileItem (`/drives=custom`). Вы можете указать несколько путей через пробел.

Параметр	Описание
`--action`	Действие, выполняемое при обнаружении индикаторов компрометации: • `Skip`. Если выбран этот вариант действия, то Kaspersky Endpoint Security только обнаруживает файлы, который могут вызывать компрометацию данных. • `QuarantineFile`. Если выбран этот вариант действия, то Kaspersky Endpoint Security удаляет вредоносный объект, обнаруженный на компьютере. Перед удалением объекта Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин. • `IsolateHost`. Если выбран этот вариант действия, то Kaspersky Endpoint Security изолирует компьютер от сети для предотвращения распространения угрозы. • `ScanCriticalAreas`. Если выбран этот вариант действия, то Kaspersky Endpoint Security запускает задачу *Проверка важных областей*. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

Сетевая изоляция

При интеграции с решениями Detection and Response в рамках действия по реагированию на угрозы устройство может быть изолировано от сети.

Особенности работы сетевой изоляции

После включения сетевой изоляции приложение разрывает все активные и блокирует все новые сетевые соединения TCP/IP на устройстве, кроме следующих:

- Соединений, указанных в исключениях из сетевой изоляции.
- Соединений, инициированных службами Kaspersky Endpoint Security.
- Соединений, инициированных Агентом администрирования Kaspersky Security Center.
- Соединений с SVM и Сервером интеграции, если приложение используется в режиме Легкого агента.
- Соединений с KSN (при интеграции с Kaspersky Managed Detection and Response).

Сетевая изоляция может применяться при выполнении одного из следующих условий:

- Включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Optimum и активирован компонент EDR Optimum.
- Включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (on-premises) или с компонентом Kaspersky Endpoint Detection and Response (KATA) и активирован компонент EDR Expert (on-premises).
- Включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response и активирован компонент MDR.

При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response (KATA) и Kaspersky Managed Detection and Response включение и выключение сетевой изоляции устройства, а также настройка исключений из сетевой изоляции выполняется на стороне соответствующего решения Detection and Response. Подробнее см. в справке Kaspersky Endpoint Detection and Response Expert (on-premises), в справке Kaspersky Anti Targeted Attack Platform или в справке Kaspersky Managed Detection and Response. Если требуется, вы можете вручную выключать сетевую изоляцию устройства:

- в свойствах устройства в Web Console (только при интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) или с Kaspersky Endpoint Detection and Response (KATA));
- в командной строке.

Выключение сетевой изоляции вручную доступно вне зависимости от того, включена ли интеграция с решениями Detection and Response, а также вне зависимости от того, распространяется ли на устройство действие политики.

При интеграции с Kaspersky Endpoint Detection and Response Optimum сетевая изоляция может применяться в одном из следующих режимов:

- Автоматический режим сетевой изоляции. Устройство может быть изолировано от сети автоматически в результате обнаружения индикаторов компрометации. Если при создании и настройке параметров задачи *Поиск IOC* в блоке **Действия при обнаружении IOC** вы установили флажки **Применять действия по реагированию при обнаружении IOC** и **Изолировать устройство от сети**, то включение сетевой изоляции происходит автоматически при обнаружении приложением индикаторов компрометации.

  Вы можете настроить следующие параметры сетевой изоляции в автоматическом режиме:

  - Изменить период времени, по истечении которого сетевая изоляция автоматически выключается.
  - Настроить исключения из сетевой изоляции для устройств, изолированных автоматически.

  > Если на устройство, изолируемое в автоматическом режиме, распространяется политика, то применяются параметры, заданные в политике. Если политика не распространяется, то применяются параметры, заданные в свойствах устройства.

- Ручной режим сетевой изоляции. Устройство можно изолировать от сети на время исследования обнаруженной угрозы. Вы можете вручную включать сетевую изоляцию устройства в окне с деталями алерта и в свойствах устройства в Web Console.

  Вы можете настроить следующие параметры сетевой изоляции в ручном режиме:

  - Изменить период времени, по истечении которого сетевая изоляция автоматически выключается.
  - Настроить исключения из сетевой изоляции для устройств, изолированных вручную.

При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете вручную выключать сетевую изоляцию устройства в свойствах устройства в Web Console и в командной строке.

Вы можете проверять статус сетевой изоляции устройства в командной строке.

Изолированному устройству автоматически присваивается тег **ISOLATED FROM NETWORK**. После выключения сетевой изоляции этот тег автоматически снимается.

Общую информацию о получении списка изолированных устройств по тегу см. в справке Kaspersky Endpoint Detection and Response Optimum.

Ограничения сетевой изоляции

При использовании сетевой изоляции настоятельно рекомендуется ознакомиться с описанными ограничениями.

Для работоспособности сетевой изоляции требуется, чтобы приложение Kaspersky Endpoint Security было запущено. Во время сбоя в работе приложения Kaspersky Endpoint Security (когда приложение не запущено), блокировка трафика при включении сетевой изоляции решениями Detection and Response не гарантируется.

DHCP и DNS не добавляются автоматически в исключения из сетевой изоляции, поэтому если сетевой адрес какого-то ресурса был изменен во время сетевой изоляции, приложение Kaspersky Endpoint Security не сможет получить к нему доступ. Это же относится к узлам отказоустойчивого сервера KATA. Не рекомендуется менять их адреса, чтобы приложение Kaspersky Endpoint Security не потеряло с ними связь.

Прокси-сервер не добавляется автоматически в исключения из сетевой изоляции, поэтому требуется добавить его в исключения вручную, чтобы приложение Kaspersky Endpoint Security не потеряло связь с сервером, обеспечивающим интеграцию.

Исключение процесса из сетевой изоляции по имени поддерживается на устройствах с версией ядра от 4.18 с поддержкой eBPF с BTF и с включенными функциями tracepoints и kprobes для трассировки ядра.

Если приложение Kaspersky Endpoint Security используется в стандартном режиме или в режиме EDR-Агента, при использовании сетевой изоляции рекомендуется:

- Использовать прокси-сервер KSN для взаимодействия с Kaspersky Security Network.
- Использовать Kaspersky Security Center в качестве прокси-сервера для активации приложения.

  В случае невозможности использования Kaspersky Security Center в качестве прокси-сервера требуется настроить параметры нужного прокси-сервера и добавить его в исключения.
- Указать Kaspersky Security Center в качестве источника обновлений баз.

Эти рекомендации неприменимы, если приложение Kaspersky Endpoint Security используется в режиме Легкого агента.

Включение и выключение сетевой изоляции устройства вручную в Web Console

Вы можете включать сетевую изоляцию устройства с помощью Web Console только при интеграции с Kaspersky Endpoint Detection and Response Optimum.

Включение и выключение сетевой изоляции устройства вручную при интеграции с Kaspersky Endpoint Detection and Response Optimum

Чтобы включить или выключить сетевую изоляцию устройства вручную:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. При необходимости выберите группу администрирования, найдите нужное устройство и нажмите на его имя.

3. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

4. В списке приложений, установленных на устройстве, нажмите на название приложения Kaspersky Endpoint Security.

5. В открывшемся окне свойств приложения на вкладке **Параметры приложения** выберите **Встроенные агенты** → **Endpoint Detection and Response**.

6. В открывшемся окне в блоке параметров **Сетевая изоляция** выполните одно из следующих действий:

   - Нажмите на кнопку **Изолировать устройство от сети**, чтобы включить сетевую изоляцию устройства. Кнопка активна, только если включен переключатель **Endpoint Detection and Response**;

     При нажатии на кнопку устройство будет изолировано на период, указанный в свойствах задачи *Включение сетевой изоляции (NetworkIsolationStart)*.

   - Нажмите на кнопку **Разблокировать изолированное устройство**, чтобы выключить сетевую изоляцию устройства. Кнопка активна независимо от состояния переключателя **Endpoint Detection and Response**.

7. Нажмите на кнопку **OK**.

Если вы включили сетевую изоляцию устройства, то Kaspersky Endpoint Security присвоит устройству тег **ISOLATED FROM NETWORK**. Если вы выключили сетевую изоляцию устройства, то Kaspersky Endpoint Security снимет этот тег с устройства.

Выключение сетевой изоляции устройства вручную при интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) или Kaspersky Endpoint Detection and Response (KATA)

Чтобы выключить сетевую изоляцию устройства вручную:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и в открывшемся окне выберите группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. В списке найдите нужное устройство и нажмите на его имя.

4. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

5. В списке приложений, установленных на устройстве, нажмите на название приложения Kaspersky Endpoint Security.

6. В открывшемся окне свойств приложения на вкладке **Параметры приложения** выберите раздел **Detection and Response**.

7. В блоке **Сетевая изоляция (EDR Expert (on-premises))** нажмите на кнопку **Разблокировать изолированное устройство**, чтобы выключить сетевую изоляцию устройства.

После выключения сетевой изоляции устройства Kaspersky Endpoint Security снимет тег **ISOLATED FROM NETWORK** с устройства.

Настройка длительности сетевой изоляции в автоматическом режиме

Вы можете настраивать длительность сетевой изоляции в автоматическом режиме только при интеграции с Kaspersky Endpoint Detection and Response Optimum.

Сетевая изоляция устройств, изолированных в результате выполнения задачи *Поиск IOC*, автоматически выключается по истечении заданного периода времени. Вы можете настраивать этот период времени в Web Console в свойствах устройства и в свойствах политики. Параметры сетевой изоляции в свойствах политики в Web Console описаны в Приложении 5. Параметры сетевой изоляции в свойствах управляемого устройства описаны в таблице ниже.

Если на устройство распространяется политика, то применяются параметры, заданные в политике, настройка автоматического выключения сетевой изоляции в свойствах устройства недоступна. Если политика на устройство не распространяется, то применяются параметры, заданные в свойствах устройства.

По умолчанию приложение выключает сетевую изоляцию через 5 часов с момента включения. После выключения сетевой изоляции устройство может работать в сети без ограничений.

Настройка автоматического выключения сетевой изоляции в свойствах устройства

Чтобы настроить автоматическое выключение сетевой изоляции устройства:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и в открывшемся окне выберите группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. Найдите нужное устройство в списке и нажмите на его имя.

4. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Приложения**.

5. В списке приложений, установленных на устройстве, нажмите на название приложения Kaspersky Endpoint Security.

6. В открывшемся окне свойств приложения на вкладке **Параметры приложения** выберите раздел **Detection and Response** и перейдите по ссылке **Endpoint Detection and Response Optimum**.

7. В блоке параметров **Сетевая изоляция** нажмите на ссылку **Настроить разблокировку устройства**.

8. В открывшемся окне **Настройка разблокировки устройства** установите флажок **Разблокировать автоматически изолированное устройство через** и в поле ввода ниже укажите период в часах, по истечении которого устройство будет автоматически разблокировано.

9. Сохраните внесенные изменения.

Настройка параметров сетевой изоляции в ручном режиме

Вы можете вручную изолировать устройство от сети только при интеграции с Kaspersky Endpoint Detection and Response Optimum.

Если вы включаете сетевую изоляцию устройства вручную, вы можете предварительно настроить параметры сетевой изоляции с помощью локальной задачи *Включение сетевой изоляции* (*NetworkIsolationStart*). Вы можете настроить исключения из сетевой изоляции и продолжительность сетевой изоляции устройства.

Задача *Включение сетевой изоляции* является предустановленной и запускается только автоматически в следующих случаях:

- Если вы нажали на кнопку **Изолировать устройство от сети** в свойствах устройства.
- Если вы включили сетевую изоляцию устройства из окна с деталями алерта.

Вы не можете создать новый экземпляр задачи *Включение сетевой изоляции* по кнопке **Добавить** или запустить ее нажатием на кнопку **Запустить**. Задача доступна только в свойствах устройства, где вы можете изменять ее параметры перед включением сетевой изоляции устройства.

Параметры задачи *Включение сетевой изоляции* применяются независимо от того, распространяется ли на устройство действие политики.

Чтобы настроить параметры сетевой изоляции устройства:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите группу администрирования, содержащую нужное вам устройство. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком управляемых устройств, и в открывшемся окне выберите группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. Найдите нужное устройство в списке и нажмите на его имя.

4. В открывшемся окне свойств управляемого устройства перейдите на вкладку **Задачи**.

5. В списке задач нажмите на задачу *Включение сетевой изоляции*.

   Откроется окно со свойствами задачи.

6. Перейдите на вкладку **Параметры приложения**.

7. По ссылке **Настроить исключения** откройте окно **Исключения**.

8. В открывшемся окне с помощью кнопок над таблицей выполните необходимое действие:

   - Если вы хотите добавить информацию об исключаемом сетевом соединении, сделайте это одним из следующих способов:

     - нажмите на кнопку **Добавить** и ввести информацию о сетевом соединении;

     - нажмите на кнопку **Добавить из профиля** и выбрать сетевой профиль из словаря.

   - Если вы хотите удалить информацию об исключаемом сетевом соединении, установите флажок напротив удаляемого сетевого соединения и нажмите на кнопку **Удалить**.

9. Нажмите на кнопку **OK**.

10. Введите необходимую продолжительность сетевой изоляции устройства в часах в поле **Изолировать устройство на**.

    По умолчанию продолжительность сетевой изоляции составляет 5 часов.

    Минимальная продолжительность сетевой изоляции не может быть меньше 1 часа.

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

Настройка исключений из сетевой изоляции в Web Console

При интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response (KATA) или Kaspersky Managed Detection and Response настройка исключений из сетевой изоляции выполняется на стороне соответствующего решения Detection and Response. Подробнее см. в справке Kaspersky Endpoint Detection and Response Expert (on-premises), в справке Kaspersky Anti Targeted Attack Platform или в справке Kaspersky Managed Detection and Response.

При интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Optimum вы можете настраивать исключения из сетевой изоляции следующими способами:

- В свойствах политики в Web Console. Исключения, настроенные в политике, применяются при автоматическом включении сетевой изоляции устройства, находящегося под действием политики.

- В свойствах устройства в Web Console. Исключения, настроенные в свойствах устройства, применяются при автоматическом включении сетевой изоляции устройства, на которое не распространяется политика.

- В параметрах локальной задачи *Включение сетевой изоляции* (*NetworkIsolationStart*). Исключения, настроенные в свойствах этой задачи, применяются при включении сетевой изоляции устройства вручную. Параметры задачи *Включение сетевой изоляции* применяются независимо от того, распространяется ли на устройство действие политики.

Для настройки исключений из сетевой изоляции в приложении доступен список *стандартных сетевых профилей*. Сетевые профили состоят из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент. Вы можете изменять параметры стандартных сетевых профилей и задавать исключения вручную.

> Добавление и удаление исключений из сетевой изоляции в свойствах устройства недоступно, если на устройство распространяется действие политики.

Как добавить исключение из сетевой изоляции в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. В блоке **Сетевая изоляция** нажмите на ссылку **Исключения**.

   Откроется окно со списком исключений из сетевой изоляции.
6. Исключить сетевое соединение возможно следующими способами:
   - Нажмите на кнопку **Добавить** и введите информацию о сетевом соединении.

     > Вы можете добавить приложение, с которым компонент не будет блокировать сетевое соединение. Этот параметр применим на устройствах с версией ядра от 4.18 с поддержкой eBPF с BTF и с включенными функциями tracepoints и kprobes для трассировки ядра.
   - Нажмите на кнопку **Добавить из профиля** и выберите сетевой профиль из словаря.
7. Сохраните внесенные изменения.

Как удалить исключения из сетевой изоляции в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. В блоке **Сетевая изоляция** нажмите на ссылку **Исключения**.

   Откроется окно со списком исключений из сетевой изоляции.
6. Установите флажок напротив нужного сетевого соединения и нажмите на кнопку **Удалить**.
7. Сохраните внесенные изменения.

Помещение файла на карантин

При реагировании на угрозы Kaspersky Endpoint Detection and Response может создавать задачи *Помещение файла на карантин*. Это нужно, чтобы минимизировать последствия угрозы. *Карантин* – это специальное локальное хранилище на компьютере. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства.

Вы можете создавать задачи *Помещение файла на карантин* следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали алерта – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Вы можете выбрать файл, который нужно удалить, прямо из деталей алерта. В результате Kaspersky Endpoint Security запустит мастер создания задач с предустановленными данными об обнаруженном файле. Вам нужно только настроить дополнительные параметры задачи, например, задать расписание запуска задачи.

- С помощью мастера создания задач.

  Мастер создания задач позволяет вручную ввести путь к файлу или путь к директории и хеш файла, который нужно удалить. Также вы можете настроить дополнительные параметры задачи, например, задать расписание запуска задачи.

- В свойствах задачи *Поиск IOC*.

  Если в результате выполнения задачи *Поиск IOC* обнаружен файл, который может вызывать компрометацию данных, то вы можете поместить этот файл на карантин прямо из результатов поиска IOC (**Параметры приложения** → **Результаты поиска IOC**). В результате Kaspersky Endpoint Security запустит мастер создания задач с предустановленными данными об обнаруженном файле. Вам нужно только настроить дополнительные параметры задачи, например, задать расписание запуска задачи.

Размер файла не должен превышать 100 МБ.

Как создать задачу Помещение файла на карантин

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

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

   b. В раскрывающемся списке **Тип задачи** выберите **Помещение файла на карантин**.

   c. В поле **Название задачи** введите короткое описание задачи.

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

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

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

   В списке задач отобразится новая задача.

6. Нажмите на новую задачу.

7. Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. В списке файлов нажмите на кнопку **Добавить**.

   Запустится мастер добавления файла.

10. Для добавления файла вам нужно ввести путь к файлу или путь к директории и хеш файла.

11. В окне свойств задачи выберите вкладку **Расписание**.

12. Настройте расписание запуска задачи.

13. Сохраните внесенные изменения.

14. Установите флажок напротив задачи.

15. Нажмите на кнопку **Запустить**.

    В результате Kaspersky Endpoint Security переместит файл в карантин.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет помещен на карантин только после перезагрузки компьютера. После перезагрузки компьютера убедитесь, что файл удален.

Задача *Помещение файла на карантин* может быть завершена с ошибкой *Доступ запрещен*, если вы пытаетесь поместить на карантин запущенный исполняемый файл. Создайте задачу завершения процесса для этого файла, а затем повторите попытку.

Задача *Помещение файла на карантин* может быть завершена с ошибкой *Недостаточно места в хранилище карантина*, если вы пытаетесь поместить на карантин большой файл. Очистите карантин или увеличьте размер карантина. Затем повторите попытку.

Получение файла с устройства

Вы можете получать файлы с компьютеров пользователей. Например, вы можете настроить получение файла журнала событий, который создает стороннее приложение. В результате выполнения задачи копия файла будет сохранена в карантине. *Карантин* – это специальное локальное хранилище на компьютере. Вы можете загрузить этот файл на компьютер из карантина в Web Console (**Операции** → **Хранилища** → **Карантин**). Оригинал файла на устройстве пользователя остается в исходной директории.

В Kaspersky Security Center в списке файлов на карантине все файлы, полученные через задачу *Получение файла*, будут иметь статус *Заражен* независимо от результатов проверки файла.

Размер файла не должен превышать 100 МБ.

Как создать задачу Получение файла

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

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

   b. В раскрывающемся списке **Тип задачи** выберите **Получение файла**.

   c. В поле **Название задачи** введите короткое описание задачи.

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

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

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

   В списке задач отобразится новая задача.

6. Нажмите на новую задачу.

7. Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. В списке файлов нажмите на кнопку **Добавить**.

   Запустится мастер добавления файла.

10. Для добавления файла вам нужно ввести путь к файлу или путь к директории и хеш файла.

11. В окне свойств задачи выберите вкладку **Расписание**.

12. Настройте расписание запуска задачи.

13. Сохраните внесенные изменения.

14. Установите флажок напротив задачи.

15. Нажмите на кнопку **Запустить**.

    В результате Kaspersky Endpoint Security создаст копию файла и поместит копию в карантин. Вы можете загрузить файл из карантина в Web Console.

Задача *Получение файла* завершается с ошибкой, если:

- указанный файл не найден;
- указаны неверные данные файла (название файла или его контрольная сумма);
- недостаточно прав на выполнение действий с указанным файлом;
- указанный файл заблокирован;
- недостаточно места на карантине;
- указанный файл слишком велик (более 100 МБ).

Удаление файла с устройства

Вы можете удаленно удалять файлы с помощью задачи *Удаление файла*. Например, вы можете удаленно удалить файл при реагировании на угрозы.

Как создать задачу Удаление файла

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

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

   b. В раскрывающемся списке **Тип задачи** выберите **Удаление файла**.

   c. В поле **Название задачи** введите короткое описание задачи.

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

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

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

   В списке задач отобразится новая задача.

6. Нажмите на новую задачу.

7. Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. Для добавления файла вам нужно ввести путь к директории и хеш файла.

10. В окне свойств задачи выберите вкладку **Расписание**.

11. Настройте расписание запуска задачи.

12. Сохраните внесенные изменения.

13. Установите флажок напротив задачи.

14. Нажмите на кнопку **Запустить**.

    В результате Kaspersky Endpoint Security удалит файл с компьютера. Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки компьютера. После перезагрузки компьютера убедитесь, что файл удален.

Запуск процесса

Вы можете удаленно запускать файлы с помощью задачи *Запуск процесса*. Например, вы можете удаленно запускать утилиту, которая создает файл с конфигурацией компьютера. Далее с помощью задачи *Получение файла*, вы можете получить созданный файл в Kaspersky Security Center Web Console.

Если в вашей операционной системе установлена система SELinux в режиме `Enforcing`, то для запуска задачи *Запуск процесса* вам нужно дополнительно настроить систему SELinux.

Как настроить SELinux для запуска задачи Запуск процесса

Если вы планируете использовать в вашей операционной системе систему SELinux в режиме `Enforcing`, для выполнения действий по реагированию при интеграции с решениями Detection and Response вам нужно дополнительно настроить систему SELinux.

Настройку SELinux требуется выполнять с root-правами.

Чтобы настроить систему SELinux для выполнения действий по реагированию:

1. Переведите систему SELinux в неблокирующий режим:

   - Если SELinux активирован, выполните команду:

     Перевести SELinux в неблокирующий режим

     ```
     setenforce Permissive
     ```

   - Если SELinux выключен, в конфигурационном файле /etc/selinux/config задайте значение параметра `SELINUX=permissive` и перезагрузите операционную систему.

2. Убедитесь, что в системе установлена утилита semanage. Если утилита не установлена, установите пакет policycoreutils-python или policycoreutils-python-utils в зависимости от типа менеджера пакетов.

3. Запустите все задачи для выполнения действий по реагированию, которые вы планируете использовать при интеграции приложения с решениями Detection and Response.

4. Убедитесь, что в файле audit.log нет ошибок.

   Посмотреть файл audit.log

   ```
   grep kesl /var/log/audit/audit.log
   ```

5. Если в файле audit.log присутствуют ошибки, создайте и загрузите новый модуль правил на основе блокирующих записей, чтобы устранить ошибки, и снова запустите задачи для выполнения действия по реагированию.

   Создать и загрузить новый модуль правил на основе блокирующих записей

   ```
   grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   semodule -i kesl.pp
   ```

6. Переведите систему SELinux в блокирующий режим.

   ```
   setenforce Enforcing
   ```

Как создать задачу Запуск процесса

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

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

   b. В раскрывающемся списке **Тип задачи** выберите **Запуск процесса**.

   c. В поле **Название задачи** введите короткое описание задачи.

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

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

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

   В списке задач отобразится новая задача.

6. Нажмите на новую задачу.

7. Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. Введите команду запуска процесса:

   - **Исполняемая команда**. Поле ввода команды запуска процесса.

     Например, если вы хотите запустить утилиту `klnagchk`, которая предназначена для проверки подключения к Серверу администрирования, `/opt/kaspersky/klnagent/bin/klnagchk`.

   - **Аргументы командной строки (необязательно)**. Поле ввода аргументов командной строки для передачи дополнительной информации в скрипт, утилиту или приложение при запуске.

     Например, вы можете ввести аргумент `-logfile /tmp/klnagchk.log`. Этот аргумент указывает утилите, что результат работы нужно сохранить в файл с именем `klnagchk.log` в директории `/tmp`. Если вам нужно передать несколько аргументов, требуется разделять их пробелами.

   - **Путь к рабочей папке (необязательно)**. Поле ввода пути к рабочей директории, в которой процесс помещает файлы.

     Например, вы можете ввести значение `/tmp` и запустить утилиту `klnagchk` с аргументами `-logfile klnagchk.log -savecert certificate.cer`. В этом случае оба файла будут созданы в директории `/tmp`.

10. В окне свойств задачи выберите вкладку **Расписание**.

11. Настройте расписание запуска задачи.

12. Сохраните внесенные изменения.

13. Установите флажок напротив задачи.

14. Нажмите на кнопку **Запустить**.

    В результате Kaspersky Endpoint Security выполнит команду в тихом режиме и запустит процесс. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты выполнения**.

Завершение процесса

Вы можете удаленно завершать процессы с помощью задачи *Завершение процесса*. Например, вы можете удаленно завершить процесс, запущенный в результате вредоносной активности.

Если вы хотите запретить запуск файла, вы можете настроить компонент Запрет запуска объектов. Вы можете запретить запуск исполняемых файлов, скриптов, файлов офисного формата.

Как создать задачу Завершение процесса

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

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

   b. В раскрывающемся списке **Тип задачи** выберите *Завершение процесса*.

c. В поле **Название задачи** введите короткое описание задачи.

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

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

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

   В списке задач отобразится новая задача.

6. Нажмите на новую задачу.

7. Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. Для завершения процесса вам нужно выбрать файл, работу которого вы хотите завершить. Вы можете выбрать файл следующими способами:

   - Введите полный путь к файлу.
   - Введите хеш файла и путь к файлу.
   - Введите идентификатор процесса PID (только для локальных задач).
   - Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.

10. В окне свойств задачи выберите вкладку **Расписание**.

11. Настройте расписание запуска задачи.

12. Сохраните внесенные изменения.

13. Установите флажок напротив задачи.

14. Нажмите на кнопку **Запустить**.

    В результате Kaspersky Endpoint Security завершит процесс на компьютере. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты**.

Запрет запуска объектов

Вы можете применить это действие по реагированию при интеграции с решениями Detection and Response от "Лаборатории Касперского", от которых приложение Kaspersky Endpoint Security получает правила запрета запуска.

Если объект соответствует критериям правил, Kaspersky Endpoint Security будет запрещать запуск этого объекта.

Запрет запуска объектов EDR Expert (on-premises)

При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), с Kaspersky Endpoint Detection and Response Expert (cloud) или с Kaspersky Endpoint Detection and Response (KATA) вы можете настроить правила запрета запуска объектов в консоли соответствующего решения.

Если включена интеграция с решением Kaspersky Endpoint Detection and Response Expert (on-premises) или с компонентом Kaspersky Endpoint Detection and Response (KATA), вы можете включать и выключать запрет запуска объектов в свойствах политики (**Параметры приложения** → **Встроенные агенты** → **Endpoint Detection and Response Expert (on-premises)**).

Чтобы включить запрет запуска объектов, переведите переключатель в положение **Запрет запуска ВКЛЮЧЕН**.

Запрета запуска объектов EDR Optimum

При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете настраивать запрет запуска объектов и правила запрета запуска объектов в Web Console.

Как включить Запрет запуска объектов в политике Kaspersky Security Center

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. Перейдите на вкладку **Запрет запуска объектов**.
6. Переведите переключатель в положение **Запрет запуска ВКЛЮЧЕН**.
7. Выберите действие при запуске или открытии объекта:
   - **Заблокировать и записать в журнал событий**. Приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета и записывает в журнал событий событие о попытках запуска объектов или открытия документов.
   - **Записать в журнал событий**. Приложение записывает событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие.
8. Сохраните внесенные изменения.

Как включить Запрет запуска объектов в свойствах управляемого устройства

1. В Web Console перейдите **Управление активами** → **Активы (Устройства)**.
2. Нажмите на ссылку с именем нужного устройства.

3. В открывшемся окне свойств выбранного устройства перейдите на вкладку **Приложения** и нажмите на ссылку <название приложения **Kaspersky Endpoint Security**>.

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

    2. Нажмите на название политики Kaspersky Endpoint Security.

       Откроется окно свойств политики.

    3. Выберите вкладку **Параметры приложения**.

    4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.

    5. Перейдите на вкладку **Запрет запуска объектов**.

    6. Переведите переключатель в положение **Запрет запуска ВКЛЮЧЕН**.

    7. Выберите действие при запуске или открытии объекта:

       - **Заблокировать и записать в журнал событий**. Приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета и записывает в журнал событий событие о попытках запуска объектов или открытия документов.

       - **Записать в журнал событий**. Приложение записывает событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие.

    8. Сохраните внесенные изменения.

4. Выберите вкладку **Параметры приложения**.

5. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.

6. Перейдите в подраздел **Запрет запуска объектов**.

7. Переведите переключатель в положение **Запрет запуска ВКЛЮЧЕН**.

8. Выберите режим работы запрета запуска объекта:

   - **Блокировать**. В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета и записывает в журнал событий событие о попытках запуска объектов или открытия документов.

   - **Информировать**. В этом режиме приложение записывает в журнал событий событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.

9. Сохраните внесенные изменения.

Включение и выключение запрета запуска объектов в свойствах устройства недоступно, если на устройство распространяется действие политики.

Как добавить правило запрета запуска объектов компонента EDR Optimum в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Если необходимо, установите флажок **Учитывать регистр при вводе пути**.
5. В свойствах политики или управляемого устройства нажмите на кнопку **Добавить** в панели инструментов над списком правил запрета запуска объектов.
6. В открывшемся окне введите название правила запрета запуска.
7. Укажите статус работы правила запрета запуска, установив переключатель в соответствующее положение.
8. В раскрывающемся списке **Тип** выберите тип объекта, который вы хотите заблокировать:
   - **Исполняемый файл**.
   - **Скрипт**.
   - **Файл офисного приложения**.

   Если вы выберете неверный тип объекта, приложение не заблокирует файл или скрипт.
9. Для добавления объекта укажите путь к объекту и/или контрольную сумму объекта (хеш SHA256 или MD5 файла) в соответствующем поле.
10. Сохраните внесенные изменения.

    Созданное правило добавлено в перечень правил в блоке параметров **Запрет запуска объектов**.

Kaspersky Endpoint Security контролирует запуск исполняемых файлов и скриптов, а также открытие файлов офисных приложений на устройстве. Запрет запуска объектов поддерживает определенный набор расширений файлов офисных приложений и определенный набор интерпретаторов скриптов. В результате запрета запуска объектов распространение угрозы может быть остановлено.

Функциональность запрета запуска объектов доступна в приложении Kaspersky Endpoint Security при выполнении одного из следующих условий:

- Включена интеграция с решением Kaspersky Endpoint Detection and Response Optimum и активирован компонент EDR Optimum.
- Включена интеграция с решением Kaspersky Endpoint Detection and Response Expert (on-premises) или Kaspersky Endpoint Detection and Response (KATA) и активирован компонент EDR Expert (on-premises).
- Включена интеграция с решением Kaspersky Endpoint Detection and Response Expert (cloud) и активирован компонент EDR Expert (cloud).

Если не включен блокирующий режим перехвата файловых операций, Запрет запуска объектов работает в режиме информирования, независимо от установленного режима работы.

> По умолчанию запрет запуска объектов выключен. Его включение может повлиять на скорость запуска приложений в операционной системе.

Для работы запрета запуска объектов вам нужно включить применение правил запрета запуска объектов.

Ограничения и особенности работы запрета запуска объектов

Ограничения запрета запуска объектов

Существуют следующие ограничения для запрета запуска объектов:

- Приложение Kaspersky Endpoint Security не блокирует объекты, заданные в правилах запрета запуска до запуска приложения.
- Приложение Kaspersky Endpoint Security не блокирует файлы, открытые до создания или изменения правила запрета запуска.
- Приложение Kaspersky Endpoint Security не блокирует работу с объектами, запущенными до создания или изменения правила запрета запуска и подпадающими под вновь заданные правила.
- Некоторые файлы могут быть критически важными для работы операционной системы и приложения. Запрет запуска таких файлов может нарушить работу системы.

Не рекомендуется создавать более 50000 правил запрета запуска, поскольку это может привести к нестабильности системы.

Особенности работы запрета запуска объектов при интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) и Kaspersky Endpoint Detection and Response (KATA)

При интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (on-premises) или с компонентом Kaspersky Endpoint Detection and Response (KATA) приложение использует *правила запрета запуска объектов компонента EDR Expert (on-premises)*. Эти правила приложение получает от Kaspersky Endpoint Detection and Response Expert (on-premises) или Kaspersky Endpoint Detection and Response (KATA).

При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) или Kaspersky Endpoint Detection and Response (KATA) вы можете:

- Включать и выключать применение правил запрета запуска объектов компонента EDR Expert (on-premises) в Web Console или в Консоли администрирования.

  При срабатывании правил запрета запуска приложение Kaspersky Endpoint Security отправляет отчет в Kaspersky Endpoint Detection and Response Expert (on-premises) или Kaspersky Anti Targeted Attack Platform. Подробнее см. в справке соответствующего решения.

- Просматривать в командной строке список правил запрета запуска объектов компонента EDR Expert (on-premises).

Особенности работы запрета запуска объектов при интеграции с Kaspersky Endpoint Detection and Response Optimum

При интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Optimum приложение использует *правила запрета запуска объектов компонента EDR Optimum*. Эти правила вы создаете вручную в Web Console. Вы также можете создавать правила запрета запуска автоматически из окна с деталями алерта.

При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете:

- Включать и выключать применение правил запрета запуска объектов компонента EDR Optimum в Web Console.
- Создавать и настраивать правила запрета запуска объектов компонента EDR Optimum в Web Console.

  Также вы можете создать правило запрета запуска объекта автоматически, запрещая запуск файла в окне с деталями алерта. Правило запрета запуска будет добавлено в политику для группы администрирования, в которую входит устройство.

  > Вы можете запрещать запуск файлов в окне с деталями алерта, только если на устройство распространяется действие политики.

- Просматривать в командной строке список правил запрета запуска объектов компонента EDR Optimum.

При интеграции с Kaspersky Endpoint Detection and Response Optimum запрет запуска объектов может работать в одном из двух режимов:

- **Блокировать**. В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета, и записывает в журнал событие о попытках запуска объектов или открытия документов.

  > Приложение Kaspersky Endpoint Security блокирует выполнение скрипта, запрещенного правилом запрета запуска, даже если он импортирован разрешенным скриптом.

- **Информировать**. В этом режиме приложение записывает в журнал событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.

Работа с карантином

Карантин – это специальное хранилище на устройстве, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения. Карантин позволяет изолировать файл для дальнейшей проверки. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства. В отличие от карантина резервное хранилище предназначено для хранения резервных копий файлов, в которых был обнаружен вредоносный код и которые были удалены или изменены в процессе лечения.

Приложение использует карантин только при интеграции с решениями Detection and Response для выполнения рекомендуемых действий по реагированию на угрозы. При интеграции приложения с Kaspersky Endpoint Detection and Response Optimum или с Kaspersky Managed Detection and Response вы также можете вручную помещать на карантин файлы, которые считаете опасными для вашего устройства.

По умолчанию для хранения файлов, помещенных на карантин, используется директория /var/opt/kaspersky/kesl/common/objects-backup/. В этой директории также хранятся объекты резервного хранилища. Вы можете изменять директорию для хранения объектов резервного хранилища и карантина с помощью командной строки.

Файлы на карантине могут содержать персональные данные. Для доступа к файлам, помещенным на карантин, требуются root-права.

Вы можете настраивать параметры карантина на устройстве с помощью политики в Web Console или в Консоли администрирования или с помощью командной строки. Вы можете настраивать следующие параметры карантина:

- Процент заполнения карантина, при котором формируется событие о заполнении карантина. По умолчанию событие формируется при заполнении карантина на 90%.
- Максимальный размер карантина в мегабайтах. При достижении максимального размера карантина приложение автоматически удаляет из карантина самые старые файлы. По умолчанию максимальный размер карантина 200 МБ, если приложение используется в стандартном режиме или в режиме EDR-Агента, и 100 МБ, если приложение используется в режиме Легкого агента.
- Путь к директории, в которой хранятся объекты резервного хранилища и карантина (этот параметр настраивается только с помощью командной строки).

Как настроить параметры карантина в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Отчеты и хранилище**.
5. В блоке **Карантин** настройте параметры:
   - **Ограничить размер карантина**. Ограничение размера карантина указанным количеством мегабайт. По умолчанию флажок установлен.
   - **Максимальный размер карантина (МБ)**. Если параметр **Ограничить размер карантина** включен, вы можете указать количество мегабайт, которым ограничивается размер карантина (по умолчанию – 200 МБ). Размер карантина не может превышать 999999 МБ.
   - **Уведомлять о заполнении карантина**. Уведомления о заполнении карантина на указанное количество процентов. По умолчанию флажок установлен.

     Вы можете указать процент заполнения карантина, при достижении которого отправляется уведомление (по умолчанию – 90%).
6. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Помещение файлов на карантин

Некоторые файлы могут быть критически важными для работы операционной системы и приложения. Помещение таких файлов на карантин может нарушить работу системы.

Помещение файла на карантин возможно только при выполнении одного из следующих условий:

- Включена интеграция приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Optimum и активирован компонент EDR Optimum.
- Включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (on-premises) или с компонентом Kaspersky Endpoint Detection and Response (KATA) и активирован компонент EDR Expert (on-premises).
- Включена интеграция приложения Kaspersky Endpoint Security с Kaspersky Managed Detection and Response и активирован компонент MDR.

Директория для хранения объектов карантина должна быть доступна для записи.

При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) или с Kaspersky Endpoint Detection and Response (KATA) файлы помещаются на карантин одним из следующих способов:

- В результате выполнения задачи, которая настраивается на стороне соответствующего решения Detection and Response. Подробнее см. в справке Kaspersky Endpoint Detection and Response Expert (on-premises) или в справке Kaspersky Anti Targeted Attack Platform.
- В результате выполнения задачи поиска IOC памяти процессов.

При интеграции с Kaspersky Managed Detection and Response файлы помещаются на карантин одним из следующих способов:

- В результате выполнения задачи, которая настраивается на стороне Kaspersky Managed Detection and Response.
- В результате выполнения команды управления карантином на устройстве.

Подробнее о работе с карантином при интеграции с Kaspersky Managed Detection and Response см. в справке Kaspersky Managed Detection and Response.

При интеграции с Kaspersky Endpoint Detection and Response Optimum файлы помещаются на карантин одним из следующих способов:

- Автоматически в результате обнаружения индикаторов компрометации.
- В результате выполнения задачи *Помещение файла на карантин*, которую вы можете создать в Web Console.
- В результате выполнения команды управления карантином на устройстве.
- В результате выполнения рекомендации из деталей алерта.

Подробнее о работе с карантином при интеграции с Kaspersky Endpoint Detection and Response Optimum см. в справке Kaspersky Endpoint Detection and Response Optimum.

Работа с файлами на карантине

Вы можете работать с файлами, помещенными на карантин:

- В Kaspersky Security Center в общем списке файлов, помещенных на карантин приложениями "Лаборатории Касперского".

  Для выполнения действий с файлами на карантине в Kaspersky Security Center вам нужно включить передачу данных на Сервер администрирования о файлах на карантине.

- Локально на устройстве с помощью командной строки.

Вы можете просматривать информацию о файлах на карантине, удалять и восстанавливать файлы из карантина.

Восстановление, удаление и получение файла из карантина доступно вне зависимости от того, включена ли интеграция с решениями Detection and Response, а также вне зависимости от того, распространяется ли на устройство действие политики.

Общий список файлов, помещенных на карантин приложениями "Лаборатории Касперского" на клиентских устройствах, формируется в Kaspersky Security Center и доступен в Консоли администрирования (**Дополнительно** → **Хранилища** → **Карантин**) и в Web Console (**Операции** → **Хранилища** → **Карантин**). Kaspersky Security Center не копирует файлы из хранилищ карантина на Сервер администрирования, все файлы размещаются в хранилищах карантина на клиентских устройствах. Подробнее о работе с файлами карантина в Kaspersky Security Center см. в справке Kaspersky Security Center.

Файл, помещенный на карантин, восстанавливается в исходное местоположение согласно заданным параметрам. Мандатная метка (только на устройствах под управлением операционных систем Astra Linux) и атрибуты (в том числе immutable и append-only) исходного файла сохраняются при восстановлении. Файл с атрибутами immutable и append-only может быть восстановлен только в заданное местоположение, в котором исходный файл отсутствует, или в исходное местоположение, но с другим именем. Для восстановления файла из карантина в другую директорию или в исходное местоположение с другим именем требуются root-права.

После завершения восстановления приложение удаляет копию восстановленного файла из карантина.

Восстановление файла из карантина завершается с ошибкой в следующих случаях:

- Восстанавливаемый файл не найден в хранилище карантина.
- Имя восстанавливаемого файла указано с ошибкой или в неверном регистре.
- Идентификатор файла указан с ошибкой.
- Директория назначения удалена, перемещена, переименована или у вас нет прав доступа к ней.

  В этом случае приложение перемещает файл в директорию /var/opt/kaspersky/kesl/common/restored/. Вы можете вручную переместить файл из этой директории в нужную директорию.

- По указанному пути уже существует одноименный файл.
- Недостаточно места на устройстве.

- Только на устройствах под управлением операционных системы Astra Linux: мандатная метка файла выше мандатной метки директории, в которую восстанавливается файл.
- Только на устройствах под управлением операционных системы Astra Linux: мандатная метка файла ниже мандатной метки директории, в которую восстанавливается файл, и для директории не установлен флаг ccnr.

Удаление файла из карантина завершается с ошибкой в следующих случаях:

- Удаляемый файл не найден в хранилище карантина.
- Имя удаляемого файла указано с ошибкой или в неверном регистре.
- Идентификатор файла указан с ошибкой.

Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum – решение, предназначенное для защиты ИТ-инфраструктуры организации от таких угроз, как эксплойты (англ. exploits), программы-вымогатели (англ. ransomware), бесфайловые атаки (англ. fileless attacks) и использование злоумышленниками законных системных инструментов для нанесения вреда устройствам или данным.

Приложение Kaspersky Endpoint Security 12.5 для Linux совместимо с решением Kaspersky Endpoint Detection and Response Optimum версии 3.1.

Интеграцию Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Optimum обеспечивает компонент приложения Kaspersky Endpoint Security – Endpoint Detection and Response Optimum (далее также *EDR Optimum*).

Для централизованного управления приложением Kaspersky Endpoint Security с компонентом EDR Optimum используйте Kaspersky Security Center Windows 15.1 или Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.

Компонент недоступен для устройств с процессором Эльбрус.

Как работает Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum выполняет мониторинг и анализ развития угрозы, а также предоставляет сотруднику службы безопасности или администратору информацию о потенциальной атаке, необходимую для принятия своевременных действий по реагированию.

Kaspersky Endpoint Detection and Response Optimum использует следующие средства анализа угроз (Threat Intelligence):

- Инфраструктура облачных служб Kaspersky Security Network (далее также KSN), предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-сайтов и программного обеспечения.
- Интеграция с порталом Kaspersky Threat Intelligence Portal, который содержит и отображает информацию о репутации файлов и веб-сайтов.
- База угроз "Лаборатории Касперского" Kaspersky Threats.

При взаимодействии с Kaspersky Endpoint Detection and Response Optimum приложение Kaspersky Endpoint Security может выполнять следующие функции:

- Отправлять в Kaspersky Security Center данные о событиях на устройствах. Приложение Kaspersky Endpoint Security передает в Kaspersky Security Center данные наблюдения за процессами, открытыми сетевыми соединениями и изменяемыми файлами, а также данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.
- Выполнять действия по реагированию, направленные на обеспечение функций безопасности, по командам, полученным от Kaspersky Security Center.

Настройка интеграции с Kaspersky Endpoint Detection and Response Optimum

Предварительные требования

Перед началом настройки интеграции с Kaspersky Endpoint Detection and Response Optimum:

- Добавьте в приложение лицензионный ключ EDR Optimum, если вы приобрели отдельную лицензию на использование этой функциональности.

  При использовании приложения Kaspersky Endpoint Security по лицензии, которая включает в себя функциональность Kaspersky Endpoint Detection and Response Optimum, действие не требуется.

  > Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, лицензионный ключ добавляется на SVM.

- Убедитесь, что включены и работают:
  - Kaspersky Security Network в стандартном или расширенном режиме.

    > Для наиболее эффективной работы Kaspersky Endpoint Detection and Response Optimum рекомендуется использовать Kaspersky Security Network в расширенном режиме.

  - следующие компоненты приложения Kaspersky Endpoint Security:
    - Защита от файловых угроз.
    - Анализ поведения.

Для полноты отправляемой телеметрии и для построения цепочки развития угроз в Kaspersky Security Center требуется дополнительно включить Защиту от веб-угроз.

Вы также можете включить запрет запуска объектов.

Основные этапы настройки

1. **Установите плагин управления Kaspersky Endpoint Detection and Response Optimum**

   Плагин управления Kaspersky Endpoint Detection and Response Optimum является единым плагином для работы с агентами на операционных системах Windows, Mac и Linux и требуется для отображения и просмотра деталей алертов. Описание процедуры установки см. в справке решения Kaspersky Endpoint Detection and Response Optimum.

   Если в вашей инфраструктуре для управления Kaspersky Endpoint Detection and Response Optimum используется Kaspersky Security Center Cloud Console, плагин установлен по умолчанию.

2. **Настройте параметры интеграции с Kaspersky Endpoint Detection and Response Optimum**

   Вы можете выполнить настройку:

   - С помощью Web Console (консоль Kaspersky Security Center и/или консоль OSMP).
   - С помощью командной строки.

   > Управление компонентом EDR Optimum с помощью Консоли администрирования Kaspersky Security Center не поддерживается.

3. **Включите передачу данных на Сервер администрирования**

   Для использования всех возможностей Kaspersky Endpoint Detection and Response Optimum вам нужно настроить следующие параметры:

   - Включить отправку в хранилище Kaspersky Security Center информации о файлах в резервном хранилище и на карантине. Для этого вам нужно в свойствах политики установить флажки:
     - **О файлах резервного хранилища**.
     - **О файлах карантина**.
   - Разрешить отображение списка алертов. Для этого вам нужно включить переключатель **Показать EDR-алерты** в главном окне Web Console в разделе **Параметры** → **Параметры интерфейса**.

     > Параметр **Показать EDR-алерты** отсутствует в Web Console версии ниже 15.1. Переход к EDR-алертам доступен из Отчета об угрозах в консоли Kaspersky Security Center.

   - Включить передачу данных о событиях сторонних приложений на управляемых устройствах. Для этого на управляемом устройстве выполните команду:

     ```
     kesl-control --set-app-settings SystemEventsTransmission=Yes
     ```

     > Включение этого параметра может значительно увеличить нагрузку на операционную систему.

4. **Убедитесь, что подключение к Kaspersky Endpoint Detection and Response Optimum выполнено успешно**

Проверьте статус работы Kaspersky Endpoint Detection and Response Optimum удобным для вас способом. Интеграция с Kaspersky Endpoint Detection and Response Optimum настроена. При обнаружении угрозы формируется алерт. В окне с деталями алерта вы можете просмотреть информацию об угрозе и выполнить действия по реагированию.

Как включить интеграцию с EDR Optimum

В Web Console вы можете включать и выключать компонент EDR Optimum, а также настраивать параметры интеграции с Kaspersky Endpoint Detection and Response Optimum в свойствах политики.

Как включить интеграцию с Kaspersky Endpoint Detection and Response Optimum в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. Включите переключатель **Endpoint Detection and Response ВКЛЮЧЕН**.
6. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Как включить интеграцию с Kaspersky Endpoint Detection and Response Optimum в командной строке

Для включения компонента EDR Optimum выполните команду:

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

1. В главном окне Web Console выберите раздел **Управление активами** → **Активы (Устройства)**.
2. Нажмите на ссылку с именем нужного устройства.
3. В открывшемся окне свойств выбранного устройства перейдите на вкладку **Приложения** и нажмите на ссылку <название приложения Kaspersky Endpoint Security>.
4. Перейдите на вкладку **Параметры приложения,** нажмите на раздел **Detection and Response**, далее нажмите на ссылку **Endpoint Detection and Response Optimum**.
5. В открывшемся окне переведите переключатель в положение **Endpoint Detection and Response Optimum включен**, чтобы включить интеграцию.

6. При необходиомсти задайте следующие настройки:

- Длительность блокировки устройства при автоматической сетевой изоляции.

  Нажмите на ссылку **Настроить разблокировку устройства** и укажите время блокировки.

- Исключения из автоматической сетевой изоляции.

7. Сохраните изменения.

Управляемое устройство настроено для интеграции с Kaspersky Endpoint Detection and Response Optimum.

Как проверить, что интеграция с EDR Optimum включена и работает

Ознакомьтесь с информацией о возможных статусах интеграции и условиях их отображения.

Способы проверки работы компонента EDR Optimum:

- В командной строке с помощью команды:

  ```
  kesl-control --app-info
  ```

  Интеграция с EDR Optimum отображается со статусом **Выполняется**.

- В Web Console:

  - С помощью *Отчета о статусе компонентов приложения*. Подробную информацию о работе с отчетами см. в справке Kaspersky Security Center.

  - Перейдите в раздел **Управление активами** → **Активы** → ссылка <имя устройства> → вкладка **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → вкладка **Общие** → **Компоненты**.

    Компонент Endpoint Detection and Response Optimum отображается со статусом **Выполняется**.

Cloud Sandbox

Cloud Sandbox – технология, которая позволяет обнаруживать сложные угрозы на компьютере. Kaspersky Endpoint Security автоматически отправляет обнаруженные файлы в Cloud Sandbox для анализа. Cloud Sandbox запускает эти файлы в изолированной среде для выявления вредоносной активности и принимает решение о репутации этих файлов. Далее данные об этих файлах попадают в Kaspersky Security Network. Таким образом, если Cloud Sandbox обнаружил вредоносный файл, Kaspersky Endpoint Security выполнит действие для устранения угрозы на всех компьютерах, на которых обнаружит этот файл.

Для работы Cloud Sandbox необходимо включить использование Kaspersky Security Network.

Если вы используете Kaspersky Private Security Network, технология Cloud Sandbox недоступна.

Технология Cloud Sandbox включена постоянно и доступна всем пользователям Kaspersky Security Network независимо от типа лицензии, которую вы используете. Если у вас развернуто решение Endpoint Detection and Response Optimum, вы можете включить отдельный счетчик для угроз, обнаруженных с помощью Cloud Sandbox. Вы можете использовать этот счетчик для составления статистики при анализе обнаруженных угроз. Kaspersky Endpoint Security будет указывать технологию обнаружения угроз Cloud Sandbox в *Отчет об угрозах* в консоли Kaspersky Security Center.

Как включить счетчик Cloud Sandbox в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response**.
5. Выберите вкладку **Cloud Sandbox**.
6. Включите переключатель **Использование Cloud Sandbox ВКЛЮЧЕНО**.
7. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Detection and Response Expert (on-premises) – решение для кибербезопасности бизнеса, позволяющее защититься от большинства киберрисков и покрыть основные сценарии распространения угроз. Компоненты Kaspersky Endpoint Detection and Response Expert (on-premises) развертываются на единой платформе управления Open Single Management Platform (OSMP). Подробнее о решении и платформе см. в справке Kaspersky Endpoint Detection and Response Expert (on-premises).

Интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premises) обеспечивает компонент приложения Kaspersky Endpoint Security – Endpoint Detection and Response Expert (on-premises) (далее также *EDR Expert (on-premises)*).

Компонент недоступен для устройств с процессором Эльбрус.

Как работает Endpoint Detection and Response Expert (on-premises)

1. **Устройства с Kaspersky Endpoint Security устанавливают защищенные соединения с сервером действий по реагированию OSMP и с сервером сбора телеметрии OSMP**
2. **Приложение Kaspersky Endpoint Security отправляет данные на сервер сбора телеметрии на платформе OSMP**

Передается следующая информация:

- данные о событиях на устройстве;
- данные об угрозах, обнаруженных приложением;
- данные о результатах обработки этих угроз;
- данные наблюдения за процессами, открытыми сетевыми соединениями и изменяемыми файлами.

3. **Приложение Kaspersky Endpoint Security выполняет действия по реагированию**

   Действия по реагированию выполняются по командам, полученным от сервера действий по реагированию на платформе OSMP.

Настройка интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises)

Предварительные требования

Перед началом настройки интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises):

- Разрешите подключение через порты 443 и 8443.
- Включите компонент Анализ поведения для передачи необходимых данных телеметрии.

  Если вы хотите получать данные об обнаружении угроз от других компонентов защиты, включите эти компоненты.

  - Защита от файловых угроз.
  - Защита от сетевых угроз.
  - Защита от веб-угроз.
  - Защита от шифрования.
  - Контроль приложений.
  - Контроль устройств.
  - Контроль целостности системы.

  > При использовании механизма eBPF для получения системной телеметрии в компоненте Анализ поведения (доступном на 64-битных операционных системах с версией ядра 4.18 и выше с поддержкой eBPF) данные телеметрии будут более полными.

- Добавьте в приложение лицензионный ключ EDR Expert (on-premises), если вы приобрели отдельную лицензию на использование этой функциональности.

  При использовании приложения Kaspersky Endpoint Security по лицензии, которая включает в себя функциональность Kaspersky Endpoint Detection and Response Expert (on-premises), действие не требуется.

Если приложение используется в режиме Легкого агента, лицензионный ключ EDR Expert (on-premises) добавляется на SVM.

- Также в платформе OSMP должны быть настроены коллектор, коррелятор и хранилище.

Основные этапы настройки

1. **Получите и обработайте сертификаты, выданные серверами OSMP**

   Во время интеграции с решением Kaspersky Endpoint Detection and Response Expert (on-premises) устройства с Kaspersky Endpoint Security устанавливают защищенные соединения по протоколу HTTPS с сервером действий по реагированию OSMP и с сервером сбора телеметрии OSMP.

   > Если в общих параметрах приложения Kaspersky Endpoint Security настроено использование прокси-сервера, то для подключения к серверам OSMP используется прокси-сервер.

   Сертификаты для защиты соединения с серверами OSMP предоставляет администратор платформы OSMP.

   Для обработки сертификатов выполните действия, описанные в статье Преобразование сертификата из формата PFX в формат PEM.

   Вы можете использовать Сертификат сервера и/или Сертификат клиента. Выбор определяется политикой безопасности вашей организации.

2. **Настройте параметры интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Вы можете выполнить настройку:

   - С помощью Web Console (консоль Kaspersky Security Center и/или консоль OSMP).
   - С помощью командной строки.

   Если вы хотите использовать функциональность запрета запуска объектов, вы можете включить применение правил запрета запуска объектов компонента EDR Expert (on-premises).

3. **Убедитесь, что подключение к платформе Endpoint Detection and Response Expert (on-premises) выполнено успешно**

   Проверьте статус работы EDR Expert (on-premises) удобным для вас способом.

4. **При необходимости выполните дополнительные настройки**

   - Если в вашей операционной системе установлена система SELinux в режиме Enforcing, то для выполнения действий по реагированию вам нужно дополнительно настроить систему SELinux.
   - Для выполнения действий по реагированию **Дамп памяти**, **Дамп процесса** отключите запрет трассировки ptrace.
   - Ознакомьтесь с ограничениями сетевой изоляции.

- Включите передачу данных о событиях сторонних приложений на управляемых устройствах. Для этого на управляемом устройстве выполните команду:

  ```
  kesl-control --set-app-settings SystemEventsTransmission=Yes
  ```

  Включение этого параметра может значительно увеличить нагрузку на операционную систему.

Как подготовить эталонный образ для корректной интеграции с EDR Expert (on-premises)

Перед подготовкой образа убедитесь, что на эталонном устройстве нет файла `/var/opt/kaspersky/.ids_generated`.

Чтобы подготовить эталонный образ для корректной интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), выполните следующие действия:

Не перезагружайте эталонное устройство и не перезапускайте приложение Kaspersky Endpoint Security во время выполнения инструкции.

1. Выполните следующие команды от имени пользователя root:

   ```
   systemctl stop kesl
   systemctl edit kesl
   ```

2. В открывшемся редакторе добавьте одну из следующих конфигураций между строками `### Anything between here and the comment below will become the contents of the drop-in file` и `### Edits below this comment will be discarded`:

   - Обновление SensorID при каждом запуске приложения на временных виртуальных машинах

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -a
     ```

   - Однократное обновление SensorID на постоянных виртуальных машинах

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -b
     ```

3. Сохраните изменения и закройте редактор.

   В результате будет создан файл `/etc/systemd/system/kesl.d/override.conf`. Проверьте, что его содержимое соответствует добавленной конфигурации.

4. Перезагрузите службу systemd, выполнив команду:

   ```
   systemctl daemon-reload
   ```

5. Создайте файл `/usr/bin/uuid-regen.sh` со следующим содержимым:

```
#!/usr/bin/env bash
# ------------------------------------------------------------
#  Kaspersky IDs updater
#  Modes:
#    -a   Always regenerate the IDs (default)
#    -b   Generate them only once – subsequent runs do nothing
#  Exit code: always 0
# ------------------------------------------------------------
set -euo pipefail
# ----- configuration ------------------------------------------------
PCID_FILE="/var/opt/kaspersky/kesl/common/pcid"
INSTALL_ID_FILE="/var/opt/kaspersky/epagent/install_id"
KESL_INI="/var/opt/kaspersky/kesl/common/kesl.ini"
# Marker that shows the script has already been executed in mode b
MARKER="/var/opt/kaspersky/.ids_generated"
# ----- default mode -------------------------------------------------
MODE="a"
# ----- parse command-line arguments ---------------------------------
while getopts ":ab" opt; do
   case $opt in
       a) MODE="a" ;;
       b) MODE="b" ;;
       \?) echo "Invalid option: -$OPTARG" >&2; exit 0 ;;
   esac
done
shift $((OPTIND-1))
# ----- helper: generate a new UUID and write to a file ---------------
write_uuid() {
   local target=$1
   /usr/bin/uuidgen > "$target"
}
# ----- helper: replace MachineId in kesl.ini -------------------------
replace_machine_id() {
   local new_id
   new_id=$(/usr/bin/uuidgen)
   /usr/bin/sed -i "s/^MachineId=.*/MachineId=${new_id}/" "$KESL_INI"
}
# ----- main logic ----------------------------------------------------
if [[ "$MODE" == "b" && -f "$MARKER" ]]; then
   # Mode b – already ran once → do nothing
   :
else
   # (re)generate all required values
   write_uuid "$PCID_FILE"
   write_uuid "$INSTALL_ID_FILE"
   replace_machine_id
   # In mode b remember that we have already executed
   if [[ "$MODE" == "b" ]]; then
       /usr/bin/touch "$MARKER"
   fi
fi
exit 0
```

6. Измените права доступа к файлу `/usr/bin/uuid-regen.sh` с помощью команды:

```
chmod 700 /usr/bin/uuid-regen.sh
```

Эталонное устройство готово к созданию образа операционной системы.

Как настроить интеграцию с EDR Expert (on-premises)

В Web Console вы можете включать и выключать компонент EDR Expert (on-premises) и настраивать интеграцию приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Expert (on-premises) в свойствах политики Kaspersky Endpoint Security.

Как настроить интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises) в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response Expert (on-premises)**.
5. Выберите опцию **Endpoint Detection and Response Expert (версия 8.0 и выше)**.
6. Добавьте серверы сбора телеметрии и серверы реагирования.

   Для этого в разделах **Подключение к серверам сбора телеметрии** и **Подключение к серверам реагирования** нажмите на кнопку **Добавить**. В открывшемся окне укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.
7. Добавьте сертификаты, нажав на ссылку **Настройки подключения** в разделах **Подключение к серверам сбора телеметрии** и **Подключение к серверам реагирования**, а затем в открывшейся панели выполните следующие действия:

   a. Добавьте сертификат сервера, нажав в одноименном разделе на кнопку **Загрузить**.

   b. При необходимости дополнительной защиты сформируйте криптоконтейнер.

      Для этого в разделе **Дополнительная защита подключения**:

      1. Установите флажок **Использовать двустороннюю аутентификацию**.
      2. Нажмите на кнопку **Загрузить** и добавьте сертификат клиента, который вы получили при выполнении основного сценария интеграции.
      3. Укажите пароль от криптоконтейнера в соответствующем поле.

      > Поле **Пароль от криптоконтейнера** является обязательным. Если пароль для сертификата клиента (криптоконтейнера) не указан, вы не сможете сохранить настройки.
8. Для применения политики на компьютерах закройте замки 🔒, сохраните внесенные изменения.

Как настроить интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises) в командной строке

1. Для добавления сертификата сервера реагирования выполните команду:

   ```
   kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
   ```
2. Для добавления сертификата сервера телеметрии выполните команду:

   ```
   kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
   ```

3. Для настройки параметров интеграции выполните команду:

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

Параметры и их возможные значения приведены в таблице ниже.

4. Для добавления сертификата клиента для подключения к серверу реагирования выполните команду:

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
```

5. Для добавления сертификата клиента для подключения к серверу телеметрии выполните команду:

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
```

6. Для включения интеграции с EDR Expert (on-premises) выполните команду:

```
kesl-control --start-task 24
```

Параметры интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises)

Параметр	Описание	Значение
`Mode`	Режим интеграции. Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) приложение Kaspersky Endpoint Security взаимодействует с серверами на платформе OSMP. Для интеграции с Kaspersky Endpoint Detection and Response (KATA) приложение Kaspersky Endpoint Security взаимодействует с серверами на платформе Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (значение по умолчанию) – режим интеграции EDR (KATA). Позволяет включить интеграцию с Kaspersky Endpoint Detection and Response (KATA), компонентом Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` – режим интеграции EDR Expert (on-premises). Позволяет включить интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premises).
`UseClientPinnedCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу действий по реагированию OSMP. Если двусторонняя аутентификация включена на стороне сервера действий по реагированию OSMP, вам нужно включить двустороннюю аутентификацию в параметрах задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* и добавить сертификат клиента перед запуском задачи.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу действий по реагированию OSMP. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`SynchronizationPeriod`	Периодичность отправки запросов на синхронизацию на сервер действий по реагированию OSMP в минутах.	Значение по умолчанию: `5`.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером действий по реагированию OSMP в секундах.	Значение по умолчанию: `10`.
`RequestTimeout`	Максимальное время ожидания ответа от сервера действий по реагированию OSMP в секундах.	Значение по умолчанию: `10`.
`EnableTelemetry`	Отправка данных о событиях на устройствах (телеметрии) на сервер сбора телеметрии OSMP.	`Yes` (значение по умолчанию) – отправлять телеметрию на сервер сбора телеметрии OSMP. `No` – не отправлять телеметрию.
Секция **[Endpoints.item_#]** содержит адрес и порт сервера действий по реагированию OSMP. Вы можете добавить несколько серверов.		

Параметр	Описание	Значение
`Address`	Адрес сервера действий по реагированию OSMP. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера.	Значение по умолчанию: `127.0.0.1`.
`Port`	Порт для подключения к серверу действий по реагированию OSMP.	Значение по умолчанию: `443`.
Секция **[TelemetrySettings]** содержит общие параметры подключения к серверам сбора телеметрии OSMP.		
`UseClientPinnedCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу сбора телеметрии OSMP. Если двусторонняя аутентификация включена на стороне сервера сбора телеметрии OSMP, вам нужно включить двустороннюю аутентификацию в параметрах задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert* и добавить сертификат клиента перед*(on-premises)* запуском задачи.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу сбора телеметрии OSMP. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером сбора телеметрии OSMP в секундах.	Значение по умолчанию: `10`.
`RequestTimeout`	Максимальное время ожидания ответа от сервера сбора телеметрии OSMP в секундах.	Значение по умолчанию: `10`.
`OnlyTaggedEvents`	Отправка телеметрии только с IOA. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию *потоковой проверки*, которая позволяет отслеживать такие события в режиме реального времени.	`Yes` – отправлять только телеметрию с индикатором атаки (Indicator of Attack, IOA). `No` (значение по умолчанию) – отправлять всю телеметрию.
Секция **[TelemetrySettings.Endpoints.item_#]** содержит адрес и порт сервера сбора телеметрии OSMP. Вы можете добавить несколько серверов.		
`Address`	Адрес сервера сбора телеметрии OSMP. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера.	Значение по умолчанию: `127.0.0.1`.
`Port`	Порт для подключения к серверу сбора телеметрии OSMP.	Значение по умолчанию: `443`.
Секция **[TelemetrySettings.EventTransferSettings]** содержит параметры передачи данных на сервер сбора телеметрии OSMP.		
`MaximumDataTransferTime`	Максимальная задержка отправки событий на сервер сбора телеметрии OSMP в секундах.	Значение по умолчанию: `30`.
`UseRequestCountLimits`	Регулирование количества запросов. Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события.	`Yes` (значение по умолчанию) – регулировать количество отправляемых событий. `No` – не регулировать количество событий.
`MaximumNumberOfEventsInHour`	Максимальное количество событий в час.	Значение по умолчанию: `3000`.
`MaximumNumberOfEventsInPackage`	Максимальное количество событий в одном пакете.	Значение по умолчанию: `1024`.
`EventLimitExceededPercentage`	Процент превышения ограничения на количество событий. Передача событий ограничивается, если соотношение событий одного типа к общему количеству событий превышает установленное ограничение в процентах.	Значение по умолчанию: `15`.

Для параметров интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) в политиках вложенного уровня иерархии предусмотрена возможность задавать собственные значения, даже если все

остальные параметры политики наследуются.

Если в родительской политике включена интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises) и включено наследование параметров в дочерней политике, то по умолчанию параметры интеграции в дочерней политике тоже наследуются и недоступны для изменения. Если вы хотите настроить собственные параметры интеграции, в раскрывающемся списке выберите вариант **Использовать собственные настройки подключения**. Параметры интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) станут доступными для изменения.

Если вы используете Web Console или командную строку, для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) вам нужно выбрать режим интеграции EDR (on-premises) в параметрах компонента EDR Expert (on-premises):

- Если вы используете Web Console, в параметрах политики выберите вариант **Endpoint Detection and Response Expert (версия 8.0 и выше)**. Чтобы настраивать интеграцию с Kaspersky Endpoint Detection and Response (on-premises) на устройстве, в Web Console требуется настроить "замки" для обеих версий (версия 8.0 и выше и версия 7.1 и ниже).

- Если вы используете командную строку, в параметрах задачи установите значение параметра `Mode=EDRExpertOnPrem`.

Как проверить, что интеграция с EDR Expert (on-premises) включена и работает

Способы проверки работы компонента EDR Expert (on-premises):

- В командной строке с помощью команды:

  ```
  kesl-control --app-info
  ```

- В Web Console.

  - В консоли Kaspersky Security Center:

    С помощью *Отчета о статусе компонентов приложения*. Подробную информацию о работе с отчетами см. в справке Kaspersky Security Center.

  - В консоли OSMP:

    - С помощью *Отчета о статусе компонентов приложения*.

    - Перейдите в раздел **Управление активами** → **Активы**, выберите вкладку **Анализ и реагирование**.

      Устройство отображается в списке со статусом телеметрии **Нормальная активность**.

    - Перейдите в раздел **Поиск угроз**.

      События телеметрии с требуемого устройства отображаются в списке событий.

Endpoint Detection and Response Expert (cloud)

Интеграция Kaspersky Endpoint Security для Linux с решением Kaspersky Endpoint Detection and Response Expert (cloud) временно недоступна. Поддержка функциональности запланирована на конец 2026 года. Следите за нашими Release Notes, чтобы быть в курсе обновлений приложения и новых возможностей.

Kaspersky Endpoint Security для Linux поддерживает работу с решением Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* – облачное решение для кибербезопасности бизнеса, которое включает в себя приложения "Лаборатории Касперского", с помощью которых организация получает возможность защититься от большинства киберрисков и покрыть основные сценарии распространения угроз. Компоненты EDR Expert (cloud) развернуты на единой платформе управления Open Single Management Platform (OSMP). Платформа обеспечивает выполнение кросс-программных сценариев в рамках единого интерфейса и позволяет интегрировать приложения "Лаборатории Касперского" и приложения сторонних производителей в единую систему безопасности.

Один из центральных элементов решения – *SIEM*. SIEM позволяет отслеживать события, полученные от всех компонентов, и выполняет взаимную корреляцию этих событий с помощью готовых и пользовательских правил. На основании журналов и телеметрии, полученных от инфраструктуры организации, EDR Expert (cloud) автоматически выявляет атаки и позволяет проводить расследование инцидентов с помощью единого графа расследования, который комбинирует все собираемые в EDR Expert (cloud) события – как от приложений "Лаборатории Касперского", так и от сторонних ИБ-продуктов.

Для реагирования на сложные инциденты EDR Expert (cloud) использует предустановленные и пользовательские сценарии. Также доступны действия по реагированию от приложений сторонних производителей и сценарии реагирования, в которых задействовано несколько приложений.

Средства анализа угроз

Kaspersky Endpoint Detection and Response использует следующие средства анализа угроз (Threat Intelligence):

- Интеграция с Kaspersky Threat Intelligence Portal, который содержит и отображает информацию о репутации файлов и веб-адресов.
- База угроз "Лаборатории Касперского" Kaspersky Threats.
- Инфраструктура облачных служб Kaspersky Security Network (далее также "KSN"), предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Принцип работы решения

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами.

Данные о событиях на компьютере (телеметрия) отправляются на сервер EDR Expert (cloud). Приложение Kaspersky Endpoint Security также передает на сервер сбора телеметрии данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

Настройка интеграции с EDR Expert (cloud) выполняется в консоли Kaspersky Security Center. Дальнейшее управление встроенным агентом осуществляется в единой платформе управления OSMP, включая запуск задач, управление объектами на карантине, просмотр отчетов и другие действия.

Ограничения в работе EDR Expert (cloud)

- Kaspersky Endpoint Security не поддерживает интеграцию с EDR Expert (cloud) в режиме Легкого агента.
- EDR Expert (cloud) недоступен для устройств с процессором Эльбрус.
- На устройствах на базе архитектуры Arm не поддерживается использование EDR Expert (cloud).
- EDR Expert (cloud) недоступен на компьютерах под управлением 64-битных операционных систем.

Как настроить интеграцию встроенного агента с EDR Expert (cloud)

Для интеграции с решением Kaspersky Endpoint Detection and Response Expert (cloud) вам нужно включить компонент Endpoint Detection and Response Expert (cloud) и настроить подключение к серверу сбора телеметрии и серверу реагирования.

Сервер сбора телеметрии – сервер, входящий в состав SIEM, который предназначен для сбора, нормализации, корреляции, анализа и хранения данных о событиях на компьютере.

Сервер реагирования – сервер, который предназначен для приема и проверки данных, исследования поведения объектов, а также публикации результатов исследования.

> Компоненты *Endpoint Detection and Response Expert (cloud)* и *Endpoint Detection and Response Expert (on-premises)* несовместимы между собой.

Условия работы EDR Expert (cloud)

Для работы EDR Expert (cloud) должны быть выполнены следующие условия:

- Инфраструктура Kaspersky Endpoint Detection and Response Expert (cloud) доступна в вашем регионе. Для получения информации о доступности инфраструктуры EDR Expert (cloud) в вашем регионе обратитесь в Службу технической поддержки.
- Установлена единая платформа управления OSMP (Open Single Management Platform).
- Приложение Kaspersky Endpoint Security установлено в стандартном режиме.
- Приложение Kaspersky Endpoint Security активировано и функциональность входит в лицензию.
- Вы приняли условия Соглашения об обработке данных Kaspersky Endpoint Detection and Response Expert (cloud).
- Включен компонент Endpoint Detection and Response Expert (cloud).
- Включен компонент Анализ поведения для передачи необходимых данных телеметрии.

  Если вы хотите получать данные об обнаружении угроз от других компонентов защиты, включите эти компоненты.

  - Защита от файловых угроз.
  - Защита от сетевых угроз.
  - Защита от веб-угроз.
  - Защита от шифрования.
  - Контроль приложений.
  - Контроль устройств.
  - Контроль целостности системы.

Этапы интеграции с EDR Expert (cloud)

Интеграция с EDR Expert (cloud) состоит из следующих этапов:

1. **Выбор режима работы EDR Expert**

   Kaspersky Endpoint Security поддерживает работу с EDR Expert в двух режимах: on-premise и cloud. Для интеграции с решением Kaspersky Endpoint Detection and Response Expert (cloud) вам нужно включить соответствующий режим во время установки приложения. По умолчанию приложение использует интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises).

2. **Активация Kaspersky Endpoint Detection and Response Expert (cloud)**

   Вам нужно приобрести отдельную лицензию на использование Kaspersky Endpoint Detection and Response Expert (cloud).

Функциональность будет доступна после добавления отдельного ключа Kaspersky Endpoint Detection and Response Expert (cloud). В результате на компьютере будет добавлено два ключа: ключ для Kaspersky Endpoint Security и ключ для Kaspersky Endpoint Detection and Response Expert (cloud).

Лицензирование отдельной функциональности Endpoint Detection and Response Expert (cloud) не отличается от лицензирования Kaspersky Endpoint Security.

Убедитесь, что функциональность EDR Expert (cloud) включена в лицензию и работает в Kaspersky Security Center или на защищаемом устройстве.

3 **Настройка подключения к серверу сбора телеметрии и серверу реагирования**

Для работы Kaspersky Endpoint Detection and Response Expert (cloud) необходимо установить доверенное соединение между Kaspersky Endpoint Security и двумя серверами: сервером сбора телеметрии и сервером реагирования. Приложение получает адреса серверов и сертификаты для установки доверенного соединения автоматически после принятия условий Соглашения об обработке данных Kaspersky Endpoint Detection and Response Expert (cloud). Таким образом, вам нужно только настроить дополнительные параметры для подключения к серверам: использование TCP-туннеля и период отправки запроса на синхронизацию с сервером.

Как настроить дополнительные параметры для подключения Kaspersky Endpoint Security к EDR Expert (cloud) в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response Expert (cloud)**.
5. Включите компонент с помощью переключателя **Endpoint Detection and Response Expert (cloud) ВЫКЛЮЧЕН**.
6. Если текущая политика является дочерней, и в родительской политике установлен запрет на изменение параметров интеграции с EDR Expert (cloud) ("замок" закрыт), вы можете настроить наследование параметров в блоке **Наследование**:
   - **Наследовать настройки подключения из политики** (значение по умолчанию). Параметры подключения будут унаследованы из родительской политики. Редактирование параметров будет недоступно.
   - **Использовать собственные настройки подключения**. Вы можете настроить параметры подключения самостоятельно.
7. На вкладке **Сервер реагирования** отображаются автоматически полученные полное доменное имя и порт сервера реагирования. Если политика безопасности в вашей инфраструктуре не позволяет подключаться к серверам EDR Expert (cloud) напрямую, вы можете настроить подключение через TCP-туннель:
   a. Установите флажок **Использовать TCP-туннель для реагирования**.
   b. Укажите адрес сервера (IPv4, IPv6), а также порт подключения к туннелю.
8. Если необходимо, настройте период отправки запросов на синхронизацию с сервером в поле **Отправлять запрос на синхронизацию на сервер каждые (мин.)**. Во время синхронизации Kaspersky Endpoint Security получает задачи по реагированию на угрозы и отправляет результаты выполнения задач.

9. Перейдите на вкладку **Сервер сбора телеметрии**.

10. Настройте параметры подключения к серверу сбора телеметрии:

    a. Нажмите на ссылку **Изменить**.

    b. В открывшемся окне выберите сервер сбора телеметрии из списка. Роль сервера сбора телеметрии в EDR Expert (cloud) выполняет коллектор KUMA. Подробнее см. в справке Kaspersky Unified Monitoring and Analysis Platform.

    Если при подключении к серверу сбора телеметрии возникла ошибка, выберите другой сервер. Если вам не удалось выполнить подключение к серверу сбора телеметрии, обратитесь в Службу технической поддержки.

    c. При необходимости вы можете вы можете настроить подключение к серверу сбора телеметрии через TCP-туннель, как для сервера реагирования.

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

Как посмотреть информацию о сертификатах в командной строке

1. Для просмотра информации о сертификате клиента выполните команду:

```
kesl-control --query-cloudxdr-client-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-client-certificate --server-type response
```

2. Для просмотра информации о сертификате сервера выполните команду:

```
kesl-control --query-cloudxdr-server-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-server-certificate --server-type response
```

В результате Kaspersky Endpoint Security покажет информацию о сертификате в следующем виде:

```
Serial number: 12 34 56 78 AB CD EF GH
Subject: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Issuer: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Valid from: 2022-07-27 13:25:35
Expires on: 2072-07-14 13:25:35
SHA1 fingerprint: a14f12df23fg3465bgh6345g567df
```

Проверьте статус работы компонента с помощью отчета *Отчет о статусе компонентов приложения*. Также вы можете посмотреть статус работы компонента на защищаемом устройстве.

Как оптимизировать отправку телеметрии EDR Expert (cloud)

Телеметрия – список событий, которые произошли на защищаемом компьютере. Kaspersky Endpoint Security анализирует данные телеметрии и отправляет их на серверы сбора телеметрии во время синхронизации. События телеметрии поступают на сервер почти непрерывно. Kaspersky Endpoint Security выполняет синхронизацию с сервером при выполнении любого из следующих условий:

- Истек период синхронизации.
- Количество событий в буфере превысило максимальное значение.

Таким образом, по умолчанию приложение выполняет синхронизацию каждые 30 секунд или при накоплении в буфере 1024 события. Вы можете настроить параметры синхронизации в политике Kaspersky Endpoint Security и выбрать оптимальные значения исходя из нагрузки на сеть (см. инструкцию ниже).

Если соединение между Kaspersky Endpoint Security и сервером отсутствует, то приложение ставит новые события в очередь. При восстановлении соединения Kaspersky Endpoint Security отправляет события из очереди на сервер по порядку. При этом, чтобы не перегрузить сервер, Kaspersky Endpoint Security может отправлять не все события. Для этого вы можете оптимизировать параметры отправки событий и, например, задать максимальное количество событий в час (см. инструкцию ниже).

Как оптимизировать отправку телеметрии в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response Expert (cloud)**.
5. В открывшемся окне перейдите на вкладку **Настройка передачи данных**.
6. Убедитесь, что установлен флажок **Отправка телеметрии ВКЛЮЧЕНА**.
7. Если требуется, включите функцию **Отправлять телеметрию только с IOA**. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию *потоковой проверки*, которая позволяет отслеживать такие события в режиме реального времени. По умолчанию функция выключена.
8. Если требуется, настройте параметры синхронизации с сервером:
   - **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд.
   - **Максимальное количество пакетов событий**. Приложение выполняет синхронизацию с сервером при заполнении буфера событиями. По умолчанию установлено значение 1024 события.
9. Перейдите на вкладку **Регулирование количества запросов**.

10. Если требуется, выключите регулирование количества запросов с помощью переключателя **Регулирование количества запросов ВКЛЮЧЕНО**.

    Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события. По умолчанию функция включена.

11. Настройте параметры оптимизации отправки событий на сервер:

    - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

    - **Процент превышения лимита событий (%)**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Endpoint Security восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.

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

Как оптимизировать отправку телеметрии в командной строке

1. Для включения отправки телеметрии выполните команду:

```
kesl-control --set-settings 39 [EnableTelemetry=<Yes|No>] [TelemetrySettings.OnlyTaggedEvents=<Yes|No>]
```

2. Для настройки параметров синхронизации с сервером выполните команду:

```
kesl-control --set-settings 39 [TelemetrySettings.EventTransferSettings.UseRequestCountLimits=<Yes|No>]
[TelemetrySettings.EventTransferSettings.MaximumDataTransferTime=<delay in sending events in seconds>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInHour=<number of events>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInPackage=<number of event packages>]
[TelemetrySettings.EventTransferSettings.EventLimitExceededPercentage=<percentage of exceeding the event
limit>]
```

Параметры интеграции с Kaspersky Endpoint Detection and Response Expert (cloud)

Параметр	Описание
`EnableTelemetry`	Отправка данных о событиях на устройствах (телеметрии) на сервер сбора телеметрии OSMP. По умолчанию отправка телеметрии включена (`Yes`).
`TelemetrySettings.OnlyTaggedEvents`	Отправка телеметрии только с IOA. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию *потоковой проверки*, которая позволяет отслеживать такие события в режиме реального времени. По умолчанию отправка телеметрии только с IOA выключена (`No`).
Секция `[TelemetrySettings.EventTransferSettings]` содержит общие параметры подключения к серверам сбора телеметрии OSMP.	
`UseRequestCountLimits`	Регулирование количества запросов. Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события. По умолчанию функция включена.

Параметр	Описание
`MaximumDataTransferTime`	Максимальная задержка отправки событий (сек.). Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд.
`MaximumNumberOfEventsInHour`	Максимальное количество событий в час. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.
`MaximumNumberOfEventsInPackage`	Максимальное количество событий в пакете. Приложение выполняет синхронизацию с сервером при заполнении буфера событиями. По умолчанию установлено значение 1024 события.
`EventLimitExceededPercentage`	Процент превышения лимита событий (%). Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Endpoint Security восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.

Как настроить исключения из телеметрии EDR Expert (cloud)

Для повышения производительности и оптимизации отправки данных на Сервер сбора телеметрии вы можете добавить исключения из телеметрии. Например, вы можете отменить обработку данных о сетевых коммуникациях для отдельных приложений.

Использование слишком большого количества правил может привести к увеличению нагрузки на Сервер сбора телеметрии и снижению производительности компьютера. Рекомендуется добавлять только необходимые правила.

Чтобы создать исключение из телеметрии в Web Console, выполните следующие действия:

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки телеметрии**.
5. Выберите вкладку **Телеметрия EDR Expert (cloud)**.
6. В блоке **Общие исключения** нажмите на кнопку **Добавить**.

   Откроется форма для добавления правила исключения из телеметрии.
7. Настройте правило исключений из телеметрии:

   a. При необходимости измените статус правила. По умолчанию правило включено.

   b. Введите имя правила.

c. Выберите действие, которое будет выполнено при срабатывании правила:

- **Не собирать**. Отфильтрованное событие будет исключено из отправляемой телеметрии.
- **Исключить IOA**. Из отправляемой телеметрии будет исключено событие о срабатывании IOA-правила. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию *потоковой проверки*, которая позволяет отслеживать такие события в режиме реального времени.

d. Если выбран вариант **Исключить IOA**, укажите IOA-правила, которые необходимо добавить в исключения:

- **Исключить все**. При выполнении заданного условия приложение будет исключать из телеметрии события, формируемые на основе всех IOA-правил.
- **Исключить по GUID**. Укажите GUID IOA-правила. Вы можете указать несколько GUID через `,`. Подробную информацию об IOA-правилах см. в справке EDR Expert (cloud).

e. Задайте условия фильтрации.

При необходимости вы можете формировать сложные критерии фильтрации, добавляя несколько условий фильтрации и групп условий, с помощью операторов **И**, **ИЛИ**, **НЕ**. Также в группу условий вы можете добавлять вложенные условия и группы условий.

8. Если требуется, в блоке **Все типы событий** добавьте исключения из телеметрии по типу событий:

a. Нажмите на название типа события.

b. В открывшемся окне нажмите на кнопку **Настроить вручную**.

c. В блоке **Правила исключения** нажмите на кнопку **Добавить**.

Откроется форма для добавления правила исключения из телеметрии. В правиле исключения из телеметрии уже предустановлено условие фильтрации `EventType`, которое соответствует типу события.

d. Задайте условия фильтрации.

9. Для применения политики на компьютерах убедитесь, что закрыты замки 🔒, и сохраните внесенные изменения.

Как экспортировать / импортировать фильтры событий EDR Expert (cloud)

Вы можете экспортировать список исключений в файл в формате JSON. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество идентификаторов событий. Также вы можете использовать функцию экспорта / импорта для резервного копирования фильтров событий или для миграции списка на другой сервер.

> Использование слишком большого количества правил может привести к увеличению нагрузки на Сервер сбора телеметрии и снижению производительности компьютера. Рекомендуется добавлять только необходимые правила.

Чтобы экспортировать / импортировать фильтры событий в Web Console, выполните следующие действия:

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Настройки телеметрии**.
5. Выберите вкладку **Телеметрия EDR Expert (cloud)**.
6. Для экспорта фильтров событий выполните следующие действия:

   a. Нажмите на кнопку **Экспортировать**.

   b. В открывшемся окне введите имя файла формата JSON, в который вы хотите экспортировать фильтры событий, а также выберите папку, в которой вы хотите сохранить этот файл.

   c. Сохраните файл.

   Kaspersky Endpoint Security экспортирует фильтры событий в JSON-файл.
7. Для импорта фильтров событий выполните следующие действия:

   a. Нажмите на кнопку **Импортировать**.

   b. В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать фильтры событий.

   c. Выберите способ импорта правил фильтрации событий: добавить к существующим правилам или заменить существующие правила на новые.

   d. Откройте файл.
8. Для применения политики на компьютерах убедитесь, что закрыты замки 🔒, и сохраните внесенные изменения.

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

      Откроется окно свойств политики.
   3. Выберите вкладку **Параметры приложения**.
   4. Перейдите в раздел **Общие настройки** → **Настройки телеметрии**.
   5. Выберите вкладку **Телеметрия EDR Expert (cloud)**.
   6. Для экспорта фильтров событий выполните следующие действия:

      a. Нажмите на кнопку **Экспортировать**.

      b. В открывшемся окне введите имя файла формата JSON, в который вы хотите экспортировать фильтры событий, а также выберите папку, в которой вы хотите сохранить этот файл.

c. Сохраните файл.

Kaspersky Endpoint Security экспортирует фильтры событий в JSON-файл.

7. Для импорта фильтров событий выполните следующие действия:

a. Нажмите на кнопку **Импортировать**.

b. В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать фильтры событий.

c. Выберите способ импорта правил фильтрации событий: добавить к существующим правилам или заменить существующие правила на новые.

d. Откройте файл.

8. Для применения политики на компьютерах убедитесь, что закрыты замки, и сохраните внесенные изменения.

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform – решение для защиты ИТ-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats (далее также "APT"). Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform.

Приложение Kaspersky Endpoint Security может интегрироваться со следующими компонентами на платформе Kaspersky Anti Targeted Attack Platform:

Kaspersky Endpoint Detection and Response (KATA)

Компонент обеспечивает защиту устройств в локальной сети организации. При интеграции с Kaspersky Endpoint Detection and Response (KATA) приложение Kaspersky Endpoint Security выполняет следующие функции:

- Отправляет данные о событиях на устройствах (телеметрию) на сервер с компонентом Central Node, который обеспечивает взаимодействие с Kaspersky Endpoint Detection and Response (KATA) (далее также *сервер KATA*).

  Приложение Kaspersky Endpoint Security передает на сервер с компонентом Central Node данные наблюдения за процессами, открытыми сетевыми соединениями и изменяемыми файлами, а также данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

- Выполняет действия по реагированию, направленные на обеспечение функций безопасности, по командам, полученным от Kaspersky Anti Targeted Attack Platform.

Поддерживается интеграция с Kaspersky Endpoint Detection and Response (KATA) версии 7.1 и ниже.

Network Detection and Response (KATA)

Компонент обеспечивает защиту внутренней сети предприятия. При интеграции с Kaspersky Network Detection and Response (KATA) приложение Kaspersky Endpoint Security может отправлять данные о событиях на устройствах (телеметрию) на сервер с компонентом Central Node, обеспечивающий взаимодействие с Kaspersky Network Detection and Response (KATA) (далее также *сервер NDR*).

Sandbox

Приложение Kaspersky Endpoint Security отправляет файлы на проверку на сервер с компонентом Central Node, обеспечивающий взаимодействие с Sandbox.

Интеграцию на платформе Kaspersky Anti Targeted Attack Platform обеспечивают следующие компоненты приложения Kaspersky Endpoint Security:

- Endpoint Detection and Response Expert (on-premises), далее также *EDR Expert (on-premises)*.

  Начиная с версии Kaspersky Endpoint Security 12.4 для Linux компонент Endpoint Detection and Response (KATA) переименован в Endpoint Detection and Response Expert (on-premises). Теперь этот компонент обеспечивает интеграцию не только с Kaspersky Endpoint Detection and Response (KATA), компонентом Kaspersky Anti Targeted Attack Platform, но и с решением Kaspersky Endpoint Detection and Response Expert (on-premises).

- Network Detection and Response (KATA), далее также *NDR (KATA)*.

- Sandbox.

Вы можете настроить интеграцию приложения Kaspersky Endpoint Security как со всеми компонентами решения Kaspersky Anti Targeted Attack Platform, так и с каждым компонентом по отдельности.

Компонент недоступен для устройств с процессором Эльбрус.

Настройка интеграции с Kaspersky Anti Targeted Attack Platform

Предварительные требования

Перед началом настройки интеграции с компонентом Kaspersky Network Detection and Response (KATA) разрешите подключение через порт 8085.

Перед началом настройки интеграции с компонентом Kaspersky Endpoint Detection and Response (KATA):

- Разрешите подключение через порты 443, 8443.

- Включите компонент Анализ поведения для передачи необходимых данных телеметрии.

  Компонент Анализ поведения доступен на устройствах с версией ядра 3.13 и выше.

  Если вы хотите получать данных об обнаружении угроз от других компонентов защиты, включите эти компоненты:

  - Защита от файловых угроз.

  - Защита от сетевых угроз.

  - Защита от веб-угроз.

- Защита от шифрования.
- Контроль приложений.
- Контроль устройств.
- Контроль целостности системы.

Данные телеметрии будут более полными при включении режима перехвата сетевого трафика eBPF. Технология eBPF доступна на компьютерах под управлением 64-битных операционных систем с версией ядра 4.18 и выше с поддержкой eBPF.

> Рекомендуем проверить, поддерживает ли компьютер компоненты, необходимые для передачи данных телеметрии.

- Добавьте в приложение лицензионный ключ EDR Expert (on-premises), если вы приобрели отдельную лицензию на использование этой функциональности.

  При использовании приложения Kaspersky Endpoint Security по лицензии, которая включает в себя функциональность Kaspersky Endpoint Detection and Response Expert (on-premises), действие не требуется.

  > Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, лицензионный ключ для активации дополнительной функциональности добавляется на SVM.

Основные этапы настройки

1. **Получите и обработайте сертификаты, выданные серверами Central Node**

   Во время интеграции с решением Kaspersky Anti Targeted Attack Platform устройства с Kaspersky Endpoint Security устанавливают защищенные соединения по протоколу HTTPS с компонентом Central Node, обеспечивающими интеграцию.

   > Если в общих параметрах приложения Kaspersky Endpoint Security настроено использование прокси-сервера, то для подключения к серверам, обеспечивающими взаимодействие с компонентами решения Kaspersky Anti Targeted Attack Platform, используется прокси-сервер.

   Сертификаты для защиты соединения с серверами, обеспечивающими взаимодействие с компонентами решения Kaspersky Anti Targeted Attack Platform предоставляет администратор Kaspersky Anti Targeted Attack Platform.

   Для обработки сертификатов выполните действия, описанные в статье Преобразование сертификата из формата PFX в формат PEM.

   Вы можете использовать Сертификат сервера и/или Сертификат клиента. Выбор определяется политикой безопасности вашей организации.

2. **Настройте параметры интеграции с Kaspersky Anti Targeted Attack Platform**

Вы можете выполнить настройку:

- С помощью Web Console (EDR (KATA) и NDR (KATA) в консоли Kaspersky Security Center и/или консоли OSMP).
- С помощью Консоли администрирования Kaspersky Security Center (EDR (KATA) и NDR (KATA)).
- С помощью командной стройки (EDR (KATA) и NDR (KATA)).

3. **Убедитесь, что подключение к Kaspersky Anti Targeted Attack Platform выполнено успешно**

   Проверьте статус работы компонентов Kaspersky Anti Targeted Attack Platform удобным для вас способом.

4. **При необходимости выполните дополнительные настройки**

   - Если в вашей операционной системе установлена система SELinux в режиме Enforcing, то для выполнения действий по реагированию вам нужно дополнительно настроить систему SELinux.
   - Ознакомьтесь с ограничениями сетевой изоляции.

Как настроить интеграцию с EDR (KATA)

В Web Console вы можете включать и выключать компонент Kaspersky Endpoint Detection and Response (KATA), а также настраивать интеграцию приложения Kaspersky Endpoint Security с этим компонентом.

Как настроить интеграцию с Kaspersky Endpoint Detection and Response (KATA) в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. В открывшемся окне свойств политики выберите вкладку **Параметры приложения**.
5. Перейдите в раздел **Встроенные агенты** → **Endpoint Detection and Response Expert (on-premises)**.
6. В правой части экрана выполните следующие действия:

   a. Выберите опцию **Endpoint Detection and Response Expert (версия 7.1 и ниже)**.

   b. В разделе **Подключение к серверам сбора телеметрии** выберите сервер сбора телеметрии, нажав на кнопку **Добавить** в панели инструментов, а затем нажмите **Выбрать сервер**.

   c. В разделе **Подключение к серверам реагирования** выберите сервер реагирования, нажав на кнопку **Добавить** в панели инструментов, а затем нажмите **Выбрать сервер**.

   d. Нажмите на ссылку **Настройки подключения** в разделах **Подключение к серверам сбора телеметрии** и **Подключение к серверам реагирования**, а затем в открывшейся панели выполните следующие действия:

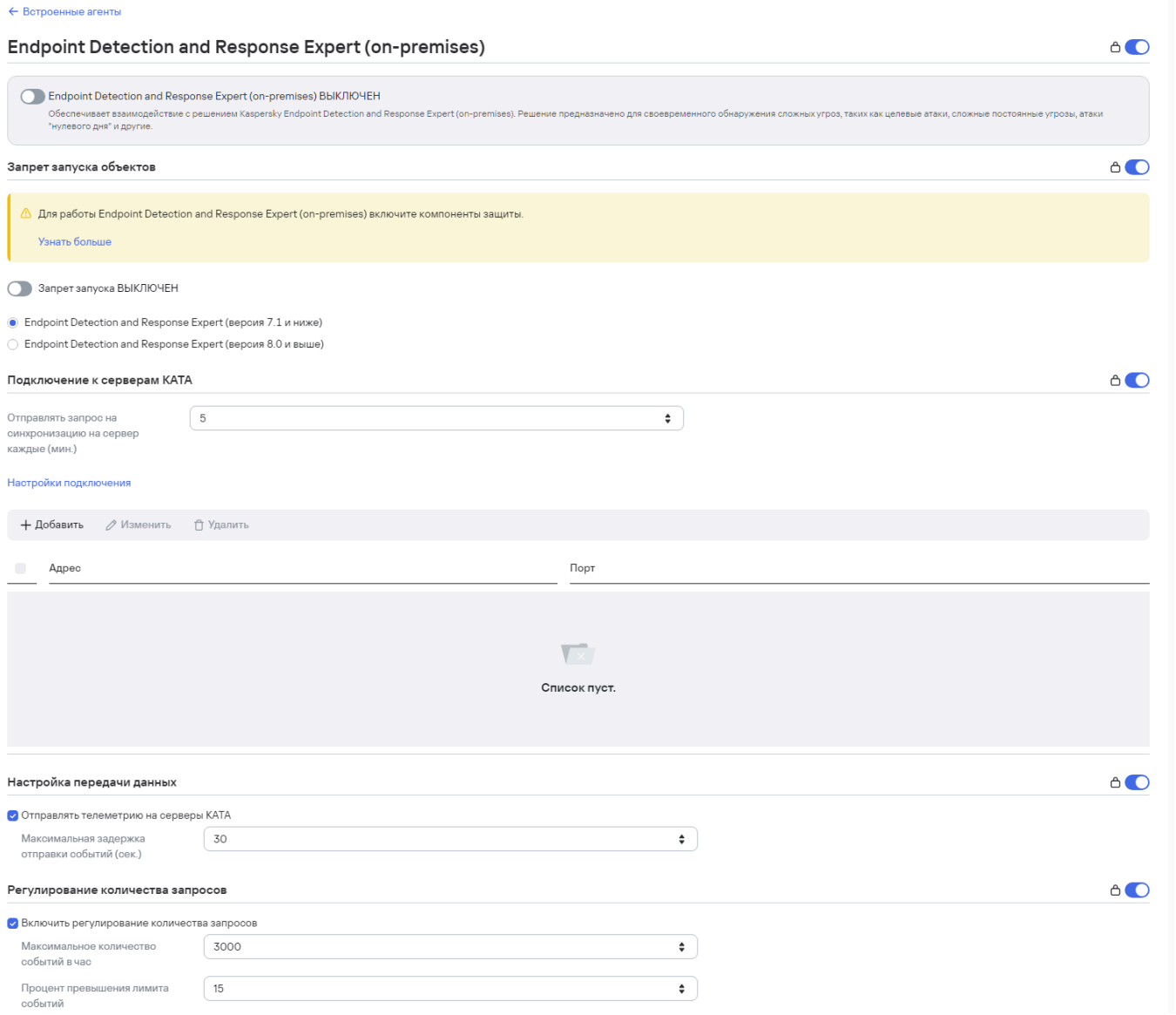
      1. Добавьте сертификат сервера, нажав на кнопку **Загрузить**.
      2. При необходимости дополнительной защиты сформируйте криптоконтейнер.

Для этого в разделе **Дополнительная защита подключения**:

- Установите флажок **Использовать двустороннюю аутентификацию**.
- Нажмите на кнопку **Загрузить** и добавьте сертификат клиента, который вы получили на шаге 1 основного сценария.
- Укажите пароль от криптоконтейнера в соответствующем поле.

> Поле **Пароль от криптоконтейнера** является обязательным. Если пароль для сертификата клиента (криптоконтейнера) не указан, вы не сможете сохранить настройки.

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



Endpoint Detection and Response Expert (on-premises)

Как настроить интеграцию с Kaspersky Endpoint Detection and Response (KATA) в командной строке

1. Для выбора режима интеграции с EDR (KATA) выполните команду:

```
kesl-control --set-settings 24 Mode=EDRKATA
```

2. Для добавления сервера Central Node выполните команду:

```
kesl-control --set-settings 24 Endpoints.item_001.Address=<central node server address>
Endpoints.item_001.Port=<central node server port>
```

3. Для добавления сертификата сервера реагирования выполните команду:

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

4. Для настройки параметров интеграции выполните команду:

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

Параметры и их возможные значения приведены в таблице ниже.

5. Для добавления сертификата клиента для подключения к серверу реагирования выполните команду:

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

6. Для включения интеграции с EDR (KATA) выполните команду:

```
kesl-control --start-task 24
```

Параметры интеграции с Kaspersky Endpoint Detection and Response (KATA)

Параметр	Описание	Значение
`Mode`	Режим интеграции. Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) приложение Kaspersky Endpoint Security взаимодействует с серверами на платформе OSMP. Для интеграции с Kaspersky Endpoint Detection and Response (KATA) приложение Kaspersky Endpoint Security взаимодействует с серверами на платформе Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (значение по умолчанию) – режим интеграции EDR (KATA). Позволяет включить интеграцию с Kaspersky Endpoint Detection and Response (KATA), компонентом Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` – режим интеграции EDR Expert (on-premises). Позволяет включить интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premises).
`UseClientPinnedCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу KATA. Если двусторонняя аутентификация включена на стороне сервера KATA, вам нужно включить двустороннюю аутентификацию в параметрах задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* и добавить сертификат клиента перед запуском задачи.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу KATA. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`SynchronizationPeriod`	Периодичность отправки запросов на синхронизацию на сервер KATA в минутах.	Значение по умолчанию: `5`.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером KATA в секундах.	Значение по умолчанию: `10`.
`RequestTimeout`	Максимальное время ожидания ответа от сервера KATA в секундах.	Значение по умолчанию: `10`.
`EnableTelemetry`	Отправки данных о событиях на устройствах (телеметрии) на KATA.	`Yes` (значение по умолчанию) – отправлять телеметрию на сервер KATA. `No` – не отправлять телеметрию.
Секция **[Endpoints.item_#]** содержит адрес и порт сервера KATA. Вы можете добавить несколько серверов.		

Параметр	Описание	Значение
`Address`	Адрес сервера KATA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера.	Значение по умолчанию: `127.0.0.1`.
`Port`	Порт для подключения к серверу KATA.	Значение по умолчанию: `443`.
Секция **[EventTransferSettings]** содержит параметры передачи данных на сервер KATA.		
`MaximumDataTransferTime`	Максимальная задержка отправки событий на сервер KATA в секундах.	Значение по умолчанию: `30`.
`UseRequestCountLimits`	Включение и выключение регулирования количества событий, отправляемых на сервер KATA.	`Yes` (значение по умолчанию) – регулировать количество отправляемых событий. `No` – не регулировать количество событий.
`MaximumNumberOfEventsInHour`	Максимальное количество событий в час.	Значение по умолчанию: `3000`.
`MaximumNumberOfEventsInPackage`	Максимальное количество событий в одном пакете.	Значение по умолчанию: `1024`.
`EventLimitExceededPercentage`	Процент превышения ограничения на количество событий. Передача событий ограничивается, если соотношение событий одного типа к общему количеству событий превышает установленное ограничение в процентах.	Значение по умолчанию: `15`.

Если вы используете Web Console или командную строку, для интеграции с Kaspersky Endpoint Detection and Response (KATA) вам нужно выбрать режим интеграции *EDR (KATA)* в параметрах компонента EDR Expert (on-premises):

- Если вы используете Web Console, в параметрах политики выберите вариант **Endpoint Detection and Response Expert (версия 7.1 и ниже)**. Чтобы настраивать интеграцию с Kaspersky Endpoint Detection and Response (KATA) на устройстве, в Web Console требуется настроить "замки" для обеих версий (версия 8.0 и выше и версия 7.1 и ниже).

- Если вы используете командную строку, в параметрах задачи установите значение параметра `Mode=EDRKATA`.

Как настроить интеграцию с NDR (KATA)

В Web Console вы можете включать и выключать компонент Kaspersky Network Detection and Response (KATA), а также настраивать интеграцию приложения Kaspersky Endpoint Security с этим компонентом.

Как настроить интеграцию с Kaspersky Network Detection and Response (KATA) в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Встроенные агенты** → **Network Detection and Response (KATA)**.

5. Включите переключатель **Network Detection and Response (KATA)**.

6. Нажмите на кнопку **Настройки подключения**.

7. Настройте параметры подключения к серверам:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу Central Node.

   - **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

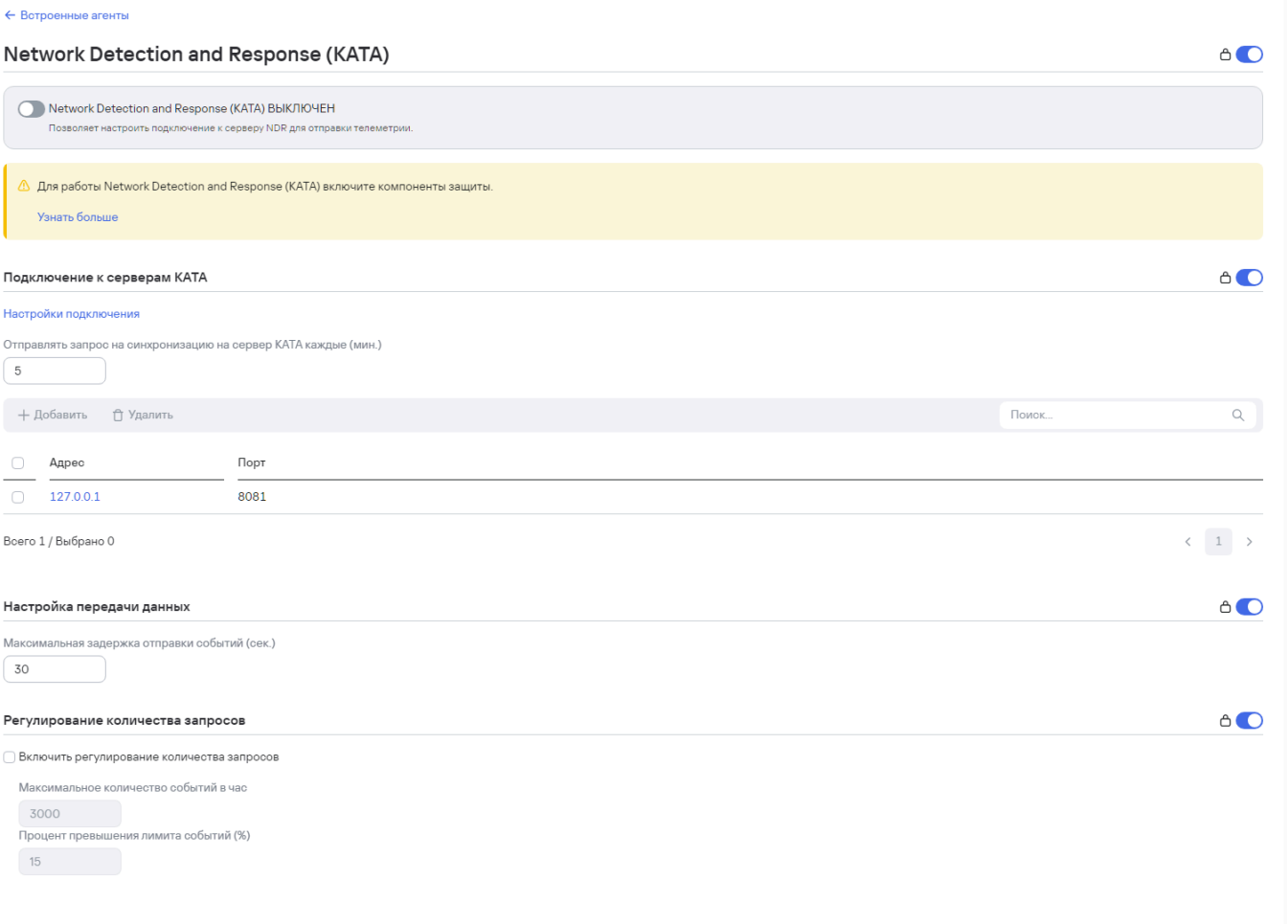
     Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

8. Нажмите на кнопку **OK**.

9. Добавьте серверы Central Node. Для этого укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.

10. Вы можете добавить несколько адресов сервера Central Node. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.

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



Network Detection and Response (KATA)

Как настроить интеграцию с Kaspersky Network Detection and Response (KATA) в командной строке

1. Для добавления сервера Central Node выполните команду:

```
kesl-control --set-settings 31 Endpoints.item_001.Address=<cenral node server address> Endpoints.item_001.Port=
<central node server port>
```

2. Для добавления сертификата сервера реагирования выполните команду:

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

3. Для настройки параметров интеграции выполните команду:

```
kesl-control --set-settings 31 [<setting name>=<setting value>]
```

Параметры и их возможные значения приведены в таблице ниже.

4. Для добавления сертификата клиента для подключения к серверу реагирования выполните команду:

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

5. Для включения интеграции с NDR (KATA) выполните команду:

```
kesl-control --start-task 31
```

Параметры задачи Интеграция с Kaspersky Network Detection and Response (KATA)

Параметр	Описание	Значение
`UseClientPinnedCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу NDR. Если проверка сертификата клиента включена на стороне сервера NDR, вам нужно включить использование сертификата клиента и добавить сертификат клиента перед запуском задачи *Интеграция с Kaspersky Network Detection and Response (KATA)*.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу NDR. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`SynchronizationPeriod`	Периодичность отправки запросов на синхронизацию на сервер NDR в минутах.	Значение по умолчанию: `5`.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером NDR в секундах.	Значение по умолчанию: `10`.
`RequestTimeout`	Максимальное время ожидания ответа от сервера NDR в секундах.	Значение по умолчанию: `10`.
Секция **[Endpoints.item_#]** содержит адрес и порт сервера NDR.		
`Address`	Адрес сервера NDR. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера.	Значение по умолчанию: `127.0.0.1`.
`Port`	Порт для подключения к серверу NDR.	Значение по умолчанию: `8081`.
Секция **[EventTransferSettings]** содержит параметры передачи событий на сервер NDR.		
`MaximumDataTransferTime`	Максимальная задержка отправки событий на сервер NDR в секундах.	Значение по умолчанию: `30`.
`MaximumNumberOfEventsInPackage`	Максимальное количество событий в одном пакете.	Значение по умолчанию: `1024`.
`UseRequestCountLimits`	Включение и выключение регулирования количества событий, отправляемых на сервер NDR.	`Yes` (значение по умолчанию) – регулировать количество отправляемых событий. `No` – не регулировать количество событий.
`MaximumNumberOfEventsInHour`	Максимальное количество событий в час.	Значение по умолчанию: `3000`.
`EventLimitExceededPercentage`	Процент превышения лимита событий. Передача событий ограничивается, если соотношение событий одного типа к общему количеству событий превышает установленное ограничение в процентах.	Значение по умолчанию: `15`.
`PingPeriod`	Периодичность опроса серверов NDR в секундах.	Значение по умолчанию: `450`.

Как проверить, что интеграция с KATA включена и работает

Вы можете проверить работу компонентов Kaspersky Anti Targeted Attack Platform следующими способами:

- В командной строке с помощью команды:

```
kesl-control --app-info
```

Интеграция с компонентами EDR (on-premises) и NDR (KATA) отображается со статусом **Задача доступна и выполняется**.

- В Web Console:
  - В консоли Kaspersky Security Center с помощью *Отчета о статусе компонентов приложения*. Подробную информацию о работе с отчетами см. в справке Kaspersky Security Center.
  - В консоли OSMP:
    - С помощью *Отчета о статусе компонентов приложения*.
    - Перейдите в раздел **Управление активами** → **Активы**, выберите вкладку **Анализ и реагирование**.

      Устройство отображается в списке со статусом телеметрии **Нормальная активность**.
    - Перейдите в раздел **Поиск угроз**.

      События телеметрии с требуемого устройства отображаются в списке событий.
- В Kaspersky Anti Targeted Attack Platform:

  Перейдите в раздел **Активы** → **Устройства**. Устройства отображаются в таблице. При необходимости вы можете отфильтровать таблицу по значениям: **Приложение EPP**, **Подключение EPP**, **Последнее соединение с EPP**.

  При нажатии на имя нужного устройства отображается панель. В разделе **Endpoint Agent** статус подключения **Активное**.

Sandbox

Технология Sandbox позволяет выполнять на специальных серверах с развернутыми виртуальными образами операционных систем анализ и проверку объектов для выявления вредоносной активности и признаков целевых атак на ИТ-инфраструктуру организации.

Приложение Kaspersky Endpoint Security может взаимодействовать с Sandbox через Open Single Management Platform (OSMP) или Kaspersky Anti Targeted Attack Platform.

Компонент недоступен для устройств с процессором Эльбрус.

Как настроить интеграцию с Sandbox

Перед началом настройки интеграции с Sandbox:

- Разрешите входящие и исходящие соединения следующим образом:
  - Входящее направление (управляющий интерфейс):
    - TCP 22
    - TCP 443
    - TCP 8443

- Исходящее направление (управляющий интерфейс):
  - TCP 80 или TCP 443
- Исходящие и соответствующие входящие направления (интерфейс для доступа к обрабатываемым объектам):

  Любой порт.

- Установите графический интерфейс (пакет kesl-gui), если хотите отправлять файлы в Sandbox вручную из контекстного меню файла или директории.

Основные этапы настройки

1. **Создайте запрос на подключение к серверу Sandbox в платформе, а затем подтвердите подключение в консоли управления Sandbox**

   См. подробнее в справках соответствующих решений:

   - Kaspersky Anti Targeted Attack Platform
   - Open Single Management Platform

   Сохраните IP-адрес сервера Sandbox любым удобным способом. Он потребуется для дальнейшей настройки интеграции.

2. **Получите и обработайте сертификаты, выданные сервером OSMP или сервером Central Node**

   Во время интеграции с Sandbox устройства с Kaspersky Endpoint Security устанавливают защищенные соединения по протоколу HTTPS с серверами, обеспечивающими интеграцию.

   > Если в общих параметрах приложения Kaspersky Endpoint Security настроено использование прокси-сервера, то для подключения к серверам, обеспечивающими взаимодействие с Sandbox, используется прокси-сервер.

   Сертификаты для защиты соединения с серверами, обеспечивающими взаимодействие с Sandbox, предоставляет администратор платформы OSMP или Kaspersky Anti Targeted Attack Platform.

   Для обработки сертификатов выполните действия, описанные в статье Преобразование сертификата из формата PFX в формат PEM.

   Вы можете использовать Сертификат сервера и/или Сертификат клиента. Выбор определяется политикой безопасности вашей организации.

3. **Настройте параметры интеграции с Sandbox**

   Для отправки файлов на проверку вам нужно включить интеграцию с KATA Sandbox и добавить сервер Central Node, которые развернуты внутри решения.

   Как настроить интеграцию с Sandbox в Web Console

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

      Откроется окно свойств политики.
   3. Выберите вкладку **Параметры приложения**.
   4. Перейдите в раздел **Встроенные агенты** → **Sandbox**.

5. В раскрывающемся списке **Тип отправки файлов на проверку** выберите требуемый способ:

- **Вручную**. При этом режиме вы можете отправить объекты на проверку в Sandbox вручную с помощью команды или из контекстного меню (**Проверить в Sandbox**).

  Мы рекомендуем выбирать этот тип, если версия Sandbox ниже 8.0.

- **Автоматически**. Приложение автоматически отправляет объекты на проверку, при этом отправить объекты на проверку в Sandbox вручную невозможно.

- **Комбинированный**. Приложение автоматически отправляет объекты на проверку, при этом вы можете отправить объекты на проверку в Sandbox вручную с помощью команды или из графического интерфейса.

6. В разделе **Подключение к серверам Sandbox**:

- Добавьте сервер интеграции, нажав на кнопку **Добавить** в панели инструментов.

  В качестве адреса вы можете указать IP-адрес платформы KATA / OSMP либо FQDN-имя.

  Если сервер Sandbox подключен к OSMP, вы можете указать только FQDN-имя сервера агента.

- Добавьте сертификат сервера Kaspersky Anti Targeted Attack Platform или OSMP, который вы получили на шаге 2 основного сценария.

  Для этого нажмите на ссылку **Настройки подключения к серверам**, а затем в открывшейся панели в разделе **TLS-сертификат сервера** нажмите на кнопку **Загрузить**.

- При необходимости дополнительной защиты сформируйте криптоконтейнер.

  Для этого в разделе **Дополнительная защита подключения**:

  - Установите флажок **Использовать двустороннюю аутентификацию**.
  - Нажмите на кнопку **Загрузить** и добавьте сертификат клиента.
  - Укажите пароль от криптоконтейнера в соответствующем поле.

  Поле **Пароль от криптоконтейнера** является обязательным. Если пароль для сертификата клиента (криптоконтейнера) не указан, вы не сможете сохранить настройки.

7. В блоке **Действие при обнаружении угрозы** выберите нужное действие:

- **Копию поместить на карантин, объект удалить**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удаляет вредоносный объект, обнаруженный на компьютере. Перед удалением объекта Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин.

- **Запустить проверку важных областей**. Если выбран этот вариант действия, то Kaspersky Endpoint Security запускает задачу *Проверка важных областей*. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

- **Создать задачу поиска IOC**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически создает задачу *Поиск IOC (автономная задача поиска IOC)*. Вы можете настроить режим запуска задачи, область поиска и действие при обнаружении IOC (*Копию поместить на карантин, объект удалить* или *Запустить проверку важных областей*). Для настройки других параметров задачи *Поиск IOC* перейдите в свойства задачи.

8. Если требуется, в блоке **Область поиска IOC** настройте параметры для задачи *Поиск IOC*:

- **Важные файловые области**. Если выбран этот вариант, Kaspersky Endpoint Security выполняет поиск IOC только в пользовательских и системных директориях.

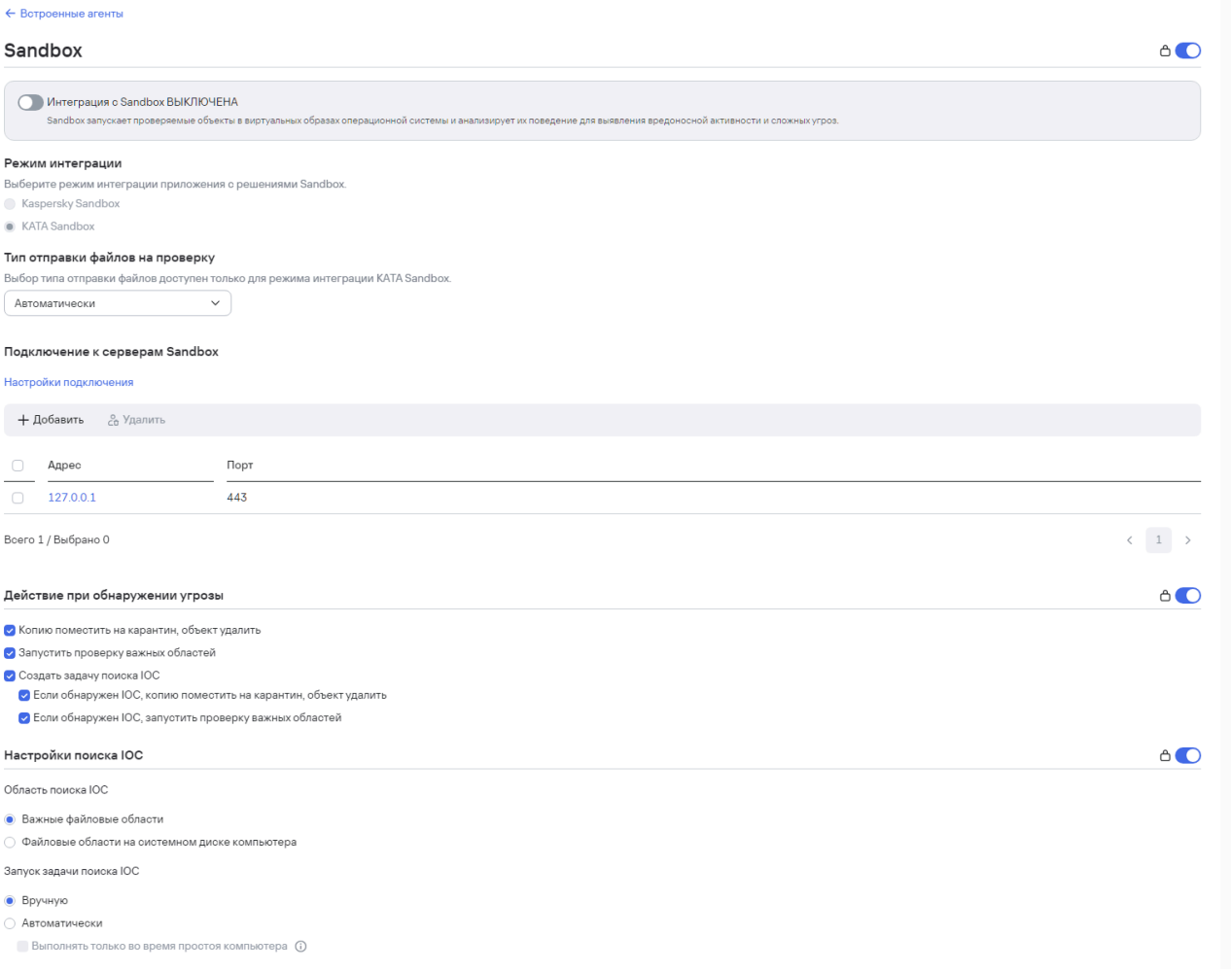
- **Файловые области на системном диске компьютера**. Если выбран этот вариант, Kaspersky Endpoint Security выполняет поиск IOC во всех файлах корневой файловой системы.

9. Если требуется, в блоке **Запуск задачи поиска IOC** настройте параметры для задачи *Поиск IOC*:

- **Вручную**. Режим запуска, при котором вы запускаете задачу *Поиск IOC* вручную в удобное для вас время.

- **Автоматически**. Режим запуска, при котором Kaspersky Endpoint Security запускает задачу *Поиск IOC* автоматически после обнаружения угрозы.

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



Sandbox

Как настроить интеграцию с Sandbox в командной строке

1. Для добавления сертификата сервера выполните команду:

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

2. Для добавления сервера Central Node или OSMP выполните команду:

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port>
```

3. Для настройки параметров интеграции выполните команду:

```
kesl-control --set-settings 29 [<setting name>=<setting value>]
```

Параметры и их возможные значения приведены в таблице ниже.

4. Для добавления сертификата клиента выполните команду:

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

5. Для включения интеграции с Sandbox выполните команду:

```
kesl-control --start-task 29
```

Параметры задачи Интеграция с Sandbox

Параметр	Описание	Значение
`UseClientCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу Sandbox. Если проверка сертификата клиента включена на стороне сервера Sandbox, вам нужно включить использование сертификата клиента и добавить сертификат клиента перед запуском задачи *Интеграция с Sandbox*.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу Sandbox. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером в секундах.	Значение по умолчанию: `10`.
`RequestTimeout`	Максимальное время ожидания ответа от сервера в секундах.	Значение по умолчанию: `10`.
`SendingMode`	Режим отправки файла на проверку в Sandbox.	`AutoOnly` (значение по умолчанию) – автоматическая отправка файлов на проверку при обращении к файлу. `Manual` – ручная отправка файлов на проверку. `AutoAndManual` – автоматическая и ручная отправка файлов на проверку.
`QuarantineFile`	Помещение файла на карантин при обнаружении угрозы.	`Yes` (значение по умолчанию) – при обнаружении угрозы исходный файл удалить, копию файла поместить на карантин. `No` – не помещать файл на карантин при обнаружении угрозы.
`ScanCriticalAreas`	Выполнение проверки важных областей при обнаружении угрозы.	`Yes` (значение по умолчанию) – при обнаружении угрозы запустить проверку важных областей. `No` – не запускать проверку важных областей при обнаружении угрозы.
`CreateIocScanTask`	Создание задачи поиска IOC при обнаружении угрозы.	`Yes` (значение по умолчанию) – при обнаружении угрозы создать задачу поиска IOC. `No` – не создавать задачу поиска IOC при обнаружении угрозы.
`QuarantineFileOnIocDetected`	Помещение объекта на карантин при обнаружении индикатора компрометации.	`Yes` (значение по умолчанию) – при обнаружении индикатора компрометации исходный объект удалить, копию объекта поместить на карантин. `No` – не помещать объект на карантин при обнаружении индикатора компрометации.
`ScanCriticalAreasOnIocDetected`	Выполнение проверки важных областей при обнаружении индикатора компрометации.	`Yes` (значение по умолчанию) – при обнаружении индикатора компрометации запустить проверку важных областей. `No` – не запускать проверку важных областей при обнаружении индикатора компрометации.
`Drives`	Области поиска индикаторов компрометации.	`Critical` (значение по умолчанию) – проверять файлы в пользовательских и системных директориях. `System` – проверять все файлы в пределах корневой файловой системы.

Параметр	Описание	Значение
`ScheduleMode`	Режим запуска задачи поиска IOC.	`Manually` (значение по умолчанию) – запускать задачу поиска IOC вручную. `AfterTreatDetected` – запускать задачу поиска IOC после обнаружения угрозы.
Секция **[Servers.item_#]** содержит параметры сервера Sandbox.		
`Address`	Адрес сервера. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера.	Значение по умолчанию: `127.0.0.1`.
`Port`	Порт для подключения к серверу.	Значение по умолчанию: `443`.
Секция **[SandboxTransferSettings]** содержит параметры передачи файлов на проверку в Sandbox.		
`SandboxQueue`	Максимальный размер директории хранения очереди запросов на проверку в мегабайтах.	Значение по умолчанию: `1024`.

4. **Убедитесь, что подключение к Sandbox выполнено успешно**

   Проверьте статус работы Sandbox удобным для вас способом.

Как проверить, что интеграция с Sandbox включена и работает

Способы проверки работы компонента Sandbox:

- В командной строке с помощью команды:

  ```
  kesl-control --app-info
  ```

  Интеграция с Sandbox отображается со статусом **Задача доступна и выполняется**.

- В Web Console

  - В консоли Kaspersky Security Center:

    С помощью *Отчета о статусе компонентов приложения*. Подробную информацию о работе с отчетами см. в справке Kaspersky Security Center.

  - В консоли OSMP:

    - С помощью *Отчета о статусе компонентов приложения*.

    - Перейдите в раздел **Поиск угроз**.

      События об успешном подключении к Sandbox отображаются в списке событий.

- В Kaspersky Anti Targeted Attack Platform

  Перейдите в раздел **Активы** → **Устройства.** Устройства отображаются в таблице. При необходимости вы можете отфильтровать таблицу по значениям: **Приложение EPP**, **Подключение EPP**, **Последнее соединение с EPP**.

  При нажатии на имя нужного устройства отображается панель. В разделе Endpoint Agent статус подключения **Активное**.

Как отправить файл на проверку в Sandbox вручную

Kaspersky Endpoint Security позволяет пользователю вручную отправлять файлы или директории на проверку в Sandbox из контекстного меню.

Для отправки файлов на проверку в Sandbox должны быть выполнены следующие условия:

- Установлен графический интерфейс Kaspersky Endpoint Security.
- Настроена интеграция приложения Kaspersky Endpoint Security с Sandbox.
- Выбран режим отправки файлов на проверку **Вручную** или **Комбинированный**.

Чтобы отправить файл или директорию на проверку в Sandbox:

1. Откройте контекстное меню файла или директории, которую вы хотите проверить.
2. Выберите приложение **Kaspersky Endpoint Security 12.5 для Linux** в качестве приложения для открытия файла или директории.

   В зависимости от среды рабочего стола названия пунктов контекстного меню могут отличаться.

3. В контекстном меню выберите **Проверить в Sandbox**.

Kaspersky Managed Detection and Response

Kaspersky Endpoint Security включает в себя встроенный агент для интеграции с решением Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* – решение, которое автоматически обнаруживает и анализирует инциденты безопасности в вашей инфраструктуре. Для этого MDR использует данные телеметрии, полученные от конечных точек, и машинное обучение. Данные об инцидентах MDR передает экспертам "Лаборатории Касперского". Далее эксперты могут самостоятельно обработать инцидент и, например, добавить новую запись в антивирусные базы. Или эксперты могут дать рекомендации по обработке инцидента и, например, предложить изолировать компьютер от сети. Подробную информацию о работе решения см. в справке Kaspersky Managed Detection and Response.

Интеграцию обеспечивает компонент приложения Kaspersky Endpoint Security – Managed Detection and Response (далее также MDR). Компонент необходимо активировать одним из способов, описанных в сценарии интеграции.

Компонент недоступен для устройств с процессором Эльбрус.

Конфигурации Kaspersky Endpoint Security для работы с MDR

Для работы с MDR предусмотрены следующие конфигурации:

- **[KES+встроенный агент]**. В этой конфигурации Kaspersky Endpoint Security является и приложением, которое обеспечивает безопасность компьютера, и приложением для работы с MDR.

- **[стороннее EPP+EDR-агент]**. В этой конфигурации безопасность IT-инфраструктуры обеспечивает система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков. Работу с MDR обеспечивает Kaspersky Endpoint Security в конфигурации Endpoint Detection and Response агента (EDR-агент). В этой конфигурации EDR-агента совместим со сторонними EPP-приложениями.

Рекомендации по созданию эталонного образа для корректной интеграции с MDR

В эталонный образ не рекомендуется включать приложение Kaspersky Endpoint Security для Linux.

Если приложение Kaspersky Endpoint Security для Linux было включено в эталонный образ, то на каждом устройстве, созданном на основе этого образа, выполните следующие действия:

1. Для создания нового UUID выполните команды:

```
uuidgen > /var/opt/kaspersky/kesl/common/pcid
uuidgen > /var/opt/kaspersky/epagent/install_id
```

2. Удалите приложение Kaspersky Endpoint Security для Linux и установите его повторно.

Если не выполнить эти действия, устройства могут идентифицироваться некорректно.

Загрузка конфигурационного файла KPSN

Если ваша конфигурация не соответствует требованиям для работы без конфигурационных файлов KPSN, то для интеграции с Kaspersky Managed Detection and Response вам нужно загрузить на Сервер администрирования Kaspersky Security Center *конфигурационный файл KPSN*. Этот файл содержит необходимые параметры для отправки телеметрии. Конфигурационный файл KPSN представляет собой файл с расширением .pkcs7 и находится в ZIP-архиве конфигурационного файла MDR. Подробнее см. в справке Kaspersky Managed Detection and Response.

Вы можете загрузить конфигурационный файл KPSN в Web Console или в Консоли администрирования.

Загружая конфигурационный файл KPSN, вы соглашаетесь автоматически передавать данные с устройства с установленным приложением Kaspersky Endpoint Security в "Лабораторию Касперского" для обработки. Не загружайте конфигурационный файл, если вы не согласны на обработку передаваемых данных. Подробное описание передаваемых данных см. в документации Kaspersky Managed Detection and Response.

Как загрузить конфигурационный файл KPSN в Web Console

1. В главном окне Web Console откройте окно свойств Сервера администрирования.
2. В списке слева выберите раздел **Параметры прокси-сервера KSN**.
3. Включите переключатель **Включить прокси-сервер KSN на Сервере администрирования**, чтобы включить службу прокси-сервера KSN.
4. Включите переключатель **Использовать Kaspersky Private Security Network**.
5. В открывшемся окне с предупреждением об особенностях использования прокси-сервера KSN на точках распространения с установленной старой версией Агента администрирования нажмите на кнопку **OK**.
6. Нажмите на кнопку **Файл с параметрами прокси-сервера KSN**.
7. Выберите конфигурационный файл KSN (файл с расширением .pkcs7) и нажмите на кнопку **Открыть**.
8. Примите условия Положения о KPSN и нажмите на кнопку **Сохранить**.

Как загрузить конфигурационный файл KPSN в Консоли администрирования (MMC)

1. В дереве Консоли администрирования откройте окно свойств Сервера администрирования.
2. Выберите раздел **Прокси-сервер KSN** → **Параметры прокси-сервера KSN**.
3. Установите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы включить службу прокси-сервера KSN.
4. Установите флажок **Настроить KPSN**.
5. В открывшемся окне с предупреждением об особенностях использования прокси-сервера KSN на точках распространения с установленной старой версией Агента администрирования нажмите на кнопку **OK**.
6. Нажмите на кнопку **Файл с параметрами прокси-сервера KSN**.
7. Выберите конфигурационный файл KSN (файл с расширением .pkcs7) и нажмите на кнопку **Открыть**.
8. Примите условия Положения о KPSN и нажмите на кнопку **Применить**.

Как загрузить конфигурационный файл KPSN в командной строке

Выполните команду:

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

Как настроить интеграцию с MDR

Перед началом настройки интеграции с Kaspersky Managed Detection and Response:

- Разрешите подключение через порты 443 и 1443.
- Разрешите соединение со следущими адресами:
  - *.ksn.kaspersky-labs.com
  - ksn-*.kaspersky-labs.com
  - ds.kaspersky.com

  Список адресов может меняться. Для получения точного адреса вы можете обратиться в техническую поддержку.

- Убедитесь, что включены и работают:
  - Kaspersky Security Network в расширенном режиме.
  - Анализ поведения.

    Для полноты отправляемой телеметрии вы можете дополнительно включить следующие компоненты: Защита от веб-угроз, Защита от сетевых угроз, Защита от файловых угроз и Защита от почтовых угроз.

Основные этапы настройки

1. **Активируйте компонент MDR одним из способов**

   - С помощью лицензионного ключа.

     Добавьте в приложение лицензионный ключ MDR, если вы приобрели отдельную лицензию на использование этой функциональности.

     При использовании приложения Kaspersky Endpoint Security по лицензии, которая включает в себя функциональность Kaspersky Managed Detection and Response, действие не требуется.

     Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента, лицензионный ключ MDR добавляется на SVM.

   - С помощью файла MDR BLOB.

     В консоли MDR скачайте конфигурационный файл MDR. Он представляет собой ZIP-архив, содержащий файл MDR BLOB и конфигурационный файл KPSN.

     Затем загрузите файл BLOB в Web Console, в Консоли администрирования или в командной строке.

   Способ активации компонента MDR и необходимость работы с конфигурационным файлом KPSN зависит от версии приложения Kaspersky Endpoint Security. Подробнее см. в справке Kaspersky Managed Detection and Response.

Если Серверы администрирования Kaspersky Security Center организованы в иерархию и на подчиненном сервере отсутствует прямой доступ в интернет, Kaspersky Managed Detection and Response не будет работать даже при наличии доступа в интернет на главном Сервере администрирования.

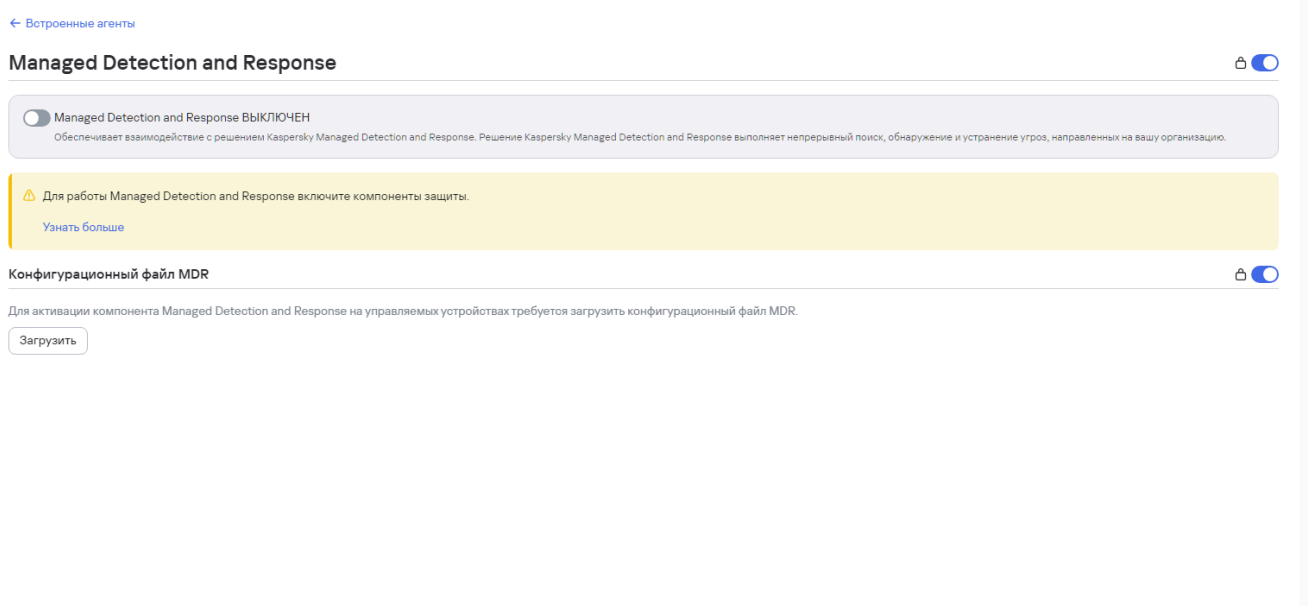
2 **Загрузите конфигурационный файл KPSN**

Если в вашей организации несколько тенантов или вы активировали компонент MDR с помощью MDR BLOB, загрузите файл KPSN на Сервер администрирования Kaspersky Security Center. Файл содержит необходимые параметры для отправки телеметрии и находится в ZIP-архиве с конфигурационным файлом MDR.

3 **Настройте параметры интеграции с Kaspersky Managed Detection and Response**

Как включить интеграцию с Kaspersky Managed Detection and Response в Web Console

1. В главном окне Web Console выберите раздел **Управление активами** → **Политики**.
2. Нажмите на нужную политику Kaspersky Endpoint Security.
3. В открывшемся окне свойств политики выберите вкладку **Параметры приложения**.
4. В разделе **Встроенные агенты** выберите **Managed Detection and Response**, а затем в правой части экрана выполните следующие настройки:
   - Переведите переключатель в положение **Managed Detection and Response ВКЛЮЧЕН**.
   - При наличии тенантов либо если вы активировали компонент MDR с помощью файла MDR BLOB, нажмите на кнопку **Загрузить**, чтобы добавить файл MDR BLOB.
5. Сохраните настройки.



Managed Detection and Response

Как включить интеграцию с Kaspersky Managed Detection and Response в командной строке

1. Для включения компонента MDR выполните команду:

```
kesl-control --set-app-settings UseMDR=Yes
```

2. Для добавления BLOB-файла выполните команду:

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

4 **Настройте политику KSN**

Как настроить параметры KSN в Web Console

1. В политике Kaspersky Endpoint Security на вкладке **Параметры приложения** перейдите в раздел **Общие настройки**.

2. Выберите **Kaspersky Security Network**, а затем в правой части экрана укажите следующие настройки:

   a. Переведите переключатель в положение **Использование Kaspersky Security Network (KSN) ВКЛЮЧЕНО**.

   b. В подразделе **Настройки KSN** установите флажок **Использовать расширенный режим KSN**.

   c. В подразделе **Прокси-сервер KSN** установите флажки:

   - **Использовать Сервер администрирования как прокси-сервер KSN**
   - **Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен**

   Сбор телеметрии будет осуществляться с Сервера администрирования либо с устройства, в зависимости от доступности указанных вариантов.

3. Сохраните настройки.

Как настроить параметры KSN в командной строке

Для включения использования KSN в расширенном режиме выполните команду:

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

5 **Включите KSN**

Как включить KSN в Web Console

1. В главном меню нажмите на имя Сервера администрирования.

2. В открывшемся окне на вкладке **Общие** выберите раздел **Прокси-сервер KSN**.

3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования Включено**.

4. В зависимости от используемого решения инфраструктуры KSN, включите соответствующий переключатель:

   - **Использовать Kaspersky Security Network Включено**.
   - **Использовать Kaspersky Private Security Network Включено**, а затем загрузите конфигурационный файл KPSN.

5. Сохраните настройки.

6. **Убедитесь, что подключение к Kaspersky Managed Detection and Response выполнено успешно**

   Проверьте статус работы Kaspersky Managed Detection and Response удобным для вас способом.

Как проверить, что интеграция с MDR включена

Способы проверки работы компонента Kaspersky Managed Detection and Response:

- В командной строке с помощью команды:

  ```
  kesl-control --app-info
  ```

  Интеграция с Kaspersky Managed Detection and Response отображается со статусом **Задача доступна и выполняется**.

- В Консоли MDR перейдите в раздел **Активы**. Устройства отображаются со статусом **OK** (зеленый).

Если компонент выключен, выполните следующие действия:

1. Обновите антивирусные базы приложения.
2. Убедитесь, что Kaspersky Security Network включен и работает в расширенном режиме.
3. Проверьте лицензионные ключи для Kaspersky Endpoint Security и MDR.
4. Убедитесь, что BLOB-файл добавлен в политику.
5. Проверьте работу компонентов, необходимых для работы MDR.

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Endpoint Security для Linux поддерживает работу с решением Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* – решение класса SIEM для управления информацией о безопасности и событиями безопасности в ИТ-инфраструктуре организации. KUMA позволяет обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб организации.

Подробнее о решении см. в справке Kaspersky Unified Monitoring and Analysis Platform.

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Unified Monitoring and Analysis Platform (KUMA).

Компонент недоступен для устройств с процессором Эльбрус.

Как настроить интеграцию с KUMA

Перед началом настройки интеграции с Kaspersky Unified Monitoring and Analysis Platform:

- Разрешите подключение через порты 443 и 1443 либо через порты, настроенные на стороне коллектора KUMA.
- Добавьте в приложение лицензионный ключ KUMA, если вы приобрели отдельную лицензию на использование этой функциональности.

  При использовании приложения Kaspersky Endpoint Security по лицензии, которая включает в себя функциональность Kaspersky Unified Monitoring and Analysis Platform, действие не требуется.

  Если приложение используется в режиме Легкого агента, лицензионный ключ KUMA добавляется на SVM.

Основные этапы настройки

1. **В платформе KUMA настройте коллектор и нормализатор.**

   Если вы хотите использовать сертификат клиента, при настройке коллектора на вкладке **Транспорт** выберите тип коннектора tcp. Далее на вкладке **Дополнительные параметры** в раскрывающемся списке **Режим TLS** выберите **Нестандартный PFX с аутентификацией клиента**.

2. **Скопируйте адрес коллектора для подключения**

   В разделе **Ресурсы** → **Активные сервисы** в таблице с сервисами скопируйте и сохраните любым удобным способом значения из столбцов **Полное доменное имя / IP-адрес** и **Порт**.

   Если для подключения используется TLS, указывайте только полное доменное имя (FQDN). Значение параметра чувствительно к регистру.

3. **Получите и обработайте сертификаты, выданные сервером KUMA**

   Использование сертификатов для обеспечения безопасности соединения не поддерживается, если подключение к серверу KUMA выполняется по протоколу UDP.

   Для подключения к серверу KUMA используется прокси-сервер, если использование прокси-сервера настроено в общих параметрах приложения Kaspersky Endpoint Security.

   Получите Сертификат сервера (CA-сертификат Microservice) см. Скачивание CA-сертификатов. Для обработки сертификата преобразуйте его в формат DER или PEM, выполнив действия, описанные в статье Преобразование сертификата из формата PFX в формат PEM.

Для дополнительной защиты вы также можете использовать Сертификат клиента, получаемый при настройке коллектора, см. шаг 1.

4. **Настройте параметры интеграции с Kaspersky Unified Monitoring and Analysis Platform**

Как настроить интеграцию с KUMA в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Встроенные агенты** → **Интеграция с KUMA**.
5. Включите переключатель **Интеграция с KUMA ВКЛЮЧЕНА**.
6. Добавьте серверы KUMA:

   a. Нажмите на кнопку **Добавить**.

   Откроется форма добавления серверов KUMA.

   b. Выберите протокол для подключения к серверу KUMA: **HTTP/HTTPS**, **TCP**, **UDP**.

   Протокол для подключения к коллектору в Kaspersky Endpoint Security должен соответствовать типу коннектора в KUMA: **http**, **tcp** или **udp**.

   Если вы выбрали протокол **HTTP/HTTPS**, то по умолчанию приложение использует HTTPS-протокол для подключения к серверам KUMA. Для использования HTTP-протокола вам нужно вручную указать протокол в адресе сервера (например, `http://server.com`).

   c. Введите адрес сервера (IPv4, IPv6), а также порт подключения к серверу (по умолчанию 443).

   Вы можете посмотреть адрес сервера в свойствах коннектора в консоли KUMA. Подробнее о коннекторах KUMA см. в справке Kaspersky Unified Monitoring and Analysis Platform.

   d. Нажмите на кнопку **OK**.

   Kaspersky Endpoint Security подключается к первому серверу KUMA из списка. Если подключение не удается, Kaspersky Endpoint Security подключается ко второму серверу KUMA и так далее по списку.
7. Если требуется, в блоке **Настройки подключения к серверам** настройте параметр **Максимальная задержка отправки событий (сек.)**. По истечении указанного времени Kaspersky Endpoint Security повторно пробует подключиться к тому же коллектору или подключается к следующему в списке коллектору, если их несколько. По умолчанию установлено значение 30 секунд.
8. Сохраните внесенные изменения.

Как настроить интеграцию с KUMA в командной строке

1. Для добавления сервера KUMA выполните команду:

```
kesl-control --set-settings 33 Servers.item_001.ServerAddress=<kuma server address>
Servers.item_001.Port=<kuma server port> Servers.item_001.ServerProtocol=<tcp|HTTPWithCompression|udp>
```

2. Для добавления сертификата сервера KUMA выполните команду:

```
kesl-control [-M] --add-kuma-server-certificate <path to the file>
```

3. Для настройки параметров интеграции выполните команду:

```
kesl-control --set-settings 33 [<setting name>=<setting value>]
```

Параметры и их возможные значения приведены в таблице ниже.

4. Для добавления сертификата клиента для подключения к серверу реагирования выполните команду:

```
kesl-control [-M] --add-kuma-client-certificate <path to the file>
```

5. Для включения интеграции с EDR (KATA) выполните команду:

```
kesl-control --start-task 33
```

Параметры задачи Интеграция с Kaspersky Unified Monitoring and Analysis Platform

Параметр	Описание	Значение
`UseTls`	Включение и выключение проверки сертификата сервера для дополнительной защиты подключения к серверу KUMA.	`Yes` – использовать сертификат для дополнительной защиты подключения к серверу KUMA. `No` (значение по умолчанию) – не использовать сертификат для защиты подключения к серверу KUMA.
`UseClientCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу KUMA. Если проверка сертификата клиента включена на стороне сервера KUMA, вам нужно включить использование сертификата клиента и добавить сертификат клиента перед запуском задачи Интеграция с Kaspersky Unified Monitoring and Analysis Platform.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу KUMA. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером KUMA в секундах.	Значение по умолчанию: `5`.
Секция **[Servers.item_#]** содержит параметры сервера KUMA.		
`ServerAddress`	Адрес сервера KUMA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Если вы установили значение параметра `UseTls=Yes`, требуется указать полное доменное имя (FQDN) сервера из сертификата, полученного при приобретении лицензии на использование KUMA.	Значение по умолчанию: `127.0.0.1`.
`ServerPort`	Порт для подключения к серверу KUMA.	Значение по умолчанию: `443`.

Параметр	Описание	Значение
`ServerProtocol`	Протокол для подключения к серверу KUMA.	`tcp` (значение по умолчанию) – использовать для подключения к серверу KUMA протокол TCP. `HTTPWithCompression` – использовать для подключения к серверу KUMA протокол HTTP с возможностью сжатия событий при их передаче. `udp` – использовать для подключения к серверу KUMA протокол UDP. При выборе протокола UDP использование сертификатов для обеспечения безопасности соединения не поддерживается (значения параметров `UseTls`, `UseClientCertificate` и `ConnectionTimeout` не учитываются), а также отсутствуют события о соединении с сервером KUMA.
Секция **[KumaTransferSettings]** содержит параметры передачи событий на сервер KUMA.		
`EventTransferTimeMax`	Максимальная задержка отправки событий на сервер KUMA в секундах.	Значение по умолчанию: `30`.

5. **Убедитесь, что подключение к Kaspersky Unified Monitoring and Analysis Platform выполнено успешно**

   Проверьте статус работы KUMA удобным для вас способом.

Как проверить, что интеграция с KUMA включена и работает

Способы проверки работы компонента KUMA:

- В командной строке с помощью команды:

  ```
  kesl-control --app-info
  ```

  Интеграция с KUMA отображается со статусом **Задача доступна и выполняется**.

- В Web Console (консоль OSMP):

  Перейдите в раздел **Поиск угроз**: события телеметрии со статусом "Соединение с KUMA установлено" с требуемого устройства отображаются в списке событий.

- В Kaspersky Unified Monitoring and Analysis Platform:

  В главном меню консоли KUMA перейдите в раздел **События**: события телеметрии Kaspersky Endpoint Security отображаются в списке.

Защита виртуальных сред

Kaspersky Endpoint Security поддерживает режим Легкого агента для работы в составе решения Kaspersky Security для виртуальных сред Легкий агент. *Kaspersky Security для виртуальных сред Легкий агент* – интегрированное решение, обеспечивающее комплексную защиту виртуальных машин от различных видов информационных угроз, сетевых и мошеннических атак. Для работы с этим решением вам нужно установить приложение в режиме Легкого агента.

При запуске Легкий агент устанавливает и поддерживает соединение с виртуальной машиной SVM (Secure Virtual Machine). На SVM развернут Сервер защиты. *Сервер защиты* – компонент решения Kaspersky Security для виртуальных сред Легкий агент, который выполняет проверку файлов на наличие вирусов и других вредоносных приложений, обновляет антивирусные базы и управляет лицензионными ключами. Легкий агент отправляет на SVM файлы или их фрагменты, которые необходимо проверять. Результаты проверки доступны для всех виртуальных машин с установленным Легким агентом благодаря технологии SharedCache. Эта технология повышает эффективность работы решения и обеспечивает более высокую скорость реакции на угрозы.

В инфраструктуре организации может быть много виртуальных машин с установленным Легким агентом и много SVM. Взаимодействие между виртуальными машинами и SVM осуществляется с помощью Сервера интеграции. *Сервер интеграции* – компонент решения Kaspersky Security для виртуальных сред Легкий агент, который формирует список доступных SVM и передает эти данные Легким агентам, участвует в обнаружении SVM Легкими агентами, обеспечивает защиту соединения между Легкими агентами и SVM, а также выполняет другие функции.

Подключение Легкого агента к SVM

1. **Получение списка доступных SVM**

   Легкий агент получает список доступных SVM.

2. **Выбор оптимального Сервера защиты (SVM)**

   Легкий агент определяет оптимальный для подключения Сервер защиты (SVM) из числа доступных для подключения в соответствии с алгоритмом выбора SVM.

3. **Проверка дополнительных параметров подключения**

   Легкий агент проверяет дополнительные параметры для подключения к SVM: теги, статус защиты подключения, доступные по лицензии функции приложения.

4. **Подключение Легкого агента к SVM**

   Легкий агент устанавливает и поддерживает соединение с выбранной SVM.

Как настроить обнаружение SVM

Вы можете выбрать один из способов обнаружения SVM Легким агентом:

- С помощью Сервера интеграции (VIIS).

  Сервер интеграции – компонент решения, который обеспечивает взаимодействие между решением Kaspersky Security для виртуальных сред Легкий агент и виртуальной инфраструктурой и формирует список доступных для подключения SVM. Легкий агент устанавливает соединение с Сервером интеграции и получает список адресов SVM.

  Сервер интеграции удобно использовать в больших виртуальных инфраструктурах, так как он автоматически распределяет нагрузку между SVM, получает информацию о доступных SVM, анализирует эту информацию и предоставляет Легким агентам список Серверов защиты (SVM), оптимальных для подключения.

  Для получения списка SVM Легким агентом вам нужно только ввести адрес Сервера интеграции.

- С помощью отказоустойчивого кластера Серверов интеграции.

Развертывание отказоустойчивого кластера Серверов интеграции доступно в Kaspersky Security для виртуальных сред Легкий агент версии 6.4. Отказоустойчивый кластер Серверов интеграции обеспечивает непрерывную защиту виртуальной среды за счет переключения SVM и Легких агентов на резервный Сервер интеграции при отказе главного Сервера интеграции. Переключение между серверами выполняет специальный компонент кластера – *балансировщик нагрузки*. Подробнее об отказоустойчивом кластере Серверов интеграции см. в справке Kaspersky Security для виртуальных сред Легкий агент.

Для получения списка SVM Легким агентом вам нужно ввести адрес устройства, на котором установлен балансировщик нагрузки.

- С помощью списка адресов SVM.

  Если вам нужно указать для Легкого агента отдельные SVM для подключения, вы можете составить список вручную.

  Для получения списка SVM Легким агентом вам нужно перечислить адреса доступных SVM.

Как настроить обнаружение SVM Легким агентом в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Режим Легкого агента** → **Настройки обнаружения SVM**.
5. Выберите способ обнаружения SVM:
   - **Использовать Сервер интеграции**. Введите параметры подключения к Серверу интеграции в зависимости от вашей инфраструктуры:
     - **Одиночный Сервер интеграции**. Введите параметры подключения к Серверу интеграции: IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства.
     - **Отказоустойчивый кластер Серверов интеграции**. Введите IP-адрес и порт балансировщика нагрузки, который входит в состав кластера.
   - **Использовать список адресов SVM, заданный вручную**. Сформируйте список SVM для подключения Легкого агента. Введите IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Каждый элемент списка нужно вводить с новой строки или отделять от предыдущего с помощью `;`.

     В списке адресов SVM требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе решения.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как посмотреть информацию о подключении Легкого агента к Серверу интеграции в командной строке

1. Убедитесь, что приложение установлено в режиме Легкого агента:

   ```
   kesl-control -V --ksvla-info
   ```

   Компонент должен иметь статус **Включен**.

2. Выведите информацию о подключении Легкого агента к Серверу интеграции:

```
kesl-control -V --viis-info
```

В результате выполнения команды в консоль выводится следующая информация:

- Адрес и порт Сервера интеграции, к которому подключается Легкий агент.
- Статус подключения к Серверу интеграции.
- Дата и время последнего соединения Легкого агента с Сервером интеграции.

Как посмотреть информацию о подключении Легкого агента к SVM в командной строке

1. Убедитесь, что приложение установлено в режиме Легкого агента:

   ```
   kesl-control -V --ksvla-info
   ```

   Компонент должен иметь статус **Включен**.

2. Выведите информацию о подключении Легкого агента к Серверу интеграции:

   ```
   kesl-control -V --svm-info
   ```

В результате выполнения команды в консоль выводится следующая информация:

- Адрес SVM, к которой подключен Легкий агент, и расположение SVM в виртуальной инфраструктуре относительно Легкого агента: локальная или не локальная.
- Способ обнаружения SVM Легким агентом: с помощью Сервера интеграции или с использованием списка адресов SVM, заданных вручную.
- Список адресов SVM, если в качестве способа обнаружения SVM выбрано использование списка адресов SVM.
- Тег для подключения Легкого агента к SVM.
- Алгоритм выбора SVM: стандартный или расширенный. Если применяется расширенный алгоритм выбора SVM, также выводится тип расположения SVM в виртуальной инфраструктуре.
- Наличие защиты соединения между Легким агентом и Сервером защиты.

Как Легкий агент выбирает SVM

В инфраструктуре организации может быть развернуто несколько SVM, к которым могут подключаться Легкие агенты. Для оптимизации нагрузки на сеть и ресурсы виртуальной инфраструктуры необходимо распределить Легкие агенты между SVM.

Алгоритмы выбора SVM

Легкие агенты могут применять следующие алгоритмы выбора SVM для подключения: Стандартный алгоритм (по умолчанию) и Расширенный алгоритм.

Алгоритмы выбора SVM

Стандартный алгоритм	Расширенный алгоритм
Если применяется этот алгоритм, после установки и запуска на виртуальной машине Легкий агент выбирает для подключения SVM, которая является *локальной* для Легкого агента. Если нет доступных для подключения локальных SVM, Легкий агент выбирает SVM, к которой подключено наименьшее количество Легких агентов, независимо от расположения SVM в виртуальной инфраструктуре. Локальность SVM относительно Легкого агента не определяется, если для Сервера защиты на этой SVM включен режим защиты больших инфраструктур. В этом случае рекомендуется использовать расширенный алгоритм выбора SVM и выбрать Сервер интеграции в качестве способа обнаружения SVM. Локальность SVM относительно Легкого агента определяется в зависимости от вида виртуальной инфраструктуры.	Если применяется этот алгоритм, вы можете определять следующие параметры выбора SVM: • учитывать или игнорировать расположение SVM в инфраструктуре при выборе SVM для подключения; • если расположение SVM учитывается, как определять локальность SVM относительно Легкого агента. Если Легкие агенты игнорируют расположение SVM в инфраструктуре, то Легкие агенты смогут подключаться к любым доступным для подключения SVM. Если Легкие агенты должны учитывать расположение SVM в инфраструктуре, вам нужно выбрать тип расположения SVM, который будет учитываться при определении локальности SVM относительно Легкого агента. Локальность SVM относительно Легкого агента определяется по-разному в зависимости от виртуальной инфраструктуры. Если Легкие агенты учитывают расположение SVM в инфраструктуре при выборе SVM для подключения, то Легкие агенты могут подключаться только к тем SVM, которые являются локальными. Например, если вы указали в качестве типа расположения SVM кластер гипервизоров, то локальными для Легкого агента будут считаться все SVM, развернутые на этом кластере гипервизоров, и Легкий агент сможет подключаться только к одной из этих SVM. Если в том же кластере, в котором работает Легкий агент, нет доступных для подключения SVM, Легкий агент не будет подключаться к SVM. При выборе SVM Легкие агенты также учитывают количество подключенных Легких агентов, чтобы обеспечить равномерное распределение Легких агентов между доступными для подключения SVM. Если для Легкого агента применяется расширенный алгоритм выбора SVM и в качестве способа обнаружения SVM выбран список адресов SVM, а на SVM включен режим защиты больших инфраструктур, то подключение Легкого агента к этой SVM возможно, только если Легкий агент игнорирует расположение SVM.
Базис Dynamix Enterprise	
В виртуальной инфраструктуре на платформе Базис Dynamix Enterprise локальной для Легкого агента считается SVM, которая развернута на том же вычислительном узле, что и виртуальная машина с установленным Легким агентом.	В виртуальной инфраструктуре на платформе Базис Dynamix Enterprise SVM может считаться локальной для Легкого агента в одном из следующих случаев: • SVM развернута на том же вычислительном узле, что и виртуальная машина с установленным Легким агентом. • SVM развернута в той же зоне, что и виртуальная машина с установленным Легким агентом. • SVM развернута в том же дата-центре (ЦОД), что и виртуальная машина с установленным Легким агентом.
Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Numa vServer и Базис Dynamix Standard	

Стандартный алгоритм	Расширенный алгоритм
В виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Numa vServer или Базис Dynamix Standard локальной для Легкого агента считается SVM, которая развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом.	В виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Numa vServer или Базис Dynamix Standard SVM может считаться локальной для Легкого агента в одном из следующих случаев: • SVM развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом. • SVM развернута на том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом. • SVM развернута в том же дата-центре, что и виртуальная машина с установленным Легким агентом.
OpenStack и Private Cloud от VK SVM	
В виртуальной инфраструктуре под управлением платформы OpenStack или Private Cloud от VK вы можете указывать, как определяется локальность SVM относительно Легкого агента, с помощью параметра `StandardAlgorithmSvmLocality` в секции `HypervisorSpecificSettings:Openstack` в конфигурационном файле Сервера интеграции appsettings.json. В зависимости от версии Сервера интеграции файл расположен по следующему пути: • /var/opt/kaspersky/viis/common/ – файл Сервера интеграции на базе Linux. • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ – файл Сервера интеграции на базе Windows. Параметр `StandardAlgorithmSvmLocality` может принимать следующие значения: • `ServerGroup` – если установлено это значение, локальной для Легкого агента считается SVM, которая находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом. Это значение используется по умолчанию. • `Project` – если установлено это значение, локальной для Легкого агента считается SVM, которая развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом. • `AvailabilityZone` – если установлено это значение, локальной для Легкого агента считается SVM, которая расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом.	В виртуальной инфраструктуре под управлением платформы OpenStack или Private Cloud от VK SVM может считаться локальной для Легкого агента в одном из следующих случаев: • SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом. • SVM развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом. • SVM расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом.

Кроме алгоритмов подключения к SVM вы можете регулировать подключение Легких агентов к SVM с помощью тегов.

Как настроить алгоритм выбора SVM для Легкого агента в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Режим Легкого агента** → **Алгоритм выбора SVM**.
5. Выберите алгоритм:

   - **Использовать стандартный алгоритм выбора SVM**. Легкий агент выбирает SVM, развернутые в том же гипервизоре.
   - **Использовать расширенный алгоритм выбора SVM**. Легкий агент выбирает SVM, развернутые в выбранном типе расположения SVM (по умолчанию **Гипервизор**).

6. Если требуется, выберите расположение SVM для расширенного алгоритма выбора SVM:

- **Гипервизор**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

  - SVM развернуты на том же гипервизоре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Numa vServer или Базис Dynamix Standard).

  - SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack или Private Cloud от VK).

  - SVM находится на том же вычислительном узле, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

  Если на том же гипервизоре или в той же Группе серверов, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Кластер**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

  - SVM развернуты в том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Numa vServer или Базис Dynamix Standard).

  - SVM развернуты в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack или Private Cloud от VK).

  - SVM находится в той же зоне, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

  Если в том же кластере гипервизоров или в рамках того же проекта OpenStack, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Дата-центр**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):

  - SVM развернуты в том же дата-центре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Numa vServer или Базис Dynamix Standard).

  - SVM расположены в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack или Private Cloud от VK).

  - SVM находится в том же ЦОД, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).

Если в том же дата-центре или в той же Зоне доступности, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.

- **Игнорировать**. Легкий агент не учитывает расположение SVM для подключения к Серверу защиты. Легкий агент учитывает другие критерии: теги, количество Легких агентов, подключенных к SVM, и другие.

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

Как распределить подключение Легких агентов между SVM

К SVM могут подключаться несколько Легких агентов. Для распределения подключения Легких агентов вы можете указать отдельный список SVM. Если вы используете Сервер интеграции для обнаружения SVM, для распределения подключений Легких агентов к SVM вы можете использовать *теги*. То есть для Легкого агента вы можете назначить список SVM для подключения по тегу. Для этого вам нужно присвоить тег Легкому агенту и указать этот тег в параметрах SVM. Подробнее об указании тегов в параметрах SVM см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Пример. В вашей инфраструктуре развернуто решение Kaspersky Endpoint Detection and Response Optimum для выделенных узлов виртуальных машин. Тогда вы можете назначить Легкому агенту тег `[EDROptimum]` для подключения к SVM, на которых добавлен лицензионный ключ EDR Optimum (EDR Optimum Add-on). В результате вам будут доступны функции EDR Optimum на виртуальной машине с Легким агентом. При подключении Легкого агента к SVM без лицензионного ключа EDR Optimum, функции решения Kaspersky Endpoint Detection and Response Optimum недоступны.

Как присвоить тег Легкому агенту для подключения к SVM в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Режим Легкого агента** → **Тег для подключения к SVM**.

5. Установите флажок **Использовать тег для подключения** и введите тег для подключения к SVM.

   В качестве тега вы можете ввести текстовую строку длиной не более 255 символов. Вы можете использовать любые символы, кроме символа `;`.

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

Как защитить соединение между Легким агентом и SVM

Вы можете настроить защиту соединения между Легкими агентами и Сервером защиты с помощью шифрования. Для этого вам требуется включить шифрование канала передачи данных между Легким агентом и Сервером защиты в параметрах Сервера защиты на SVM и в параметрах Легкого агента.

Легкий агент, для которого включена защита соединения, может подключаться только к тем SVM, на которых включено шифрование канала передачи данных между Легким агентом и Сервером защиты. Легкий агент, для которого выключена защита соединения, может подключаться только к тем SVM, на которых шифрование канала выключено или разрешено незащищенное соединение между Сервером защиты и Легким агентом.

Подробнее о настройке защиты соединения на Сервере защиты см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Защита соединения с помощью шифрования может привести к снижению производительности работы решения Kaspersky Security для виртуальных сред Легкий агент.

Как настроить защиту соединения на Легком агенте в Web Console

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Режим Легкого агента** → **Защита соединения**.
5. Установите флажок **Шифровать канал передачи данных между Легким агентом и Сервером защиты**.
6. Для применения политики на компьютерах закройте замки, сохраните внесенные изменения.

Как узнать статус работы Легкого агента

В командной строке вы можете посмотреть следующую информацию об использовании приложения в режиме Легкого агента:

- о параметрах использования приложения в режиме Легкого агента;
- о подключении Легкого агента к Серверу интеграции;
- о подключении Легкого агента к SVM.

Просмотр информации о параметрах использования приложения в режиме Легкого агента

```
kesl-control [-V] --ksvla-info
```

В результате выполнения команды в консоль выводится следующая информация:

- Режим Легкого агента для защиты виртуальных сред: Включен или Выключен.

  Если режим Легкого агента включен, приложение используется в составе решения Kaspersky Security для виртуальных сред Легкий агент.

- Режим защиты инфраструктуры VDI: Включен или Выключен.

  Режим защиты инфраструктуры VDI позволяет оптимизировать работу приложения Kaspersky Endpoint Security на временных виртуальных машинах. Если режим защиты инфраструктуры VDI включен, то обновления, требующие перезагрузки защищенной виртуальной машины, не устанавливаются на временных виртуальных машинах. При получении обновлений, требующих перезагрузки, Легкий агент, установленный на временной виртуальной машине, отправляет в Kaspersky Security Center сообщение о необходимости обновления шаблона защищенных виртуальных машин.

- Тип виртуальной машины: временная или постоянная.

- Роль виртуальной машины: Сервер или Рабочая станция.

- Идентификатор виртуальной машины – UUID.

Просмотр информации о подключении Легкого агента к Серверу интеграции

```
kesl-control [-V] --viis-info
```

В результате выполнения команды в консоль выводится следующая информация:

- Адрес и порт Сервера интеграции, к которому подключается Легкий агент.

- Статус подключения к Серверу интеграции.

- Дата и время последнего соединения Легкого агента с Сервером интеграции.

Если в вашей инфраструктуре развернут отказоустойчивый кластер Серверов интеграции на базе Linux, выводится адрес и порт балансировщика нагрузки. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Просмотр информации о подключении Легкого агента к SVM

```
kesl-control [-V] --svm-info
```

В результате выполнения команды в консоль выводится следующая информация:

- Адрес SVM, к которой подключен Легкий агент, и расположение SVM в виртуальной инфраструктуре относительно Легкого агента: локальная или не локальная.

- Способ обнаружения SVM Легким агентом: с помощью Сервера интеграции или с использованием списка адресов SVM, заданных вручную.

- Список адресов SVM, если в качестве способа обнаружения SVM выбрано использование списка адресов SVM.

- Тег для подключения Легкого агента к SVM.

- Алгоритм выбора SVM: стандартный или расширенный. Если применяется расширенный алгоритм выбора SVM, также выводится тип расположения SVM в виртуальной инфраструктуре.

- Наличие защиты соединения между Легким агентом и Сервером защиты.

Информацию о параметрах подключения Легких агентов к Серверу интеграции и SVM см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Лучшие практики

При развертывании Kaspersky Endpoint Security для Linux вы можете использовать рекомендации, приведенные в этом разделе, для настройки защиты компьютеров и оптимизации производительности. Также при проблемах производительности компьютера см. базу знаний Службы технической поддержки.

Оптимизация потребления ресурсов приложением

При работе приложения с параметрами, настроенными по умолчанию, возможно снижение производительности системы на некоторых устройствах в результате совместного использования системных ресурсов прикладными приложениями и приложением Kaspersky Endpoint Security.

Рекомендуемый сценарий настройки приложения для оптимизации потребления ресурсов системы:

1. **Распределение устройств по группам администрирования в соответствии с ролью устройств в инфраструктуре**

   Выполните инвентаризацию устройств по выполняемым функциям и поместите их в разные группы администрирования с учетом этих функций. Например, в одну администрирования группу поместите веб-серверы, в другую группу администрирования поместите серверы баз данных, в третью группу администрирования поместите рабочие станции пользователей и так далее.

2. **Настройка приложения для типовых серверных ролей**

   Выполните рекомендуемую настройку приложения на устройствах в соответствии с их ролью в инфраструктуре.

3. **Анализ производительности на пилотных устройствах**

   Выделите одно или два пилотных устройства в каждой из групп администрирования. Для каждого устройства проанализируйте, как приложение Kaspersky Endpoint Security использует системные ресурсы и как меняется производительность установленных приложений на устройствах.

4. **Настройка приложения на пилотных устройствах по результатам анализа производительности**

   Если производительность прикладных приложений значительно снижается или количество системных ресурсов, которые потребляет приложение Kaspersky Endpoint Security, критично для работы операционной системы и прикладных приложений, выполните рекомендуемую настройку Защиты от файловых угроз и задач проверки.

   Чтобы снизить влияние компонентов Защита от веб-угроз, Защита от сетевых угроз и Анализ поведения на работу прикладных приложений, оптимизируйте работу этих компонентов.

5. **Настройка приложения на всех устройствах**

   Если указанные действия привели к приросту производительности на устройстве, выполните аналогичную настройку приложения на других устройствах того же типа.

Анализ работы приложения на устройстве

При проверке объектов приложение Kaspersky Endpoint Security использует ресурсы процессора, ввод-вывод дисковой подсистемы и оперативную память.

Посмотреть информацию о потреблении ресурсов приложением

```
top -bn1|grep kesl
```

Выполнять команду нужно в момент нагрузки на систему.

Вывод команды показывает количество потребляемой памяти и занимаемого процессорного времени:

```
651 root        20      0 3014172 2.302g 154360 S 120.0 30.0    0:32.80 kesl
```

В столбце 6 отображается количество резидентной памяти – 2.302g.

В столбце 9 отображается процент использования ядер процессора – 120.0, где каждое ядро принимается за 100 процентов. Таким образом, 120% означает, что одно ядро занято полностью, а второе – на 20%.

Для получения информации о производительности приложения вы также можете настроить сбор метрик о ресурсах операционной системы, используемых приложением.

Если работа приложения Kaspersky Endpoint Security критически замедляет работу системы, вам нужно определить, какие компоненты и задачи приложения занимают ресурсы системы.

Для этого выполните следующие исследования на устройстве:

1. **Проанализируйте потребление ресурсов задачей Защита от файловых угроз (задача типа OAS)**

   В результате вы сможете установить, связаны ли проблемы производительности с задачей Защита от файловых угроз или с задачами проверки (задачи типов ODS и ContainerScan), и выполнить рекомендации для соответствующих задач.

   Как проанализировать потребление ресурсов задачей Защита от файловых угроз

   1. Остановите все задачи проверки и мониторинга.

   2. Убедитесь, что задачи проверки по требованию (задачи типов ODS и ContainerScan) не будут запущены по расписанию во время исследования:

      a. Получите список всех задач приложения:

      ```
      kesl-control --get-task-list
      ```

      b. Получите параметры расписания всех задач типов ODS и ContainerScan:

      ```
      kesl-control --get-schedule <task ID |name>
      ```

      Если команда выводит `RuleType=Manual`, то задача запускается только вручную.

c. Для всех задач, у которых значение параметра `RuleType` отличается от `Manual`, измените расписание запуска:

```
kesl-control --set-schedule <task ID |name> RuleType=Manual
```

3. Включите создание файлов трассировки приложения с высоким уровнем детализации:

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. Запустите задачу Защита от файловых угроз, если она не запущена:

```
kesl-control --start-task 1
```

5. Создайте нагрузку на систему в том же режиме, который вызвал проблемы с производительностью. Достаточно нескольких часов.

6. Проанализируйте полученные файлы трассировки. По умолчанию файлы трассировки сохраняются в директории /var/log/kaspersky/kesl.

> Под нагрузкой приложение записывает много информации в файлы трассировки, при этом по умолчанию хранится 10 файлов по 500 МБ, поэтому старая информация будет перезаписываться.

Если проблемы с производительностью и потреблением ресурсов продолжаются, значит требуется оптимизировать работу Защиты от файловых угроз.

Если проблемы с производительностью и потреблением ресурсов перестали проявляться, значит, скорее всего, проблемы вызывают задачи проверки по требованию (задачи типов ODS и ContainerScan) или задача Анализ поведения. Требуется оптимизировать работу задач проверки или проанализировать работу задачи Анализ поведения.

7. Выключите создание файлов трассировки приложения:

```
kesl-control --set-app-settings TraceLevel=None
```

2 Проанализируйте потребление ресурсов задачей Анализ поведения (задача типа Behavior_Detection)

В результате вы сможете установить, связаны ли проблемы производительности с задачей Анализ поведения или с задачами проверки (задачи типов ODS и ContainerScan), и выполнить рекомендации для соответствующих задач.

Как проанализировать потребление ресурсов задачей Анализ поведения

1. Остановите все задачи проверки и мониторинга.

2. Убедитесь, что задачи проверки по требованию (задачи типов ODS и ContainerScan) не будут запущены по расписанию во время исследования:

   a. Получите список всех задач приложения:

```
kesl-control --get-task-list
```

b. Получите параметры расписания всех задач типов ODS и ContainerScan:

```
kesl-control --get-schedule <task ID|name>
```

Если команда выводит `RuleType=Manual`, то задача запускается только вручную.

c. Для всех задач, у которых значение параметра `RuleType` отличается от `Manual`, измените расписание запуска:

```
kesl-control --set-schedule <task ID|name> RuleType=Manual
```

3. Включите создание файлов трассировки приложения с высоким уровнем детализации:

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. Запустите задачу Анализ поведения, если она не запущена:

```
kesl-control --start-task 20
```

5. Создайте нагрузку на систему в том же режиме, который вызвал проблемы с производительностью. Достаточно нескольких часов.

6. Проанализируйте полученные файлы трассировки. По умолчанию файлы трассировки сохраняются в директории /var/log/kaspersky/kesl.

> Под нагрузкой приложение записывает много информации в файлы трассировки, при этом по умолчанию хранится 10 файлов по 500 МБ, поэтому старая информация будет перезаписываться.

Если проблемы с производительностью и потреблением ресурсов продолжаются, значит требуется оптимизировать работу Анализа поведения.

Если проблемы с производительностью и потреблением ресурсов перестали проявляться, значит, скорее всего, проблемы вызывают задачи проверки по требованию (задачи типов ODS и ContainerScan). Требуется оптимизировать работу этих задач.

7. Выключите создание файлов трассировки приложения:

```
kesl-control --set-app-settings TraceLevel=None
```

3 Определите наиболее часто проверяемые объекты

Вы можете исключать из проверки неопасные часто проверяемые объекты и файлы для оптимизации работы Защиты от файловых угроз и задач проверки.

Определите, являются ли опасными объекты и файлы, которые были проверены наибольшее количество раз. Например, неопасными можно признать файлы баз данных, директории и файлы журналов, если запись в них ведет доверенный процесс. В случае затруднения обратитесь в Службу технической поддержки.

Как определить наиболее часто проверяемые объекты

1. Получите список объектов, которые были проверены наибольшее количество раз:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c | sort -k1 -n -
r|less
```

Результат загружается в приложение просмотра текста less, в самом начале отображаются те объекты, которые были проверены наибольшее количество раз.

Если вам нужно агрегировать статистику по проверке объектов в директориях для определенной глубины вложенности директорий, начиная от корневой директории `/`, то вы можете добавить в команду `cut -d/ -f 1-X`, где X – заданная глубина вложенности. Например:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | cut -d/ -f 1-4 | sort | uniq -c |
sort -k1 -n -r|less
```

2. Если в системе осуществляется частая запись файлов различными службами, такие файлы будут повторно проверяться в отложенной очереди. Получите список путей, которые были проверены в отложенной очереди наибольшее количество раз:

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' |
sort | uniq -c | sort -k1 -n -r
```

Файлы, проверенные наибольшее количество раз, будут отображаться в начале списка.

Если вам нужно агрегировать статистику по проверке объектов в директориях для определенной глубины вложенности директорий, начиная от корневой директории `/`, то вы можете добавить в команду `cut -d/ -f 1-X`, где X – заданная глубина вложенности. Например:

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' |
tr -d ',' |  cut -d/ -f 1-3 | sort | uniq -c | sort -k1 -n -r
```

4. **Определите процессы, запуск которых приложение Kaspersky Endpoint Security обнаруживает наиболее часто**

Вы можете исключать из проверки неопасные часто запускаемые процессы для оптимизации работы Анализа поведения.

Как определить наиболее часто запускаемые процессы

Выполните команду:

```
kesl-control --get-statistic --processes
```

Команда позволяет вывести список процессов, запуск которых приложение Kaspersky Endpoint Security обнаруживает наиболее часто, и количество этих запусков.

5. **Определите пути, по которым происходит большое количество перехватов файловых операций**

Вы можете исключать директории из перехвата файловых операций для оптимизации работы Защиты от файловых угроз и задач проверки.

Как получить информацию о перехватах файловых операций

Вы можете получать информацию о перехватах файловых операций следующими способами:

- Получить статистику по файлам, которые компонент Защита от файловых угроз проверяет наиболее часто:

  ```
  kesl-control --get-statistic --files
  ```

  Команда позволяет вывести статистические данные о файловых операциях, перехваченных за последние 24 часа.

- Выполнить более точный анализ с помощью файлов трассировки приложения. Анализируя файлы трассировки, вы можете получить список файлов, перехваченных приложением, и определить пути, по которым происходит большое количество перехватов файловых операций.

  По умолчанию файлы трассировки не создаются.

  Включить создание файлов трассировки

  ```
  kesl-control --set-app-settings TraceLevel=Detailed
  ```

  Включение трассировки может оказать негативное влияние на общую производительность системы. Рекомендуется выключить создание файлов трассировки, когда необходимость записи трассировок пропадет.

  Выключить создание файлов трассировки

  ```
  kesl-control --set-app-settings TraceLevel=None
  ```

- Получить список перехваченных файлов:

  ```
  grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print
  $2}'|sort | uniq -c | sort -k1 -n -r
  ```

  Если вам нужно агрегировать статистику по перехвату файловых операций в директориях для определенной глубины вложенности директорий, начиная от корневой директории `/`, то вы можете добавить в команду `cut -d/ -f 1-X`, где X – заданная глубина вложенности. Например:

  ```
  grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print
  $2}'| cut -d/ -f 1-3|sort | uniq -c | sort -k1 -n -r|less
  ```

Анализ работы приложения выполняется с помощью командной строки. Если устройство находится под управлением политики Kaspersky Security Center, на время проведения исследования разрешите управление локальными задачами.

Рекомендации для Защиты от файловых угроз и задач проверки

Общие рекомендации

Исключения из проверки

Исключения из проверки позволяют поддерживать баланс между защищенностью и производительностью системы.

Рекомендуется исключить из проверки:

- Файлы данных и индексные файлы баз данных. По мнению вирусных экспертов "Лаборатории Касперского" опасность проникновения вирусов через такие файлы отсутствует.
- Неопасные объекты из списка наиболее часто проверяемых объектов.

Исключения можно настраивать по пути (в том числе можно задать тип монтирования), маске файла, типу угрозы и пути к процессу, совершающему файловые операции.

> Приложение не проверяет объекты, исключенные из проверки, но минимальные задержки в файловых операциях присутствуют, так как приложение все равно выполняет перехват и блокировку файловых операций. Если даже минимальные задержки в работе системы критичны, рекомендуется настроить исключения из перехвата файловых операций.

Где настроить исключения:

- Для Защиты от файловых угроз – в политике с помощью Web Console или Консоли администрирования или локально на устройстве с помощью командной строки.
- Для задач проверки с типами ODS и ContainerScan – в параметрах задач в Kaspersky Security Center или локально на устройстве с помощью командной строки.

  > Исключения для одной задачи проверки не распространяются на другие задачи проверки. Для каждой задачи проверки требуется настроить свои исключения.

Примеры настройки исключений для Защиты от файловых угроз с помощью командной строки

```
Исключить директорию /tmp/logs и все поддиректории и файлы рекурсивно
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

```
Исключить конкретный файл или файлы по маске в директории /tmp/logs
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

```
Исключить по рекурсивной маске все файлы с расширением .log в директории /tmp/ и поддиректориях
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Исключения из перехвата файловых операций

Файлы, исключенные из проверки, все равно могут перехватываться приложением во время работы Защиты от файловых угроз и задач проверки. Приложение перехватывает события файловых операций и блокирует действия до окончания обработки событий. После проверки приложение может:

- снять блокировку и разрешить операцию;
- заблокировать операцию и выполнить действия, заданные в параметрах защиты или проверки.

Перехват событий требует времени на обработку, это влияет на производительность других приложений и операционной системы.

> Если ваша ОС поддерживает технологию fanotify и соответствует требованиям, настройте использование обновляемого модуля ядра в работе приложения. Обновляемый модуль ядра входит в комплект поставки приложения. Использование обновляемого модуля ядра позволяет оптимизировать перехват системных событий.

Чтобы исключить файлы определенной директории не только из проверки, но и из перехвата, настройте исключение точек монтирования (глобальные исключения). Исключение точек монтирования позволяет исключать из перехвата файловых операций локальные или удаленные директории, смонтированные на устройстве.

Вы можете посмотреть список обнаруженных на устройстве точек монтирования с помощью Web Console, Консоли администрирования или командной строки. В списке отображается информация о том, добавлена ли точка монтирования в исключения из проверки.

Специалисты "Лаборатории Касперского" рекомендуют использовать глобальные исключения, если:

- соединение со смонтированным удаленным ресурсом, например NFS или SMB, работает медленно;
- критичны даже минимальные задержки в работе системы.

Вы можете указать тип точки монтирования (Local, AllRemoteMounted, Mounted:NFS, Mounted:SMB или Mounted:Custom) или конкретные точки монтирования. Приложение не отслеживает исключенные области.

> Для защиты общих сетевых ресурсов используйте приложение Kaspersky Endpoint Security на том устройстве, где ресурсы хранятся физически.

Если для перехвата системных событий вы используете обновляемый модуль ядра, из перехвата можно исключать конкретные локальные или удаленные директории, смонтированные на устройстве, а не только точки монтирования целиком.

> Если для перехвата системных событий вы используете механизм на основе технологии fanotify, для путей, которые не являются точками монтирования, глобальные исключения не действуют.

Вы можете настраивать глобальные исключения в политике с помощью Web Console или Консоли администрирования или локально на устройстве с помощью командной строки.

Пример настройки глобального исключения для директории /tmp с помощью командной строки

Чтобы исключить из перехвата все файлы в директории /tmp:

1. Если для перехвата системных событий вы используете механизм на основе технологии fanotify, проверьте, является ли директория /tmp точкой монтирования:

   ```
   mount
   ```

   Если директории нет в выводе команды mount:

   a. Создайте точку монтирования:

   ```
   mount --bind /tmp/ /tmp
   ```

   b. Добавьте следующую строку в файл /etc/fstab, чтобы созданная точка монтирования осталась в системе после перезагрузки:

   ```
   /tmp /tmp none defaults,bind 0 0
   ```

   Если для перехвата системных событий вы используете обновляемый модуль ядра, пропустите этот шаг.

2. Добавьте директорию /tmp в глобальные исключения:

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
   ```

3. Перезапустите приложение, чтобы применить глобальные исключения:

   ```
   systemctl restart kesl
   ```

Ограничение на использование оперативной памяти приложением

Вы можете ограничивать количество оперативной памяти, которое приложение Kaspersky Endpoint Security использует при проверке файлов компонентом Защита от файловых угроз и при выполнении задач проверки с типами ODS и ContainerScan.

Ограничение на использование памяти может быть полезным для систем с большим объемом оперативной памяти (более 5 ГБ).

По умолчанию ограничение на использование памяти приложением – 8192 МБ. Вы можете регулировать размер оперативной памяти, используемой приложением:

- В политике с помощью параметра **Ограничение на использование памяти для задач проверки (МБ)**.
- Локально на устройстве с помощью параметра `ScanMemoryLimit` в конфигурационном файле kesl.ini.

Если указанное значение параметра меньше 2 МБ, приложение будет использовать минимальное значение (2 МБ). Если указанное значение параметра превышает размер оперативной памяти устройства, приложение будет использовать до 25% оперативной памяти. Это значение изменить невозможно.

> Параметр ограничивает только количество памяти, которое используется при проверке файлов, то есть общий размер памяти, потребляемый приложением, может быть больше значения, заданного этим параметром.

Дополнительные рекомендации для Защиты от файловых угроз

Проверка только при открытии файла

Измените режим проверки файлов так, чтобы проверка выполнялась только при открытии файла. По умолчанию приложение проверяет файл при попытке открытия и повторно при попытке закрытия, если файл был изменен.

Вы можете изменить режим проверки файлов в параметрах Защиты от файловых угроз:

- В политике с помощью Web Console или Консоли администрирования: установите для параметра **Режим Защиты от файловых угроз** значение **При открытии**.
- Локально на устройстве:

  ```
  kesl-control --set-set 1 ScanByAccessType=Open
  ```

Изменения, внесенные в файл после открытия, не будут проверяться до следующего обращения к файлу.

Проверка архивов

Убедитесь, что проверка архивов выключена (значение по умолчанию). Проверка архивов снижает производительность из-за того, что доступ к файлу с архивом блокируется до того, как файл будет распакован во временную директорию /tmp и проверен. Под архивами имеются в виду как традиционные архивы, так и упакованные объекты, например типа .jar.

Вы можете включать и выключать проверку архивов с помощью Web Console или Консоли администрирования (параметр **Проверять архивы**) или локально на устройстве с помощью командной строки (параметр `ScanArchived`).

Проверка файлов, копируемых из сетевых директорий

Настройте исключение из проверки файлов, копируемых из сетевых директорий. Файлы будут проверяться только после завершения копирования в локальную директорию.

Для исключения из проверки файлов в сетевых директориях вам нужно настроить исключение по процессам для утилиты, предназначенной для копирования из сетевых директорий (например, для утилиты `cp`).

Если вы управляете приложением с помощью Kaspersky Security Center, вы можете настроить исключение по процессам в Web Console или в Консоли администрирования. Если вы управляете приложением с помощью командной строки, вы можете настроить исключение по процессам, добавив в параметры задачи типа OAS секцию `[ExcludedForProgram.item_#]`.

Дополнительные рекомендации для задач проверки

Расписание запуска задач

Настройте расписание запуска задач проверки так, чтобы задачи запускались в разное время. Приложение позволяет запускать задачи проверки одновременно, но потребление ресурсов может сильно увеличиться. Проверьте расписание всех задач типов ODS и ContainerScan локально на устройстве или через Kaspersky Security Center.

Запускайте проверку во время наименьшей нагрузки на сервер.

Проверка удаленных директорий

Убедитесь, что в область действия задач проверки не включены удаленные директории, смонтированные на устройстве по протоколам SMB и NFS.

Рекомендуется проверять эти директории непосредственно на устройстве, предоставляющем ресурс. Если такой возможности нет, не выполняйте проверку на серверах с критическими сервисами, так как такая задача может выполняться достаточно долго (в зависимости от скорости соединения и количества файлов).

Использование глобальных исключений и исключений Защиты от файловых угроз

Убедитесь, что в параметрах задачи Поиск вредоносного ПО включены параметры:

- **Использовать глобальные исключения** (`UseGlobalExclusions`) – исключать из проверки точки монтирования, указанные в глобальных исключениях.
- **Использовать исключения Защиты от файловых угроз** (`UseOASExclusions`) – использовать настроенные исключения Защиты от файловых угроз во время проверки.

По умолчанию оба параметра включены.

> В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE в качестве пути для исключения вы можете указать `/.snapshots/*/snapshot/`.

Рекомендации для Защиты от веб-угроз и Защиты от сетевых угроз

Общие рекомендации

Межсетевой экран операционной системы

Если в системе настроены свои (или firewalld) сетевые правила с Drop политиками, то для корректной работы приложения добавьте разрешающее правило для разрешения входящих соединений локального устройства (loopback).

Пример команды для iptables

```
iptables -A INPUT -i lo -j ACCEPT
```

Список контролируемых сетевых портов

Ограничьте список контролируемых приложением сетевых портов. По умолчанию приложение контролирует только выбранные сетевые порты. Если устройство использует подключение по протоколу SMB, убедитесь, что используется значение по умолчанию:

- В политике в Web Console или в Консоли администрирования: в параметрах проверки сетевого трафика выбран вариант **Контролировать только выбранные сетевые порты**.
- Локально на устройстве: параметр проверки сетевого трафика `MonitorNetworkPort` имеет значение `Selected`.

Использование приложения совместно с HAProxy

При использовании приложения совместно с балансировщиком HAProxy выполните следующие действия:

1. Откройте конфигурационный файл /var/opt/kaspersky/kesl/common/kesl.ini, создайте секцию `[Environment]` и добавьте в нее параметр `TcpSynInterceptDisabled=1`.
2. Перезапустите приложение:

   ```
   systemctl restart kesl
   ```

Использование приложения совместно с Kubernetes

Для совместной работы компонентов Защита от веб-угроз и Защита от сетевых угроз и кластера Kubernetes с сетевыми плагинами Calico и Cilium настройте параметры `WtpFwMark`, `NtpFwMark`, `BypassFwMark` и `BypassNflogMark` в конфигурационном файле kesl.ini.

Что делать при возникновении ошибки "Нарушена целостность модулей приложения"

Рекомендации для Защиты от веб-угроз

Политика проверки сертификатов

Компонент Защита от веб-угроз по умолчанию расшифровывает и проверяет сетевой трафик, передаваемый по защищенным соединениям. При этом компонент может использовать интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата.

Если устройство не имеет прямого выхода в интернет, выполните одно из следующих действий:

- Выберите локальный способ проверки сертификатов в параметрах проверки сетевого трафика:
  - В политике с помощью Web Console или Консоли администрирования: установите для параметра **Политика проверки сертификатов** значение **Локальная проверка**.
  - Локально на устройстве с помощью командной строки:

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  Приложение не будет использовать интернет для проверки сертификатов.

- Настройте использование прокси-сервера для доступа в интернет:
  - В политике с помощью Web Console или Консоли администрирования: настройте параметры прокси-сервера.
  - Локально на устройстве с помощью командной строки:

    Включить использование прокси-сервера с аутентификацией

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<user name>:<password>@<IP address of the proxy server>:<port number>
    ```

    Включить использование прокси-сервера без аутентификации

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<IP address of the proxy server>:<port number>
    ```

Рекомендации для Защиты от сетевых угроз

Совместимость с правилами REDIRECT

Чтобы обеспечить совместимость правил перехвата компонента Защита от сетевых угроз с правилами REDIRECT (например, перенаправление с 443 порта на 8443):

1. Удалите правило:

   ```
   iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
   ```

2. Добавьте вместо него следующие правила:

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports
8443
iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT
--to-destination :8443
```

Рекомендации для Анализа поведения

Рекомендуется исключить из проверки активность процессов, которые наиболее часто проверяются компонентом Анализ поведения.

Чтобы определить наиболее часто запускаемые процессы, выполните команду:

```
kesl-control --get-statistic --processes
```

Команда позволяет вывести список процессов, запуск которых приложение Kaspersky Endpoint Security обнаруживает наиболее часто, и количество этих запусков.

Вы можете настроить исключения в политике с помощью Web Console или Консоли администрирования или локально на устройстве с помощью командной строки.

По умолчанию из проверки исключается только указанный процесс, Анализ поведения продолжает проверять дочерние процессы исключенного процесса.

Примеры настройки исключений с помощью командной строки

Исключить из проверки активность приложений my_program1 и my_program2

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0001.ProgramPath=/bin/my_program2
```

Исключить из проверки активность приложения my_program1 и его дочерних процессов

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0000.ApplyToDescendants=Yes
```

Совместная работа с решениями "Лаборатории Касперского"

Приложение Kaspersky Endpoint Security поддерживает совместную работу с некоторыми решениями "Лаборатории Касперского". Для оптимальной совместной работы приложений воспользуйтесь рекомендациями, представленными в этом разделе.

Kaspersky Security Center Linux

При совместной работе Kaspersky Endpoint Security для Linux и Kaspersky Security Center Linux рекомендуем использовать настройки, описанные в этой статье.

Рекомендуемые настройки

Компонент приложения	Рекомендуемое состояние компонента	Рекомендации
Защита от файловых угроз	Включен	Добавьте исключения из защиты: • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent` • `/var/lib/postgresql/<PostgreSQL version>`
Поиск вредоносного ПО	Включен	
Проверка съемных дисков	Выключен	–
Анализ поведения	Включен	Используйте настройки по умолчанию.
Защита от сетевых угроз	Включен	Выберите режим перехвата сетевого трафика eBPF `NetInterceptorMode=UseEBPF`
Защита от веб-угроз	Включен	Используйте настройки по умолчанию.
Защита от шифрования	Выключен	–
Проверка контейнеров	Выключен	–
Инвентаризация	Выключен	–
Контроль устройств	Выключен	–
Контроль приложений	Выключен	–
Сетевой экран	Выключен	–
Веб-Контроль	Выключен	–
Контроль целостности системы	Включен	Добавьте области проверки: • /etc • /opt/kaspersky/kesl/ • /opt/kaspersky/ksc64
Проверка целостности системы	Выключен	–
Endpoint Detection and Response Expert (on-premises)	Включен	Используйте настройки по умолчанию.
Endpoint Detection and Response Expert (cloud)	Выключен	–
Managed Detection and Response	Включен	Используйте настройки по умолчанию.
Network Detection and Response (KATA)	Выключен	–
Интеграция с KUMA	Выключен	–
Sandbox	Выключен	–
Действия по реагированию	Есть ограничения	Для действий по реагированию невозможно исключить объекты, необходимые для работы Kaspersky Endpoint Security для Linux, а также критические объекты системы. При запуске действий по реагированию убедитесь, что их выполнение не нарушит работу системы и используемых приложений.
Графический интерфейс	Не установлен	–

Компонент приложения	Рекомендуемое состояние компонента	Рекомендации
Веб-плагин управления Kaspersky Endpoint Security для Linux	Установлен	Используйте настройки по умолчанию.
MMC-плагин управления Kaspersky Endpoint Security для Linux	Установлен	Используйте настройки по умолчанию.
Агент администрирования	Установлен	Используйте настройки по умолчанию.
Механизм перехвата файловых операций	Системный механизм перехвата на основе технологии fanotify	Используйте настройки по умолчанию.
Источник телеметрии системных событий	eBPF+auditd	`TelemetrySource=Default`
Защита от эксплойтов	Выключен	–
Использование Kaspersky Security Network	Включен	Используйте настройки по умолчанию.
Защита от почтовых угроз	Включен	Используйте настройки по умолчанию.
Защита от атак BadUSB	Выключен	–
Глобальные исключения	Настроены	Если вы устанавливаете Kaspersky Security Center с помощью скрипта быстрой установки, добавьте в исключения точки монтирования: `/var/lib/postgresql/<PostgreSQL version>/main` где `<PostgreSQL version>` – номер используемой версии СУБД PostgreSQL.

Network Detection and Response (KATA)

При совместной работе Kaspersky Endpoint Security для Linux и Network Detection and Response (KATA) рекомендуем использовать настройки, описанные в этой статье.

Также ознакомьтесь с документацией решения Kaspersky Anti Targeted Attack (KATA) Platform.

Настройки Kaspersky Endpoint Security для Linux на серверах с компонентом Sensor

Рекомендуемые настройки для серверов Sensor

Компонент приложения	Рекомендуемое состояние компонента	Рекомендации
Защита от файловых угроз	Включен	Добавьте исключения из защиты: • `[container-name:*kata_scanner*]/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*preprocessor_icap*]/tmp/content` • `[container-name:*preprocessor_span*]/tmp/suricata` • `[container-name:*preprocessor_span*]/mnt/kaspersky/nta` • `[container-name:*preprocessor_smtp*]/tmp/` • `[container-name:*preprocessor_pop*]/tmp/` • `[container-name:*sandbox_scan*]/tmp/` • `[container-name:*]/var/log/kaspersky`
Поиск вредоносного ПО	Выключен	–
Проверка съемных дисков	Выключен	–
Анализ поведения	Включен	Используйте настройки по умолчанию.
Защита от сетевых угроз	Выключен	–
Защита от веб-угроз	Выключен	–
Защита от шифрования	Выключен	–
Проверка контейнеров	Включен	Включите Мониторинг контейнеров для проверки в реальном времени запущенных контейнеров и пространств имен `NamespaceMonitoring=Yes`
Инвентаризация	Выключен	–
Контроль устройств	Выключен	–
Контроль приложений	Выключен	–
Сетевой экран	Выключен	–
Веб-Контроль	Выключен	–
Контроль целостности системы	Выключен	–
Проверка целостности системы	Выключен	–
Endpoint Detection and Response Expert (on-premises)	Выключен	–
Endpoint Detection and Response Expert (cloud)	Выключен	–
Managed Detection and Response	Выключен	–
Network Detection and Response (KATA)	Выключен	–
Интеграция с KUMA	Выключен	–
Sandbox	Выключен	–

Компонент приложения	Рекомендуемое состояние компонента	Рекомендации
Действия по реагированию	Выключены	–
Графический интерфейс	Не установлен	–
Агент администрирования	Установлен	Используйте настройки по умолчанию.
Механизм перехвата файловых операций	Системный механизм перехвата на основе технологии fanotify	Используйте настройки по умолчанию.
Источник телеметрии системных событий	eBPF+auditd	`TelemetrySource=Default`
Защита от эксплойтов	Выключен	–
Использование Kaspersky Security Network	Включен	Используйте настройки по умолчанию.
Защита от почтовых угроз	Выключен	–
Защита от атак BadUSB	Выключен	–
Файлы трассировки	–	Измените директорию для файлов трассировки на директорию вне каталога `/var/log/kaspersky`. Например, используйте директорию `/var/log/kesl`.
Глобальные исключения	Настроены	Исключите следующие точки монтирования: • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp/apttmp/*` • `/tmp/suricata/*` • `/tmp/traffic/*` • `/tmp/apt_certs/*` Исключение точек монтирования /tmp/apttmp/*, /tmp/suricata/*, /tmp/traffic/* и /tmp/apt_certs/* применяется для защиты серверов NDR (KATA) версии 8.0 и ниже. • `/varog/kaspersky` • `/var/opt/kaspersky` • `/data` • `/data/volumes/dumps`

Настройки Kaspersky Endpoint Security для Linux на серверах с компонентом Central Node

Рекомендуемые настройки для серверов Central Node

Компонент приложения	Рекомендуемое состояние компонента	Рекомендации
Защита от файловых угроз	Включен	Добавьте исключения из защиты: • `[container-name:*edr_synchronizer*]/tmp/` • `[container-name:*ids_alert_syncer*]/tmp/` • `[container-name:kata_product_main_1_kata_scanner]/storage` • `[container-name:kata_product_main_1_postgresql_server]/var/lib/postgresql` • `[container-name:kata_product_main_1_clickhouse]/var/lib/clickhouse` • `[container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/var/opt/kaspersky/apt-agents` • `[container-name:*kata_scanner*]/var/lib/nginx/body` • `[container-name:*kata_scanner*]/apt_spool` • `[container-name:*kata_scanner*]/tmp/` • `[container-name:*kafka*]/tmp/` • `[container-name:*ksn_proxy*]/tmp/` • `[container-name:*preprocessor_smtp*]/tmp/` • `[container-name:*preprocessor_pop*]/tmp/` • `[container-name:*preprocessor_icap*]/tmp/` • `[container-name:*preprocessor_span*]/tmp/` • `[container-name:*sandbox_scan*]/tmp/` • `[container-name:*statistics_clickhouse_importer*]/tmp/` • `[container-name:*updates_consistency_checker*]/tmp/` • `[container-name:*web_backend*]/tmp/` • `[container-name:*]/var/opt/kaspersky` • `/tmp/` • `/var/log/kaspersky`
Поиск вредоносного ПО	Выключен	–
Проверка съемных дисков	Выключен	–
Анализ поведения	Включен	Используйте настройки по умолчанию.
Защита от сетевых угроз	Выключен	–
Защита от веб-угроз	Выключен	–
Защита от шифрования	Выключен	–
Проверка контейнеров	Включен	Включите Мониторинг контейнеров для проверки в реальном времени запущенных контейнеров и пространств имен `NamespaceMonitoring=Yes`
Инвентаризация	Выключен	–
Контроль устройств	Выключен	–
Контроль приложений	Выключен	–
Сетевой экран	Выключен	–
Веб-Контроль	Выключен	–
Контроль целостности системы	Выключен	–
Проверка целостности системы	Выключен	–
Endpoint Detection and Response Expert (on-premises)	Выключен	–

Компонент приложения	Рекомендуемое состояние компонента	Рекомендации
Endpoint Detection and Response Expert (cloud)	Выключен	–
Managed Detection and Response	Выключен	–
Network Detection and Response (KATA)	Выключен	–
Интеграция с KUMA	Выключен	–
Sandbox	Выключен	–
Действия по реагированию	Выключены	–
Графический интерфейс	Не установлен	–
Агент администрирования	Установлен	Используйте настройки по умолчанию.
Механизм перехвата файловых операций	Системный механизм перехвата на основе технологии fanotify	Используйте настройки по умолчанию.
Источник телеметрии системных событий	eBPF+auditd	`TelemetrySource=Default`
Защита от эксплойтов	Выключен	–
Использование Kaspersky Security Network	Включен	Используйте настройки по умолчанию.
Защита от почтовых угроз	Выключен	–
Защита от атак BadUSB	Выключен	–
Файлы трассировки	–	Измените директорию для файлов трассировки на директорию вне каталога `/var/log/kaspersky`. Например, используйте директорию `/var/log/kesl`.
Глобальные исключения	Настроены	Добавьте в исключения точки монтирования: • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp/apttmp/*` • `/tmp/suricata/*` • `/tmp/traffic/*` • `/tmp/apt_certs/*` Исключение точек монтирования /tmp/apttmp/*, /tmp/suricata/*, /tmp/traffic/* и /tmp/apt_certs/* применяется для защиты серверов NDR (KATA) версии 8.0 и ниже. • `/var/log/kaspersky` • `/var/opt/kaspersky` • `/data`

Kaspersky Unified Monitoring and Analysis Platform

При совместной работе Kaspersky Endpoint Security для Linux и Kaspersky Unified Monitoring and Analysis Platform рекомендуем использовать настройки, описанные в этой статье.

Компонент приложения	Рекомендуемое состояние компонента	Рекомендации
Защита от файловых угроз	Включен	Добавьте исключения из защиты: • `/opt/kaspersky/kuma` • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent`
Поиск вредоносного ПО	Выключен	–
Проверка съемных дисков	Выключен	–
Анализ поведения	Включен	Исключите из проверки активность процесса `/opt/kaspersky/kuma`
Защита от сетевых угроз	Включен	Выключите блокирование скомпрометированного устройства `BlockAttackingHosts=No`
Защита от веб-угроз	Выключен	–
Защита от шифрования	Выключен	–
Проверка контейнеров	Выключен	–
Инвентаризация	Выключен	–
Контроль устройств	Выключен	–
Контроль приложений	Выключен	–
Сетевой экран	Выключен	–
Веб-Контроль	Выключен	–
Контроль целостности системы	Выключен	–
Проверка целостности системы	Выключен	–
Endpoint Detection and Response Expert (on-premises)	Выключен	–
Endpoint Detection and Response Expert (cloud)	Выключен	–
Managed Detection and Response	Выключен	–
Network Detection and Response (KATA)	Выключен	–
Интеграция с KUMA	Выключен	–
Sandbox	Выключен	–
Действия по реагированию	Выключены	–
Графический интерфейс	Не установлен	–
Агент администрирования	Установлен	Используйте настройки по умолчанию.
Механизм перехвата файловых операций	Системный механизм перехвата на основе технологии fanotify	Используйте настройки по умолчанию.
Источник телеметрии системных событий	eBPF+auditd	`TelemetrySource=Default`
Защита от эксплойтов	Выключен	–
Использование Kaspersky Security Network	Включен	Используйте настройки по умолчанию.
Защита от почтовых угроз	Выключен	–
Защита от атак BadUSB	Выключен	–

Справочник по компонентам приложения

Команды управления Kaspersky Endpoint Security

Управление приложением Kaspersky Endpoint Security в командной строке выполняется с помощью команд управления Kaspersky Endpoint Security.

Вы можете посмотреть справку по командам управления с помощью команды:

```
kesl-control --help <prefix of command group>
```

где `<prefix of command group>` может принимать следующие значения:

- `-A` – команды управления Контролем приложений.
- `-B` – команды управления резервным хранилищем.
- `-C` – команды управления общими параметрами проверки контейнеров.
- `-D` – команды управления Контролем устройств.
- `-E` – команды просмотра текущих событий приложения.
- `-F` – команды управления сетевым экраном.
- `-H` – команды управления устройствами, заблокированными Защитой от шифрования и Защитой от сетевых угроз.
- `-J` – команды управления сбором метрик о состоянии операционной системы.
- `-L` – команды управления лицензионными ключами.
- `-M` – команды управления параметрами интеграции приложения Kaspersky Endpoint Security с Kaspersky Unified Monitoring and Analysis Platform.
- `-N` – команды управления параметрами проверки защищенных соединений.
- `-Q` – команды управления карантином.
- `-R` – команды управления параметрами интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (cloud) и с Kaspersky Endpoint Detection and Response Optimum.
- `-S` – команды статистики.
- `-T` – команды управления задачами и параметрами приложения.
- `-U` – команды управления пользователями и ролями пользователей.
- `-V` – команды приложения в режиме Легкого агента.

- `-W` – команды вывода событий из журнала событий приложения.
- `-X` – команды управления параметрами интеграции приложения Kaspersky Endpoint Security с Sandbox.

В командной оболочке bash можно включить автоматическое дополнение команд kesl-control.

```
Включить автоматическое дополнение команды kesl-control в текущей сессии оболочки bash
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

```
Включить автоматическое дополнение для всех новых сессий оболочки bash
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~/.bashrc
```

Команды управления лицензионными ключами

`-L` – префикс указывает, что команда принадлежит к группе команд управления лицензионными ключами.

> Команды добавления и удаления лицензионных ключей могут быть выполнены, если приложение используется в стандартном режиме или в режиме EDR-агента. Если приложение используется в режиме Легкого агента, команды управления ключами завершаются с ошибкой.

kesl-control --add-active-key

Команда позволяет добавить в приложение активный лицензионный ключ с помощью файла ключа или кода активации.

С помощью этой команды вы можете добавлять ключи для активации приложения и ключи для активации компонентов, которые не включены в вашу лицензию. Указывать тип ключа в команде не требуется.

```
Добавить лицензионный ключ с помощью файла ключа
kesl-control [-L] --add-active-key <key file path>
```

```
Добавить лицензионный ключ с помощью кода активации
kesl-control [-L] --add-active-key <activation code>
```

Где:

`<key file path>` – путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.

`<activation code>` – код активации.

```
Пример добавления ключа с помощью файла /home/test/00000001.key в качестве активного ключа
kesl-control --add-active-key /home/test/00000001.key
```

kesl-control --add-reserve-key

Команда позволяет добавить в приложение резервный лицензионный ключ с помощью файла ключа или кода активации.

С помощью этой команды вы можете добавлять ключи для активации приложения и ключи для активации компонентов, которые не включены в вашу лицензию. Указывать тип ключа в команде не требуется.

> Если активный ключ еще не добавлен в приложение на устройстве, команда завершается с ошибкой.

Добавить резервный лицензионный ключ с помощью файла ключа

```
kesl-control [-L] --add-reserve-key <key file path>
```

Добавить резервный лицензионный ключ с помощью кода активации

```
kesl-control [-L] --add-reserve-key <activation code>
```

Где:

`<key file path>` – путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.

`<activation code>` – код активации.

Пример добавления резервного ключа с помощью файла /home/test/00000002.key

```
kesl-control --add-reserve-key /home/test/00000002.key
```

kesl-control --remove-active-key

Команда позволяет удалить активный лицензионный ключ.

Удалить активный лицензионный ключ EDR Optimum

```
kesl-control [-L] --remove-active-key [--edr-optimum]
```

Удалить активный лицензионный ключ KUMA

```
kesl-control [-L] --remove-active-key [--kuma]
```

Удалить активный лицензионный ключ MDR

```
kesl-control [-L] --remove-active-key [--mdr]
```

Удалить активный лицензионный ключ EDR Expert (on-premises)

```
kesl-control [-L] --remove-active-key [--edr-kata]
```

Удалить активный лицензионный ключ EDR Expert (cloud)

```
kesl-control [-L] --remove-active-key [--cxdr]
```

Удалить активный лицензионный ключ KWSM

```
kesl-control [-L] --remove-active-key [--khcs]
```

Где:

`--edr-optimum` – удалить активный лицензионный ключ EDR Optimum.

`--kuma` – удалить активный лицензионный ключ KUMA.

`--mdr` – удалить активный лицензионный ключ MDR.

`--edr-kata` – удалить активный лицензионный ключ EDR Expert (on-premises).

`--cxdr` – удалить активный лицензионный ключ EDR Expert (cloud).

`--khcs` – удалить активный лицензионный ключ KWSM.

Если в команде вы не укажете ключ `--edr-optimum`, `--kuma`, `--mdr`, `--edr-kata`, `--cxdr` или `--khcs`, в результате выполнения команды будет удален активный ключ, с помощью которого вы активировали приложение.

kesl-control --remove-reserve-key

Команда позволяет удалить резервный лицензионный ключ.

Удалить резервный лицензионный ключ EDR Optimum

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]
```

Удалить резервный лицензионный ключ KUMA

```
kesl-control [-L] --remove-reserve-key [--kuma]
```

Удалить резервный лицензионный ключ MDR

```
kesl-control [-L] --remove-reserve-key [--mdr]
```

Удалить резервный лицензионный ключ EDR Expert (on-premises)

```
kesl-control [-L] --remove-reserve-key [--edr-kata]
```

Удалить резервный лицензионный ключ EDR Expert (cloud)

```
kesl-control [-L] --remove-reserve-key [--cxdr]
```

Удалить резервный лицензионный ключ KWSM

```
kesl-control [-L] --remove-reserve-key [--khcs]
```

Где:

`--edr-optimum` – удалить резервный лицензионный ключ EDR Optimum.

`--kuma` – удалить резервный лицензионный ключ KUMA.

`--mdr` – удалить резервный лицензионный ключ MDR.

`--edr-kata` – удалить резервный лицензионный ключ EDR Expert (on-premises).

`--cxdr` – удалить резервный лицензионный ключ EDR Expert (cloud).

`--khcs` – удалить резервный лицензионный ключ KWSM.

Если в команде вы не укажете ключ `--edr-optimum`, `--kuma`, `--mdr`, `--edr-kata`, `--cxdr` или `--khcs`, в результате выполнения команды из приложения будет удален резервный ключ.

kesl-control -L --query

Команда позволяет вывести информацию о лицензии, по которой активировано приложение, и об используемых лицензионных ключах.

```
kesl-control -L --query [--json]
```

Где:

`--json` – выводить данные в формате JSON.

kesl-control --load-mdr-blob

Команда позволяет загрузить на устройство файл BLOB, который может использоваться при интеграции с Kaspersky Managed Detection and Response. Файл BLOB находится в ZIP-архиве конфигурационного файла MDR.

```
kesl-control [-L] --load-mdr-blob <path to MDR BLOB file>
```

kesl-control --remove-mdr-blob

Команда позволяет удалить с устройства файл BLOB, который может использоваться при интеграции с Kaspersky Managed Detection and Response.

```
kesl-control [-L] --remove-mdr-blob
```

Команды управления пользователями и ролями

-U – префикс указывает, что команда принадлежит к группе команд управления пользователями и ролями.

Управление ролями пользователей

Вывод списка пользователей и ролей

```
kesl-control [-U] --get-user-list
```

Назначение роли определенному пользователю

```
kesl-control [-U] --grant-role <role> <user>
```

Отзыв роли у определенного пользователя

```
kesl-control [-U] --revoke-role <role> <user>
```

Где:

`<user>` – имя пользователя или группы пользователей.

`<role>` – роль пользователя или группы пользователей.

Настройки Защиты паролем

Команды позволяют управлять Защитой паролем.

Включение или выключение Защиты паролем

```
kesl-control --set-permission-manager-settings Enabled=<Yes|No>
```

Просмотр текущих настроек Защиты паролем

```
kesl-control --get-permission-manager-settings
```

Изменение разрешений пользователя или группы пользователей

```
kesl-control --set-permissions <user> [--group] <permissions>=<Yes|No> [--file <file name>] [--json]
```

Просмотр текущих разрешений для пользователя или группы пользователей

```
kesl-control --get-permissions <user> [--group] [--file <file name>] [--json]
```

Удаление пользователя или группы пользователей, для которых настроены разрешения

```
kesl-control --remove-permissions <user> [--group]
```

Где:

`<user>` – имя пользователя или группы пользователей.

`<permissions>` – пользовательские разрешения.

`--group` – применить к группе пользователей. Если ключ не указан, параметр применяется к отдельному пользователю.

`--file <path to file>` – сохранить или импортировать параметры в конфигурационный файл. Если ключ не указан, результат команды будет выведен в консоли.

`--json` – выводить параметры в формате JSON.

Управление политикой на устройстве

> Для выключения политики на устройстве пользователю необходимо разрешение "Выключение политики Kaspersky Security Center".

Если пользователь выключил политику на устройстве, после перезагрузки устройства или Kaspersky Endpoint Security политика снова становится активной.

Выключить политику на устройстве

```
kesl-control --disable-policy
```

Применить политику к устройству

```
kesl-control --enable-policy
```

Управление параметрами и задачами приложения

`-T` – префикс указывает, что команда принадлежит к группе команд управления параметрами и задачами приложения.

`-C` – префикс указывает, что команда принадлежит к группе команд управления общими параметрами проверки контейнеров.

`-N` – префикс указывает, что команда принадлежит к группе команд управления параметрами проверки сетевого трафика.

kesl-control --export-settings

Команда позволяет вывести в консоль или экспортировать в конфигурационный файл все параметры приложения (включая общие параметры проверки контейнеров, параметры проверки защищенных соединений, общие параметры приложения и параметры задач).

```
kesl-control [-T] --export-settings [--file <path to file>] [--json]
```

Где:

`--file <path to file>` – полный путь к конфигурационному файлу, в который будут сохранены параметры приложения.

`--json` – выводить параметры в формате JSON.

kesl-control --import-settings

Предоставляйте доступ к конфигурационному файлу только доверенным пользователям. Перед импортом параметров в приложение проверяйте пути к каталогам, файлам настроек, исполняемым файлам, карантину. Не импортируйте конфигурационный файл из недоверенных источников. Компрометация конфигурационного файла может оказать влияние на безопасность, целостность или работоспособность инфраструктуры вашей организации, а также пользовательских данных.

Команда позволяет импортировать из конфигурационного файла все параметры приложения (включая общие параметры проверки контейнеров, параметры проверки защищенных соединений, общие параметры приложения и параметры задач).

```
kesl-control [-T] --import-settings --file <path to configuration file> [--json]
```

Где:

`--file <path to file>` – полный путь к конфигурационному файлу, параметры из которого будут импортированы в приложение.

`--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

kesl-control --update-application

Команда позволяет установить загруженное обновление модулей приложения.

Команда не может быть выполнена, если приложение используется в режиме Легкого агента.

```
kesl-control [-T] --update-application
```

Команды управления общими параметрами приложения

kesl-control --get-app-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения общих параметров приложения.

```
kesl-control [-T] --get-app-settings [--file <path to file>] [--json]
```

Где:

`--file <path to file>` – путь к конфигурационному файлу, в который будут выведены общие параметры приложения. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON.

kesl-control --set-app-settings

Команда позволяет устанавливать значения общих параметров приложения с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Задать параметры с помощью ключей команды

```
kesl-control [-T] --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Задать параметры с помощью конфигурационного файла

```
kesl-control [-T] --set-app-settings --file <path to file> [--json]
```

Где:

`<setting name>=<setting value>` – имя и значение одного из общих параметров приложения.

`--file <path to file>` – полный путь к конфигурационному файлу, параметры из которого будут импортированы в приложение.

`--json` – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команды управления параметрами задач

kesl-control --get-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения параметров указанной задачи.

```
kesl-control [-T] --get-settings <task ID|name> [--file <path to file>] [--json]
```

Где:

`<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`--file <path to file>` – путь к конфигурационному файлу, в который будут выведены параметры задачи. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON.

kesl-control --set-settings

Команда позволяет устанавливать значения параметров указанной задачи с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Задать параметры с помощью ключей команды

```
kesl-control [-T] --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>] [--add-path <path>] [--del-path <path>] [--add-exclusion <path>] [--del-exclusion <path>]
```

Задать параметры с помощью конфигурационного файла

```
kesl-control [-T] --set-settings <task ID/name> --file <path to file> [--json]
```

Где:

`<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`<setting name>=<setting value>` – имя и значение одного из параметров задачи.

`--add-path <path>` – добавить путь к директории с проверяемыми объектами.

`--del-path <path>` – удалить путь к директории с проверяемыми объектами.

`--add-exclusion <path>` – добавить путь к директории с объектами, которые нужно исключить из проверки.

`--del-exclusion <path>` – удалить путь к директории с исключаемыми объектами.

`--file <path to file>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры задачи.

`--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

kesl-control --set-to-default

Команда позволяет восстановить значения по умолчанию для параметров указанной задачи.

```
kesl-control [-T] --set-settings <task ID|name> --set-to-default
```

Где:

`<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

kesl-control --get-schedule

Команда позволяет вывести в консоль или в конфигурационный файл текущее расписание запуска указанной задачи.

```
kesl-control [-T] --get-schedule <task ID|name> [--file <path to file>] [--json]
```

Где:

`<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`--file <path to file>` – путь к конфигурационному файлу, в который будут выведены параметры расписания задачи. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON.

kesl-control --set-schedule

Команда позволяет устанавливать расписание указанной задачи с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Задать параметры с помощью ключей команды

```
kesl-control [-T] --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

Задать параметры с помощью конфигурационного файла

```
kesl-control [-T] --set-schedule <task ID|name> --file <path to file> [--json]
```

Где:

`<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`<setting name>=<setting value>` – имя и значение одного из параметров расписания задач.

`--file <path to file>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры расписания задачи.

`--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команды управления задачами

kesl-control --get-task-list

Команда позволяет вывести список существующих задач приложения.

```
kesl-control [-T] --get-task-list [--json]
```

Где:

`--json` – выводить параметры в формате JSON.

Для каждой задачи отображается следующая информация:

- `Name` – имя задачи.
- `ID` – идентификатор задачи.

- `Type` – тип задачи.
- `State` – текущее состояние задачи.

Если политика Kaspersky Security Center запрещает пользователям просматривать и изменять локальные задачи, информация о задачах `Scan_My_Computer`, `Critical_Areas_Scan`, `Container_Scan`, `Inventory_Scan`, `Update` и `Rollback` недоступна.

kesl-control --get-task-state

Команда позволяет вывести состояние указанной задачи.

```
kesl-control [-T] --get-task-state <task ID|name> [--json]
```

Где:

`<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`--json` – выводить параметры в формате JSON.

Для задач приложения предусмотрены следующие состояния:

- `Started` – задача запущена
- `Starting` – задача запускается
- `Stopped` – задача остановлена
- `Stopping` – задача останавливается

Задачи типов `ODS`, `ODFIM` и `InventoryScan` могут также находиться в одном из следующих состояний:

- `Pausing` – приостанавливается
- `Suspended` – приостановлена
- `Resuming` – возобновляется

kesl-control --create-task

Команда позволяет создать задачу указанного типа с параметрами по умолчанию или с параметрами, указанными в конфигурационном файле.

Создавать можно только пользовательские задачи. Предустановленные задачи недоступны для создания.

В зависимости от режима использования приложения можно создавать пользовательские задачи следующих типов:

- стандартный режим: `ODS`, `Update`, `Rollback`, `ODFIM`, `ContainerScan` и `InventoryScan`;
- режим Легкого агента: `ODS`, `ODFIM`, `ContainerScan` и `InventoryScan`.

Создать задачу с параметрами по умолчанию

```
kesl-control [-T] --create-task <task name> --type <task type>
```

Создать задачу с параметрами из конфигурационного файла

```
kesl-control [-T] --create-task <task name> --type <task type> [--file <path to file>] [--json]
```

Где:

`<task name>` – имя, которое вы задаете для новой задачи.

`<task type>` – обозначение типа создаваемой задачи.

`--file <path to file>` – полный путь к конфигурационному файлу, параметры из которого будут использоваться при создании задачи.

`--json` – импортировать параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

kesl-control --delete-task

Команда позволяет удалить задачу.

Удалять можно только пользовательские задачи. Предустановленные задачи недоступны для удаления.

```
kesl-control [-T] --delete-task <task ID|name>
```

Где:

`<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

kesl-control --start-task

Команда позволяет запустить задачу.

Можно запускать все предустановленные и пользовательские задачи, кроме задачи типа `License`.

```
kesl-control [-T] --start-task <task ID|name> [-W] [--progress]
```

Где:

`<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`-W` – включить вывод текущих событий.

`--progress` – отображать ход выполнения задачи.

Пример запуска задачи с идентификатором 1 и включением вывода текущих событий, связанных с задачей

```
kesl-control --start-task 1 -W
```

Если при запуске задачи произошла ошибка и задача не запустилась, то после перезапуска приложения выполняется повторная попытка запуска задачи.

kesl-control --stop-task

Команда позволяет остановить задачу.

Можно останавливать все предустановленные и пользовательские задачи, кроме задачи типа `License`.

```
kesl-control [-T] --stop-task <task ID|name> [-W]
```

Где:

`<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`-W` – включить вывод текущих событий.

kesl-control --suspend-task

Команда позволяет приостановить задачу.

Можно приостановить только задачи типов `ODS`, `ODFIM` и `InventoryScan`.

```
kesl-control [-T] --suspend-task <task ID|name>
```

Где:

`<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

kesl-control --resume-task

Команда позволяет возобновить выполнение задачи.

Можно возобновить только задачи типов `ODS`, `ODFIM` и `InventoryScan`.

```
kesl-control [-T] --resume-task <task ID|name>
```

Где:

`<task ID|name>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

kesl-control --scan-file

Команда позволяет создать и запустить задачу выборочной проверки.

```
kesl-control [-T] --scan-file <path> [--action <action>]
```

Где:

`<path>` – путь к файлу или директории, которые нужно проверить. Вы можете указать несколько путей, разделяя их пробелами.

`--action <action>` – действие, которое приложение будет выполнять над зараженными объектами. Если вы не укажете ключ `--action`, приложение будет выполнять рекомендуемое действие.

kesl-control --scan-container

Команда позволяет создать и запустить задачу выборочной проверки контейнера или образа.

```
kesl-control [-T] --scan-container <ID|name[:tag]>
```

Где:

`<ID|name[:tag]>` – имя или идентификатор контейнера или образа. Для проверки нескольких объектов можно использовать маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Команды управления общими параметрами проверки контейнеров

kesl-control --get-container-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения общих параметров проверки контейнеров.

```
kesl-control [-C] --get-container-settings [--file <path to file>] [--json]
```

Где:

`--file <path to file>` – путь к конфигурационному файлу, в который будут выведены общие параметры проверки контейнеров. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON.

kesl-control --set-container-settings

Команда позволяет устанавливать значения общих параметров проверки контейнеров с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Задать параметры с помощью ключей команды

```
kesl-control [-C] --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Задать параметры с помощью конфигурационного файла

```
kesl-control [-C] --set-container-settings --file <path to file> [--json]
```

Где:

`<setting name>=<setting value>` – имя и значение одного из общих параметров проверки контейнеров.

`--file <path to file>` – полный путь к конфигурационному файлу, из которого в приложение будут импортированы общие параметры проверки контейнеров.

`--json` – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Команды управления параметрами проверки сетевого трафика

`-N` – префикс указывает, что команда принадлежит к группе команд управления параметрами проверки сетевого трафика.

kesl-control -N --query

Команда позволяет выводить списки исключений из проверки зашифрованных соединений:

- список исключений, добавленных пользователем;
- список исключений, добавленных приложением;
- список исключений, полученных из баз приложения.

Вывести список исключений, добавленных пользователем

```
kesl-control -N --query user
```

Вывести список исключений, добавленных приложением

```
kesl-control -N --query auto
```

Вывести список исключений, полученных из баз приложения

```
kesl-control -N --query kl
```

kesl-control --clear-web-auto-excluded

Команда позволяет очистить список доменов, которые приложение автоматически исключило из проверки.

```
kesl-control -N --clear-web-auto-excluded
```

kesl-control --get-net-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения параметров проверки сетевого трафика.

```
kesl-control [-N] --get-net-settings [--file <path to file>] [--json]
```

Где:

`--file <path to file>` – путь к конфигурационному файлу, в который будут выведены параметры проверки сетевого трафика. Если вы не укажете ключ `--file`, параметры будут выведены в консоль.

Если вы укажете имя файла без пути, файл будет создан в текущей директории. Если файл существует по указанному пути, он будет перезаписан. Если указанная директория не существует, конфигурационный файл не будет создан.

`--json` – выводить параметры в формате JSON.

kesl-control --set-net-settings

Команда позволяет устанавливать значения параметров проверки сетевого трафика с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Задать параметры с помощью ключей команды

```
kesl-control [-N] --set-net-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Задать параметры с помощью конфигурационного файла

```
kesl-control [-N] --set-net-settings --file <path to file> [--json]
```

Где:

`<setting name>=<setting value>` – имя и значение одного из параметров проверки сетевого трафика.

`--file <path to file>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры проверки сетевого трафика.

`--json` – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

kesl-control --list-certificates

Команда позволяет вывести список доверенных корневых сертификатов.

```
kesl-control [-N] --list-certificates
```

kesl-control --add-certificate

Команда позволяет добавить сертификат в список доверенных корневых сертификатов.

```
kesl-control [-N] --add-certificate <path to certificate>
```

Где:

`<path to certificate>` – путь к файлу сертификата, который вы хотите добавить, в формате PEM или DER.

kesl-control --remove-certificate

Команда позволяет удалить сертификат из списка доверенных корневых сертификатов.

```
kesl-control [-N] --remove-certificate <certificate subject>
```

kesl-control --add-bypass-endpoints

Команда позволяет добавить исключение из перехвата трафика.

```
kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

Где:

`<in|out>` – направление трафика в исключаемом соединении: входящий или исходящий.

`<remote IP address>` – адрес удаленного устройства в формате IPv4 или IPv6. При исключении входящего трафика из перехвата будет исключаться трафик с указанного IP-адреса. При исключении исходящего трафика из перехвата будет исключаться трафик на указанный IP-адрес.

`<destination port>` – порт на защищенном устройстве (исключение для входящего трафика) или порт на удаленном устройстве (исключение для исходящего трафика). Трафик на этот порт исключается из перехвата.

kesl-control --list-bypass-endpoints

Команда позволяет просмотреть список настроенных исключений из перехвата трафика.

```
kesl-control [-N] --list-bypass-endpoints
```

kesl-control --remove-bypass-endpoints

Команда позволяет удалить исключение из перехвата трафика.

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

Где:

`<in|out>` – направление трафика в исключаемом соединении: входящий или исходящий.

`<remote IP address>` – адрес удаленного устройства в формате IPv4 или IPv6, трафик на который или с которого исключается из перехвата (в зависимости от направления трафика).

`<destination port>` – порт на защищенном устройстве (исключение для входящего трафика) или порт на удаленном устройстве (исключение для исходящего трафика).

Мониторинг состояния и защиты

Команды статистики

-S – префикс указывает, что команда принадлежит к группе команд статистики.

kesl-control --app-info

Команда позволяет вывести информацию о приложении.

```
kesl-control [-S] --app-info [--json] [--check-permissions]
```

Где:

`--json` – выводить параметры в формате JSON.

`--check-permissions` – выводить пути к директориям приложения с неверно настроенными правами.

kesl-control --supported-tech-info

Команда позволяет вывести список функций приложения, информацию об их статусах (используется или не используется) и технологиях Linux, с помощью которых реализованы эти функции приложения.

```
kesl-control [-S] --supported-tech-info [--json]
```

Где:

`--json` – выводить функции в формате JSON.

kesl-control --get-statistic

Команда позволяет вывести статистику о работе приложения и список точек монтирования, обнаруженных на устройстве.

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

Где:

`--files` – статистика о файлах, которые наиболее часто проверяет компонент Защита от файловых угроз, и количество обращений компонента к этим файлам.

`--processes` – статистика о процессах, запуск которых приложение Kaspersky Endpoint Security обнаруживает наиболее часто, и количество этих запусков.

> Исключение процессов из проверки компонентом Анализ поведения не удаляет их из статистики, но увеличивает производительность приложения Kaspersky Endpoint Security.

`--mountpoints` – список точек монтирования. В выводе пути к точкам монтирования отсортированы следующим образом:

- статичные, системные, служебные и другие точки монтирования;
- смонтированные пакеты snap и точки монтирования внутри их пространств имен;
- точки монтирования, созданные системой управления контейнерами Docker.

Вы можете указать один или несколько ключей в любой комбинации или не указать ни одного ключа. Если вы не укажете ключи, приложение выведет три списка: статистику о наиболее часто проверяемых файлах, статистику о наиболее часто запускаемых процессах и список обнаруженных на устройстве точек монтирования.

kesl-control --omsinfo

Команда позволяет создать файл формата JSON для интеграции с Microsoft Operations Management Suite.

```
kesl-control [-S] --omsinfo --file <path to file>
```

Команда вывода событий

`-W` – префикс указывает на команду вывода событий из журнала событий приложения.

kesl-control -W

Команда включает вывод текущих событий приложения. Команда возвращает название события и дополнительную информацию о событии. Вы можете использовать команду для вывода всех текущих событий приложения или только событий, связанных с запущенной задачей.

```
kesl-control -W [--query "<filter conditions>"]
```

Где:

`<filter conditions>` – одно или несколько логических выражений в формате `<field> <comparison operation> '<value>'`, скомбинированных с помощью логического оператора `and`, для вывода определенных текущих событий.

Команды управления событиями приложения

-E – префикс указывает, что команда принадлежит к группе команд управления событиями приложения.

kesl-control -E

Команда позволяет вывести информацию обо всех событиях из журнала событий приложения. С помощью утилиты `less` вы можете перемещаться по списку отображаемых событий.

```
kesl-control -E
```

kesl-control -E --query

Команда позволяет вывести информацию о событиях из журнала событий приложения. С помощью утилиты `less` вы можете перемещаться по списку отображаемых событий. Вы можете использовать фильтр для вывода определенных событий, а также выводить список событий в указанный файл.

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--file <path to file>] [--
json] [--reverse]
```

Где:

`<database file>` – полный путь к файлу базы данных журнала событий, из которого вы хотите вывести события. По умолчанию приложение сохраняет информацию о событиях в базе данных /var/opt/kaspersky/kesl/private/storage/events.db. Расположение базы данных определяется общим параметром приложения `EventsStoragePath`.

`<filter conditions>` – одно или несколько логических выражений в формате `<field> <comparison operator> '<value>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.

`<number>` – количество последних событий из выборки (то есть количество записей от конца выборки), которые нужно вывести.

`--file <path to file>` – полный путь к файлу, в который вы хотите вывести события. Если вы укажете имя файла, не указав путь к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, файл не будет создан.

Если вы не укажете ключ `--file`, список событий будет выведен в консоль.

`--json` – выводить события в формате JSON.

`--reverse` – выводить события в обратном порядке (от самого нового события наверху к более старым внизу).

Команда управления сбором метрик о состоянии системы

kesl-control --export-metrics

Команда позволяет настроить сбор метрик о состоянии операционной системы.

```
kesl-control [-J] --export-metrics [--period <interval in seconds between exports>|--interactive]
```

Где:

`--period` – периодический вывод результатов в командную строку;

`<interval in seconds between exports>` – интервал времени между выводами результатов команды в командную строку (в секундах);

`--interactive` – интерактивный вывод (по нажатию клавиши **Enter**).

Контроль безопасности

Команды управления Контролем устройств

-D – префикс указывает, что команда принадлежит к группе команд управления контролем устройств.

Управление параметрами Контроля устройств

Посмотреть текущие параметры Контроля устройств

```
kesl-control --get-settings 15 [--file <path to file>] [--json]
```

Изменить параметры Контроля приложений

```
kesl-control --set-settings 15 [<setting>=<value>] [--file <path to file>] [--json]
```

Где:

`<setting>=<value>` – параметр и значение Контроля устройств.

--file <path to file> – сохранить или импортировать параметры в конфигурационный файл. Если ключ не указан, результат команды будет выведен в консоли.

`--json` – выводить данные в формате JSON.

Управление устройствами

Просмотреть список подключенных устройств

```
kesl-control [-D] --get-device-list [--all] [--json] [--export <file>]
```

Где:

`--all` – выводить список всех подключенных устройств.

`--json` – выводить список подключенных устройств в формате JSON.

`--export <file>` – экспортировать список подключенных устройств в JSON-файл. Экспорт выполняется в формате списка подключенных устройств.

Приложение Kaspersky Endpoint Security отобразит следующую информацию о подключенных устройствах:

- **Тип устройства**. Тип подключенного устройства. Например, `OpticalDrive` или `HardDrive`.
- **Идентификатор**. Идентификатор подключенного устройства.
- **Название**. Название подключенного устройства.
- **Путь**. Путь к устройству в виртуальной операционной системе sysfs.
- **Системный диск**. Параметр показывает, является ли подключенное устройство системным диском (да или нет).
- **Шина**. Шина подключения. Возможные значения: `UnknownBus`, `USB`, `FireWire`.
- **Драйвер**. Название используемого драйвера, читаемое виртуальной операционной системой sysfs.

Доверенные устройства

Команда позволяет просматривать список доверенных устройств, добавлять в него устройства и удалять из него устройства, а также импортировать список доверенных устройств из файла.

```
kesl-control [-D] --trusted-devices [--list] [--add <ID>] [--delete <ID>] [--merge|--add|--replace --file <file>]
```

Где:

`--list` – вывести список доверенных устройств.

`--add <ID>` – добавить устройство в список доверенных устройств по идентификатору или маске идентификатора устройства.

`--delete <ID>` – удалить устройство из списка доверенных устройств по идентификатору или маске идентификатора устройства.

`--merge` – объединить списки доверенных устройств при импорте. Если в текущем списке и в импортируемом списке есть записи для устройства с одним и тем же идентификатором, то параметры существующей записи изменяются. Для устройств, которых нет в текущем списке, записи добавляются.

`--add` – дополнить текущий список доверенных устройств при импорте. В список устройств добавляются только записи для устройств, которых ранее не было.

`--replace` – заменить текущий список доверенных устройств. Существующий список доверенных устройств заменяется импортируемым списком.

`--file <file>` – импортировать список доверенных устройств из указанного файла. Вам нужно указать полный путь к файлу в формате JSON.

Временный доступ к заблокированному устройству

Команды позволяют создать файл запроса и загрузить ключ доступа, чтобы получить временный доступ к заблокированному устройству:

Создать файл запроса

```
kesl-control [-D] --request-temporary-device-access --device-id <device ID> --access-duration <access duration> --path <path to access request file>
```

Загрузить ключ доступа

```
kesl-control [-D] --upload-temporary-device-access-key --path <access key>
```

Где:

`--device-id <device ID>` – идентификатор заблокированного устройства, к которому вы хотите получить доступ.

`--access-duration <access duration>` – период времени, на который вы хотите получить доступ к устройству (в часах). Возможные значения: 1–100.

`--path <path to access request file>` – путь к директории, в которой вы хотите сохранить файл запроса доступа с расширением .akey.

`--path <access key>` – путь к файлу с ключом доступа к устройству (файлу с расширением .acode).

Команды управления Контролем приложений

-A – префикс указывает, что команда принадлежит к группе команд управления контролем приложений.

Управление задачей Инвентаризация

Посмотреть список приложений, обнаруженных на клиентском устройстве

```
kesl-control [-A] --get-app-list [--json]
```

Где:

`--json` – выводить данные в формате JSON.

Просмотр категорий приложений

Посмотреть список созданных категорий Контроля приложений

```
kesl-control [-A] --get-categories [--names <name of category 1> <name of category 2> ... <name of category N>] [--file <path to file>] [--json]
```

Где:

`<category name 1> <category name 2> ... <category name N>` – названия категорий. Если вы хотите просмотреть информацию о нескольких категориях, укажите названия категорий через пробел.

`--file <path to file>` – сохранить или импортировать параметры в конфигурационный файл. Если ключ не указан, результат команды будет выведен в консоли.

`--json` – выводить данные в формате JSON.

Управление категориями приложений

Создать категорию приложений:

1. Выведите список категорий приложений в конфигурационный файл:

```
kesl-control --set-categories --file <path to file>
```

2. Добавьте категории приложений в следующем виде:

```
[
   {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 2>"
   }
]
```

Для указания пути к файлу в полях `Exclude` и `Include` вы можете использовать маски.

3. Импортируйте список категорий в приложение:

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --
file <path to file>
```

Изменить список категорий Контроля приложений

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --file
<path to file>
```

Где:

`FilePath like <application>` – полный путь к исполняемому файлу приложения.

`FileHash == <hash>` – SHA256-хеш исполняемого файла приложений.

`<category ID>` – уникальный идентификатор категории. Обязательный параметр. Указывайте `GUID` без дефисов.

`<category name 1> <category name 2> ... <category name N>` – названия категорий. Обязательный параметр.

Если вы хотите изменить информацию о нескольких категориях, укажите названия категорий через пробел. Если вы не укажете название категории, она не будет создана или будет удалена из списка существующих категорий.

`--file <path to file>` – сохранить или импортировать параметры в конфигурационный JSON-файл.

Управление параметрами Контроля приложений

Посмотреть текущие параметры Контроля приложений

```
kesl-control --get-settings 21 [--file <path to file>] [--json]
```

Изменить параметры Контроля приложений

```
kesl-control --set-settings 21 [<setting>=<value>] [--file <path to file>] [--json]
```

Где:

`<setting>=<value>` – параметр и значение Контроля приложений.

`--file <path to file>` – сохранить или импортировать параметры в конфигурационный файл. Если ключ не указан, результат команды будет выведен в консоли.

`--json` – выводить данные в формате JSON.

Вернуть параметры по умолчанию

Удалить список категорий приложений и правил Контроля приложений и восстановить значения параметров по умолчанию

```
kesl-control --set-settings 21 --set-to-default
```

Полезные статьи

Как задавать маски

Вы можете использовать символ * (любая последовательность символов) или символ ? (один любой символ) для формирования маски имени файла или директории.

Вы можете указать символ * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/*/file*/` или `/dir/file*/`.

Вы можете указать символ ? вместо любого одного символа (включая символ `/`) в имени файла или директории.

Команды управления Веб-Контролем

Управление параметрами Веб-Контроля

Посмотреть текущие параметры Веб-Контроля

```
kesl-control --get-settings 26 [--file <path to file>] [--json]
```

Изменить параметры Веб-Контроля

```
kesl-control --set-settings 26 [<setting>=<value>] [--file <path to file>] [--json]
```

Где:

`<setting>=<value>` – параметр и значение Веб-Контроля. Вы можете изменить любое количество параметров.

`--file <path to file>` – сохранить или импортировать параметры в конфигурационный файл. Если ключ не указан, результат команды будет выведен в консоли.

`--json` – выводить данные в формате JSON.

Вернуть параметры по умолчанию

Удалить настроенные параметры и восстановить значения параметров Веб-Контроля по умолчанию

```
kesl-control --set-settings 26 --set-to-default
```

Защита сетевых соединений

Команды управления заблокированными устройствами

-H – префикс указывает, что команда принадлежит к группе команд управления устройствами, заблокированными Защитой от шифрования и Защитой от сетевых угроз.

kesl-control --get-blocked-hosts

Команда позволяет вывести в консоль список заблокированных устройств.

```
kesl-control [-H] --get-blocked-hosts
```

kesl-control --allow-hosts

Команда позволяет разблокировать заблокированные устройства.

```
kesl-control [-H] --allow-hosts <address>
```

Где:

`<address>` – IP-адрес устройства или подсети (IPv4/IPv6, включая адреса в короткой форме). Вы можете указать несколько IP-адресов устройств или подсетей, разделяя их пробелами.

Команды управления сетевым экраном

-F – префикс указывает, что команда принадлежит к группе команд управления сетевым экраном.

kesl-control --add-rule

Команда позволяет добавить новое сетевое пакетное правило.

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

Где:

`--name <rule name>` – название сетевого пакетного правила.

`--action <Allow|Block>` – действие, применяемое к соединениям, указанным в сетевом пакетном правиле.

`--protocol <protocol>` – тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность.

`--direction <direction>` – направление отслеживаемой сетевой активности.

`--remote <remote address>:<port>` – сетевой адрес удаленного устройства.

`--local <local address>:<port>` – сетевой адрес устройства с установленным приложением Kaspersky Endpoint Security.

`--at <index>` – порядковый номер правила в списке сетевых пакетных правил. Если ключ `--at` не указан или его значение больше количества правил в списке, новое правило добавляется в конец списка.

Для параметров, значения которых вы не указали в команде, устанавливаются значения по умолчанию.

kesl-control --del-rule

Команда позволяет удалить сетевое пакетное правило с указанным названием или с указанным индексом в списке правил.

Удалить сетевое пакетное правило с помощью названия правила

```
kesl-control [-F] --del-rule --name <rule name>
```

Удалить сетевое пакетное правило с помощью порядкового номера правила

```
kesl-control [-F] --del-rule --index <index>
```

Где:

`--name <rule name>` – название сетевого пакетного правила.

`--index <index>` – порядковый номер правила в списке сетевых пакетных правил.

kesl-control --move-rule

Команда позволяет изменить приоритет выполнения сетевого пакетного правила.

Изменить приоритет выполнения сетевого пакетного правила с помощью названия правила

```
kesl-control [-F] --move-rule --name <rule name> --at <index>
```

Изменить приоритет выполнения сетевого пакетного правила с помощью порядкового номера правила

```
kesl-control [-F] --move-rule --index <index> --at <index>
```

Где:

`--name <rule name>` – название сетевого пакетного правила.

`--index <index>` – текущий порядковый номер правила в списке сетевых пакетных правил.

`--at <index>` – новый порядковый номер правила в списке сетевых пакетных правил.

kesl-control --add-zone

Команда позволяет добавить адрес в сетевую зону.

```
kesl-control [-F] --add-zone --zone <zone> --address <address>
```

Где:

`--zone <zone>` – предустановленное имя сетевой зоны.

`--address <address>` – сетевой адрес или подсеть.

kesl-control --del-zone

Команда позволяет удалить адрес из сетевой зоны.

Удалить адрес из сетевой зоны, указав адрес или подсеть

```
kesl-control [-F] --del-zone --zone <zone> --address <address>
```

Удалить адрес из сетевой зоны с помощью порядкового номера адреса

```
kesl-control [-F] --del-zone --zone <zone> --index <address index>
```

Где:

`--zone <zone>` – предустановленное имя сетевой зоны.

`--address <address>` – сетевой адрес или подсеть.

`--index <address index>` – порядковый номер адреса в сетевой зоне.

kesl-control -F --query

Команда позволяет посмотреть правила сетевого экрана, созданные с помощью приложения Kaspersky Endpoint Security.

```
kesl-control -F --query
```

Защита от сложных угроз и целевых атак

Команды управления карантином

-Q – префикс указывает, что команда принадлежит к группе команд управления карантином.

kesl-control -Q --mass-remove

Команда позволяет удалить из карантина все или только указанные файлы.

Удалить все файлы

```
kesl-control -Q --mass-remove
```

Удалить файлы, соответствующие условиям фильтра

```
kesl-control -Q --mass-remove --query "<filter conditions>"
```

Где:

`<filter conditions>` – одно или несколько логических выражений в формате `<field> <comparison operator> '<value>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.

kesl-control --put

> Команда доступна только при интеграции Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Optimum или с Kaspersky Managed Detection and Response.

Команда позволяет поместить файл на карантин.

```
kesl-control [-Q] --put <file path> [--md5] [--sha256] [--save-original-file]
```

Где:

`<file path>` – путь к файлу, который вы хотите поместить на карантин.

`--md5` – хеш-сумма MD5 файла, который вы хотите поместить на карантин.

`--sha256` – хеш-сумма SHA256 файла, который вы хотите поместить на карантин.

`--save-original-file` – не удалять исходный файл. Если вы не укажете этот ключ, исходный файл будет удален.

kesl-control -Q --query

Команда позволяет вывести информацию о файлах на карантине.

```
Вывести информацию обо всех файлах на карантине
kesl-control -Q --query [-n <number>] [--json]
```

```
Вывести информацию о файлах на карантине, соответствующих условиям фильтра
kesl-control -Q --query ["<filter conditions>"] [-n <number>]
```

Где:

`<filter conditions>` – одно или несколько логических выражений в формате `<field> <comparison operator> '<value>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса. Если вы не укажете условия фильтра, приложение выведет информацию обо всех файлах на карантине.

`<number>` – количество последних файлов на карантине, которые нужно вывести. Если вы не укажете ключ `-n`, будут выведены последние 30 файлов. Для отображения всех файлов укажите значение 0.

`--json` – выводить данные в формате JSON.

kesl-control -Q --restore

Команда позволяет восстановить файл из карантина.

```
kesl-control -Q --restore <file ID> [--file <file path>]
```

Где:

`<file ID>` – идентификатор файла на карантине.

`--file <file path>` – новое имя файла и путь к директории, в которой его требуется сохранить. Если вы не укажете ключ `--file`, файл будет восстановлен с исходным именем в исходное местоположение. Если директория удалена или у пользователя нет прав доступа к этой ней, приложение помещает файл в директорию /var/opt/kaspersky/kesl/common/restored/. Вы можете вручную переместить файл из этой директории в нужную директорию.

Команды управления компонентом EDR Expert (on-premises)

-R – префикс указывает, что команда принадлежит к группе команд управления параметрами интеграции с решениями Detection and Response от "Лаборатории Касперского".

kesl-control --add-kataedr-server-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат сервера KATA, сервера действий по реагированию OSMP или сервера сбора телеметрии OSMP (в зависимости от режима интеграции).

```
kesl-control [-R] --add-kataedr-server-certificate <file> [--server-type <response|telemetry>]
```

Где:

`<file>` – путь к файлу, содержащему сертификат сервера.

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (on-premises) выбор сервера, сертификат которого нужно добавить или заменить:

- `response` – сервер действий по реагированию OSMP;
- `telemetry` – сервер сбора телеметрии OSMP.

Если вы добавляете или заменяете сертификат сервера KATA, не указывайте ключ `--server-type`.

kesl-control --remove-kataedr-server-certificate

Команда позволяет удалить сертификат сервера KATA, сервера действий по реагированию OSMP или сервера сбора телеметрии OSMP (в зависимости от режима интеграции).

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type <response|telemetry>]
```

Где:

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (on-premises) выбор сервера, сертификат которого нужно удалить:

- `response` – сервер действий по реагированию OSMP;
- `telemetry` – сервер сбора телеметрии OSMP.

Если вы удаляете сертификат сервера KATA, не указывайте ключ `--server-type`.

kesl-control --query-kataedr-server-certificate

Команда позволяет вывести информацию о сертификате сервера KATA, сервера действий по реагированию OSMP или сервера сбора телеметрии OSMP (в зависимости от режима интеграции).

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

Где:

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (on-premises) выбор сервера, информацию о котором нужно вывести:

- `response` – сервер действий по реагированию OSMP;
- `telemetry` – сервер сбора телеметрии OSMP.

Если вы хотите посмотреть информацию о сертификате сервера KATA, не указывайте ключ `--server-type`.

kesl-control --add-kataedr-client-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат клиента, используемый для защиты подключения к серверу KATA, серверу действий по реагированию OSMP или серверу сбора телеметрии OSMP (в зависимости от режима интеграции).

```
kesl-control [-R] --add-kataedr-client-certificate <file>  [--server-type <response|telemetry>]
```

Где:

`<file>` – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

> Необходимо указать пароль от криптоконтейнера. В противном случае при нажатии **`Enter`** отобразится ошибка `Certificate password is required and cannot be empty`.

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (on-premises) выбор сервера, для которого нужно добавить клиентский сертификат:

- `response` – сервер действий по реагированию OSMP;
- `telemetry` – сервер сбора телеметрии OSMP.

Если вы добавляете или заменяете клиентский сертификат для подключения к серверу KATA, не указывайте ключ `--server-type`.

kesl-control --remove-kataedr-client-certificate

Команда позволяет удалить сертификат клиента, используемый для защиты подключения к серверу KATA, серверу действий по реагированию OSMP или серверу сбора телеметрии OSMP (в зависимости от режима интеграции).

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type <response|telemetry>]
```

Где:

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (on-premises) выбор сервера, для которого нужно удалить клиентский сертификат:

- `response` – сервер действий по реагированию OSMP;
- `telemetry` – сервер сбора телеметрии OSMP.

Если вы удаляете клиентский сертификат, используемый для подключения к серверу KATA, не указывайте ключ `--server-type`.

kesl-control --query-kataedr-client-certificate

Команда позволяет вывести информацию о сертификате клиента, используемого для защиты подключения к серверу KATA, серверу действий по реагированию OSMP или серверу сбора телеметрии OSMP (в зависимости от режима интеграции).

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

Где:

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (on-premises) выбор сервера, для которого нужно вывести информацию о клиентском сертификате:

- `response` – сервер действий по реагированию OSMP;
- `telemetry` – сервер сбора телеметрии OSMP.

Если вы хотите посмотреть информацию о клиентском сертификате, используемом для подключения к серверу KATA, не указывайте ключ `--server-type`.

Команды управления компонентом EDR Expert (cloud)

-R – префикс указывает, что команда принадлежит к группе команд управления параметрами интеграции с решениями Detection and Response от "Лаборатории Касперского".

kesl-control --query-cloudxdr-server-certificate

Команда позволяет вывести информацию о сертификате сервера действий по реагированию OSMP или сервера сбора телеметрии OSMP.

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type <response|telemetry>
```

Где:

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (cloud) выбор сервера, информацию о котором нужно вывести:

- `response` – сервер действий по реагированию OSMP;
- `telemetry` – сервер сбора телеметрии OSMP.

kesl-control --query-cloudxdr-client-certificate

Команда позволяет вывести информацию о сертификате клиента, используемого для защиты подключения к серверу действий по реагированию OSMP или серверу сбора телеметрии OSMP.

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type <response|telemetry>
```

Где:

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (cloud) выбор сервера, для которого нужно вывести информацию о клиентском сертификате:

- `response` – сервер действий по реагированию OSMP;
- `telemetry` – сервер сбора телеметрии OSMP.

Команды управления компонентом NDR (KATA)

-R – префикс указывает, что команда принадлежит к группе команд управления параметрами интеграции с решениями Detection and Response от "Лаборатории Касперского".

kesl-control --add-katandr-server-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат сервера NDR.

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

Где:

`<file>` – путь к файлу, содержащему сертификат сервера.

kesl-control --remove-katandr-server-certificate

Команда позволяет удалить сертификат сервера NDR.

```
kesl-control [-R] --remove-katandr-server-certificate
```

kesl-control --query-katandr-server-certificate

Команда позволяет вывести информацию о сертификате сервера NDR.

```
kesl-control [-R] --query-katandr-server-certificate
```

kesl-control --add-katandr-client-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат клиента, используемый для защиты подключения к серверу NDR.

```
kesl-control [-R] --add-katandr-client-certificate <file>
```

Где:

`<file>` – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

> Необходимо указать пароль от криптоконтейнера. В противном случае при нажатии **`Enter`** отобразится ошибка `Certificate password is required and cannot be empty`.

kesl-control --remove-katandr-client-certificate

Команда позволяет удалить сертификат клиента, используемый для защиты подключения к серверу NDR.

```
kesl-control [-R] --remove-katandr-client-certificate
```

kesl-control --query-katandr-client-certificate

Команда позволяет вывести информацию о сертификате клиента.

```
kesl-control [-R] --query-katandr-client-certificate
```

Команды управления сетевой изоляцией устройства

-R – префикс указывает, что команда принадлежит к группе команд управления параметрами интеграции с решениями Detection and Response от "Лаборатории Касперского". Сетевая изоляция устройств применяется как действие по реагированию на обнаружение угрозы при интеграции с указанными решениями Detection and Response.

kesl-control --isolation-stat

Команда позволяет вывести в консоль текущее состояние сетевой изоляции: включена или выключена.

```
kesl-control [-R] --isolation-stat
```

kesl-control --isolation-off

Команда позволяет временно выключить сетевую изоляцию устройства.

```
kesl-control [-R] --isolation-off
```

Команды управления параметрами интеграции с KUMA

-M – префикс указывает, что команда принадлежит к группе команд управления параметрами интеграции с Kaspersky Unified Monitoring and Analysis Platform.

kesl-control --add-kuma-server-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат сервера KUMA.

```
kesl-control [-M] --add-kuma-server-certificate <path to file>
```

Где:

`<path to file>` – путь к файлу формата DER или PEM, содержащему сертификат сервера.

kesl-control --remove-kuma-server-certificate

Команда позволяет удалить сертификат сервера KUMA.

```
kesl-control [-M] --remove-kuma-server-certificate
```

kesl-control --query-kuma-server-certificate

Команда позволяет вывести информацию о сертификате сервера KUMA.

```
kesl-control [-M] --query-kuma-server-certificate
```

kesl-control --add-kuma-client-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат клиента, используемый для защиты подключения к серверу KUMA.

```
kesl-control [-M] --add-kuma-client-certificate <path to file>
```

Где:

`<path to file>` – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

> Необходимо указать пароль от криптоконтейнера. В противном случае при нажатии **`Enter`** отобразится ошибка `Certificate password is required and cannot be empty`.

kesl-control --remove-kuma-client-certificate

Команда позволяет удалить сертификат клиента, используемый для защиты подключения к серверу KUMA.

```
kesl-control [-M] --remove-kuma-client-certificate
```

kesl-control --query-kuma-client-certificate

Команда позволяет вывести информацию о сертификате клиента.

```
kesl-control [-M] --query-kuma-client-certificate
```

Команды управления параметрами интеграции с Sandbox

-X – префикс указывает, что команда принадлежит к группе команд управления параметрами интеграции с Sandbox.

kesl-control --add-sandbox-server-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат сервера, обеспечивающего взаимодействие с Sandbox.

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

Где:

`<file>` – путь к файлу формата DER или PEM, содержащему сертификат сервера.

kesl-control --remove-sandbox-server-certificate

Команда позволяет удалить сертификат сервера, обеспечивающего взаимодействие с Sandbox.

```
kesl-control [-X] --remove-sandbox-server-certificate
```

kesl-control --query-sandbox-server-certificate

Команда позволяет вывести информацию о сертификате сервера, обеспечивающего взаимодействие с Sandbox.

```
kesl-control [-X] --query-sandbox-server-certificate
```

kesl-control --add-sandbox-client-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат клиента, используемый для защиты подключения к серверу, обеспечивающему взаимодействие с Sandbox.

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

Где:

`<file>` – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

> Необходимо указать пароль от криптоконтейнера. В противном случае при нажатии **`Enter`** отобразится ошибка `Certificate password is required and cannot be empty`.

kesl-control --remove-sandbox-client-certificate

Команда позволяет удалить сертификат клиента, используемый для защиты подключения к серверу, обеспечивающего взаимодействие с Sandbox.

```
kesl-control [-X] --remove-sandbox-client-certificate
```

kesl-control --query-sandbox-client-certificate

Команда позволяет вывести информацию о сертификате клиента.

```
kesl-control [-X] --query-sandbox-client-certificate
```

kesl-control --sandbox

Команда позволяет отправить файлы в Sandbox на проверку.

```
kesl-control [-X] --sandbox <path 1> <path 2>
```

Где:

`<path>` – путь к файлу или директории, которые вы хотите проверить. Вы можете указать несколько путей, разделяя их пробелами.

Команды управления поиском IOC

`-T` – префикс указывает, что команда принадлежит к группе команд управления параметрами и задачами приложения.

kesl-control --scan-ioc

Команда запускает поиск индикаторов компрометации на устройстве (IOC).

```
kesl-control [-T] --scan-ioc --path <path to directory or file> [--process on|off] [--hint <regular expression>]
[--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--
excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

Где:

`--path <path to directory or file>` – путь к IOC-файлу или директории с IOC-файлами с расширением .IOC или .XML, с помощью которых требуется выполнить проверку.

> Вы можете указать несколько путей, разделяя их пробелами. Вы также можете указать оба типа путей (к файлу и к директории).

`--process` – включение анализа процессов, запущенных на устройстве.

Возможные аргументы:

- `on` – включить анализ процессов, запущенных на устройстве (значение по умолчанию).
- `off` – выключить анализ процессов, запущенных на устройстве.

Если вы не укажете ключ `--process`, приложение выполнит анализ процессов, только если в используемом IOC-файле указаны данные этих процессов (`ProcessItem`).

`--hint <regular expression>` – регулярное выражение, которому соответствует полный путь к файлу (`FileItem`) или исполняемому файлу процесса (`ProcessItem`), который требуется проанализировать.

Вы можете использовать следующие элементы регулярных выражений:

- метасимволы: `.` `^` `$` `|`
- классы символов: `digit`, `alpha`, `lower`, `upper`, `cntrl`
- квантификаторы: `*` `+` `?` `{n}` `{n,}` `{n, m}`
- отрицание: `[^a-c]`
- экранируемые символы: `\a` `\e` `\f`, `\n` `\r` `\t` `\v` `\b`

`--arpentry` – включение анализа записей в ARP-таблице (`ArpEntryItem`).

Возможные аргументы:

- `on` – включить анализ записей в ARP-таблице (значение по умолчанию).
- `off` – выключить анализ записей в ARP-таблице.

Если вы не укажете ключ `--arpentry`, приложение выполнит анализ таблицы ARP, только если в используемом IOC-файле указаны данные этой таблицы (`ArpEntryItem`).

`--ports` – включение анализа портов, открытых для соединения.

Возможные аргументы:

- `on` – включить анализ портов, открытых для соединения и проверять активные соединения на устройстве (значение по умолчанию).
- `off` – выключить анализ портов, открытых для соединения и не проверять активные соединения на устройстве.

Если вы не укажете ключ `--ports`, приложение выполнит анализ портов, только если в используемом IOC-файле указаны данные этих портов (`PortItem`).

`--system` – включение анализа окружения системы.

Возможные аргументы:

- `on` – включить анализ окружения системы (значение по умолчанию).
- `off` – выключить анализ окружения системы.

Если вы не укажете ключ `--system`, приложение выполнит анализ окружения системы только если в используемом IOC-файле указаны данные об окружении системы (`SystemInfoItem`).

`--files` – включение анализа файлов.

Возможные аргументы:

- `on` – включить анализ файлов (значение по умолчанию).
- `off` – выключить анализ файлов.

Если вы не укажете ключ `--files`, приложение выполнит анализ файлов, только если в используемом IOC-файле указаны данные этих файлов (`FileItem`).

`--drives` – области, подлежащие проверке.

Возможные аргументы:

- `all` – проверять все доступные файловые области.
- `system` – проверять все файлы в пределах корневой файловой системы.

- `critical` – проверять файлы в пользовательских и системных директориях (значение по умолчанию).
- `custom` – проверять только файлы в указанных вами областях.

Если вы не укажете ключ `--drives`, приложение выполнит анализ файлов в пользовательских и системных директориях.

`--excludes <list of exclusions>` – список путей, исключаемых из проверки.

Исключения, заданные этим ключом, являются глобальными и действуют независимо от типа области или списка директорий. Такие исключения имеют приоритет над другими ключами, включая `--hint` и `--scope`.

> Исключения задаются в виде путей, но не могут содержать рекурсивные элементы или символы маски (например, `*`).

Если вы не укажете ключ `--excludes`, проверка будет выполнена без исключений.

Вы можете указать несколько исключений, разделяя их пробелом.

`--scope <list of directories>` – список дополнительных директорий, подлежащих проверке.

> Этот ключ является обязательным, если для ключа `--drives` вы указали аргумент `custom`.

`--action` – действие, выполняемое при обнаружении индикаторов компрометации.

Возможные аргументы:

- `Skip` – приложение не будет выполнять никаких действий с обнаруженным объектом, но информация о нем сохранится в результатах выполнения задачи (значение по умолчанию).
- `QuarantineFile` – приложение поместит обнаруженный объект на карантин.
- `IsolateHost` – приложение изолирует от сети устройство, на котором обнаружен объект.
- `ScanCriticalAreas` – приложение выполнит проверку важных областей.

Важные области, которые проверяет Kaspersky Endpoint Security

- /lib/systemd
- /lib/udev
- /lib/dbus-1.0
- /usr/local/lib/systemd/user
- /usr/share/dbus-1
- /usr/share/gdm/autostart
- /usr/share/gnome/autostart

- /var/spool/at
- /var/spool/at/spool
- /var/spool/anacron
- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

Вы можете указать несколько действий, разделяя их запятыми.

> Если вы указали аргумент `Skip`, остальные аргументы добавлять не нужно. Аргумент `Skip` может использоваться только самостоятельно.

kesl-control --get-response-task-list

Команда выводит информацию о запущенных задачах *Поиск IOC* на устройстве.

```
kesl-control [-T] --get-response-task-list
```

В результате приложение покажет информацию о запущенных задачах в следующем виде:

Идентификатор задачи: <task ID>

Действие по реагированию: locScan

Дата создания: <date and time of task creation>

Запуск задачи: <task launch schedule>

Состояние: <task status>

Kaspersky Endpoint Security обновляет информацию о запущенных задачах *Поиск IOC* при каждой синхронизации с сервером. Вы можете настроить период синхронизации в параметрах интеграции с решением Detection and Response от "Лаборатории Касперского" (параметр `SynchronizationPeriod`). По умолчанию приложение выполняет синхронизацию с сервером каждые 5 минут.

kesl-control --delete-response-task <task ID>

Команда удаляет задачу *Поиск IOC* по идентификатору. Приложение удаляет задачу на компьютере локально. Если вы не удалили задачу в Web Console или консоли OSMP, приложение восстановит эту задачу при следующей синхронизации с сервером.

```
kesl-control [-T] --delete-response-task-list <task ID>
```

Команды приложения в режиме Легкого агента

-V – префикс указывает, что команда принадлежит к группе команд приложения Kaspersky Endpoint Security, используемого в режиме Легкого агента.

> Команды могут быть выполнены, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента.

kesl-control --ksvla-info

Команда позволяет вывести информацию об использовании приложения в режиме Легкого агента.

```
kesl-control --ksvla-info
```

kesl-control --viis-info

Команда позволяет вывести информацию о подключении приложения в режиме Легкого агента к Серверу интеграции.

```
kesl-control --viis-info
```

kesl-control --svm-info

Команда позволяет вывести информацию о подключении приложения в режиме Легкого агента к SVM.

```
kesl-control --svm-info
```

Параметры приложения в командной строке

Задача Обновление

В таблице ниже описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Обновление (`Update`).

Параметры задачи Обновление

Параметр	Описание	Значения
`ConnectionTimeout`	Время ожидания (в секундах) ответа от источника обновлений при попытке соединения с ним. Если в течение указанного промежутка времени от источника обновлений не приходит ответ, приложение обращается к другому указанному источнику обновлений.	Вы можете указывать только целые числа в диапазоне от 0 до 120. Значение по умолчанию: 10.
`ApplicationUpdateMode`	Режим загрузки и установки автоматически устанавливаемых обновлений приложения (автопатчей).	`Disabled` – не загружать и не устанавливать автопатчи. `DownloadOnly` (значение по умолчанию) – автоматически загружать автопатчи, но не устанавливать их. `DownloadAndInstall` – автоматически загружать и устанавливать автопатчи. После установки автопатча будет автоматически перезапущено.
Секция **[Sources.item_#]** содержит следующие параметры:		
`Enabled`	Использование источника обновлений, указанного в параметре `SourceType`. Для выполнения задачи требуется включить использование хотя бы одного источника обновлений.	`Yes` (значение по умолчанию) – приложение использует источник обновлений. `No` – приложение не использует источник обновлений.

Параметр	Описание	Значения
`SourceType`	Источник, из которого приложение будет получать обновления.	`KLServers` (значение по умолчанию) – приложение получает обновления с одного из серверов обновлений "Лаборатории Касперского". Обновления загружаются по протоколу HTTPS. `SCServer` – приложение загружает обновления на защищаемое устройство с установленного в локальной сети Сервера администрирования. Вы можете выбрать этот источник обновлений, если вы используете Kaspersky Security Center для централизованного управления защитой устройств в вашей организации. `Custom` – приложение загружает обновления из пользовательского источника, указанного в параметре `URL`. Вы можете указывать директории FTP-, HTTP- и HTTPS-серверов или директории на любом смонтированном устройстве защищаемого клиентского устройства, включая директории на удаленных устройствах, смонтированные по протоколам Samba или NFS.
`URL`	Адрес пользовательского источника обновлений в локальной сети или в интернете.	Значение по умолчанию не задано. Примеры: `URL=http://example.com/bases/` – адрес HTTP-сервера, на котором расположена директория с обновлениями. `URL=/home/bases/` – директория на защищаемом устройстве, в которой содержатся базы приложения.

Защита устройств от угроз

Задача Защита от файловых угроз

В командной строке вы можете управлять защитой от файловых угроз с помощью предустановленной задачи Защита от файловых угроз (`File_Threat_Protection`).

Задача Защита от файловых угроз запущена по умолчанию. Вы можете запускать и останавливать эту задачу вручную.

Для запуска и остановки задачи Защита от файловых угроз из командной строки требуются права роли Администратор.

Вы можете настраивать параметры защиты от файловых угроз, изменяя параметры предустановленной задачи Защита от файловых угроз.

В таблице ниже описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Защита от файловых угроз.

Параметр	Описание	Значения
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения. Не рекомендуется включать этот параметр, так как проверка архивов снижает производительность из-за того, что доступ к файлу с архивом блокируется до того, как файл будет распакован во временную директорию и проверен.	`Yes` – проверять архивы. Если для параметра `ActionOnThreat` указано значение `DisinfectDeleteIfNotPossible` и лечение невозможно, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` (значение по умолчанию) – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` – проверять самораспаковывающиеся архивы. `No` (значение по умолчанию) – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронной почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
`SkipPlainTextFiles`	Временное исключение из проверки файлов в текстовом формате. Параметр позволяет оптимизировать проверку журналов работы приложений. Параметр применяется, если вы используете механизм перехвата системных событий на основе технологии fanotify. При использовании обновляемого модуля ядра проверка оптимизирована за счет применения кеша результатов проверки.	`Yes` – не проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. `No` (значение по умолчанию) – проверять файлы в текстовом формате.
`SkipDatabaseJournals`	Временное исключение из проверки файлов журналов баз данных. Параметр позволяет оптимизировать проверку журналов баз данных. Параметр применяется, если вы используете механизм перехвата системных событий на основе технологии fanotify. При использовании обновляемого модуля ядра проверка оптимизирована за счет применения кеша результатов проверки.	`Yes` – не проверять файлы журналов баз данных, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. `No` (значение по умолчанию) – проверять файлы журналов баз данных.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.

Параметр	Описание	Значения
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 60.
`ActionOnThreat`	Выбор действия, которое приложение будет выполнять над зараженными объектами.	`DisinfectDeleteIfNotPossible` (лечить; удалять, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. `DisinfectBlockIfNotPossible` (лечить; блокировать, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение блокирует доступ к зараженному объекту. `Block` (блокировать) – приложение блокирует доступ к зараженному объекту. Значение по умолчанию: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Включение исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Исключение из проверки объектов по именам или маскам.
	С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Включение исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats.item_#`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию о незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.

Параметр	Описание	Значения
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию о проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию о необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам. Параметр неприменим для устройств с процессором Эльбрус.	`Yes` (значение по умолчанию) – включить эвристический анализатор. `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет. Параметр неприменим для устройств с процессором Эльбрус.	`Light` – наименее тщательная проверка, минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) – рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.
`ScanByAccessType`	Режим работы задачи Защита от файловых угроз. Параметр `ScanByAccessType` применяется только в задаче Защита от файловых угроз.	`SmartCheck` (значение по умолчанию) – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс во время своей работы многократно обращается к файлу в течение некоторого времени и изменяет его, повторно проверять файл только при последней попытке закрытия файла этим процессом. `OpenAndModify` – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. `Open` – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: `All objects`. Пример `AreaDesc="Scanning of email databases"`
`UseScanArea`	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	`Yes` (значение по умолчанию) – проверять указанную область. `No` – не проверять указанную область.

Параметр	Описание	Значения
`AreaMask.item_#`	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (проверять все объекты). Пример `AreaMask_item_<item number>=*doc`
`Path`	Путь к директории с проверяемыми объектами.	`<path to local folder>` – проверять объекты в указанной директории. Для указания пути вы можете использовать маски и теги. `Shared:NFS` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. `Shared:SMB` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. `Mounted:NFS` – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `AllShared` – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. `<file system type>` – проверять все ресурсы указанной файловой системы устройства.
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из проверки.	`Yes` (значение по умолчанию) – исключать указанную область. `No` – не исключать указанную область.
`AreaMask.item_#`	Ограничение области исключения из проверки. В области исключения приложение не проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает из проверки все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать из проверки все объекты).
`Path`	Путь к директории с исключаемыми объектами.	`<path to local folder>` – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать маски и теги. `Mounted:NFS` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `<file system>` – исключать из проверки все ресурсы указанной файловой системы устройства.
Секция **[ExcludedForProgram.item_#]** содержит следующие параметры:		

Параметр	Описание	Значения
`ProgramPath`	Путь к исключаемому процессу. Если для перехвата системных событий используется обновляемый модуль ядра, указанный процесс исключается из перехвата во всех пространствах имен.	`<path to process>` – исключать из проверки процесс в указанной локальной директории.
`ApplyToDescendants`	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром `ProgramPath`.	`Yes` – исключать из проверки указанный процесс и все его дочерние процессы. `No` (значение по умолчанию) – исключать из проверки только указанный процесс, не исключать из проверки дочерние процессы.
`AreaDesc`	Описание области исключения процессов.	Значение по умолчанию: `All objects`.
`UseExcludedForProgram`	Исключение указанной области из проверки.	`Yes` (значение по умолчанию) – исключать указанную область. `No` – не исключать указанную область.
`AreaMask.item_#`	Ограничение области исключения процессов. В области исключения процессов приложение не проверяет только файлы, указанные помощью масок в формате shell. Если параметр не указан, приложение исключает из проверки все объекты в области исключения процессов. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать из проверки все объекты).
`Path`	Путь к директории с файлами, которые изменяет процесс.	`<path to local folder>` – исключать из проверки объекты в указанной директории. Для указания пути можно использовать маски. `Shared:NFS` – исключать из проверки ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. `Shared:SMB` – исключать из проверки ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. `Mounted:NFS` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `AllShared` – исключать из проверки все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. `<file system type>` – исключать из проверки все ресурсы указанной файловой системы устройства.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Как использовать теги

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Где:

`<id>` – идентификатор контейнера.

`<name>` – имя контейнера.

`<path to local directory>` – путь к локальной директории.

Также вы можете использовать уникальные комбинации из тегов `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` и `[image-name:<name>]/path to local directory>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

Оптимизация проверки сетевых директорий

Для оптимизации защиты от файловых угроз вы можете настроить исключение из проверки файлов, копируемых из сетевых директорий в локальную директорию. Для этого вам нужно настроить исключение по процессам для утилиты, предназначенной для копирования из сетевых директорий (например, для утилиты `cp`).

Чтобы настроить исключение сетевых директорий из проверки:

1. Выведите параметры задачи Защита от файловых угроз (`File_Threat_Protection`, ID:1) в конфигурационный файл с помощью команды:

   ```
   kesl-control --get-settings 1 --file <full path to the configuration file> [--json]
   ```

2. Откройте конфигурационный файл и добавьте секцию `[ExcludedForProgram.item_#]` со следующими параметрами:

   - `ProgramPath` – путь к исключаемому процессу или к директории с исключаемыми процессам.
   - `ApplyToDescendants` – параметр, показывающий, нужно ли исключать из проверки дочерние процессы исключаемого процесса (возможные значения: `Yes` или `No`).
   - `AreaDesc` – описание области исключения по процессам, содержащее дополнительную информацию об области исключения.
   - `UseExcludedForProgram` – включить исключение указанной области при работе задачи (возможные значения: `Yes` или `No`).
   - `Path` – путь к файлам или к директории с файлами, которые изменяет процесс.
   - `AreaMask.item_#` – маска имени файла для файлов, которые вы хотите исключить из проверки. Вы также можете указать полный путь к файлу.

   Пример

   ```
   [ExcludedForProgram.item_0000]
   ProgramPath=/usr/bin/cp
   ApplyToDescendants=No
   AreaDesc=
   UseExcludedForProgram=Yes
   Path=AllRemoteMounted
   AreaMask.item_0000=*
   ```

3. Выполните команду:

   ```
   kesl-control --set-settings 1 --file <full path to the configuration file> [--json]
   ```

   Укажите ключ `--json`, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

Приложение не будет проверять файлы в сетевых директориях, при этом сама команда `cp` (для приведенного выше примера) и локальные файлы будут проверяться.

Поиск вредоносного ПО

В командной строке вы можете выполнять проверку на наличие вредоносного ПО следующими способами:

- С помощью предустановленной задачи Поиск вредоносного ПО (`Scan_My_Computer`). Вы можете запускать, останавливать, приостанавливать и возобновлять эту задачу вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры проверки, изменяя параметры этой задачи.

- С помощью пользовательских задач поиска вредоносного ПО (задач типа `ODS`). Вы можете запускать, останавливать, приостанавливать и возобновлять пользовательские задачи вручную и настраивать расписание запуска задач.

Вы можете выполнять *выборочную проверку* указанных файлов и директорий с помощью следующей команды:

```
kesl-control --scan-file
```

Задача Поиск вредоносного ПО

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Поиск вредоносного ПО (`Scan_My_Computer`).

Параметры задачи Поиск вредоносного ПО

Параметр	Описание	Значения
`ScanFiles`	Включение проверки файлов.	`Yes` (значение по умолчанию) – проверять файлы. `No` – не проверять файлы.
`ScanBootSectors`	Включение проверки загрузочных секторов.	`Yes` (значение по умолчанию) – проверять загрузочные секторы. `No` – не проверять загрузочные секторы.
`ScanComputerMemory`	Включение проверки памяти процессов и памяти ядра.	`Yes` (значение по умолчанию) – проверять память процессов и память ядра. `No` – не проверять память процессов и память ядра.
`ScanStartupObjects`	Включение проверки объектов автозапуска.	`Yes` (значение по умолчанию) – проверять объекты автозапуска. `No` – не проверять объекты автозапуска.
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	`Yes` (значение по умолчанию) – проверять архивы. Если для параметра `ActionOnThreat` указано значение `DisinfectDeleteIfNotPossible` и лечение невозможно, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` (значение по умолчанию) – проверять самораспаковывающиеся архивы. `No` – не проверять самораспаковывающиеся архивы.

Параметр	Описание	Значения
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронной почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
`QueueScanTasks`	Отложенный запуск задач проверки, запланированных по расписанию, если запущенная ранее проверка по расписанию еще выполняется. Kaspersky Endpoint Security ставит запланированные задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, запланировано запускать задачу проверки в 18:00 и в 20:00. Задача проверки, которая должна запуститься в 20:00, будет отложена, если задача проверки, запущенная в 18:00, еще выполняется. Задача запустится после завершения задачи, запущенной в 18:00.	`Yes` – ставить в очередь задачи проверки, запланированные по расписанию, если текущая проверка еще выполняется. `No` (значение по умолчанию) – запускать запланированные задачи проверки по расписанию, даже если текущая проверка еще не завершена.
`ActionOnThreat`	Выбор действия, которое приложение будет выполнять над зараженными объектами.	`DisinfectDeleteIfNotPossible` (лечить; удалять, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. `DisinfectInformIfNotPossible` (лечить; информировать, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение сохраняет в журнале информацию об этом. `Inform` (информировать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Включение исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.
	Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

Параметр	Описание	Значения
`UseExcludeThreats`	Включение исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats.item_#`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (значение по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.
`UseOASExclusions`	Включение использования исключений Защиты от файловых угроз при проверке.	`Yes` (значение по умолчанию) – использовать исключения Защиты от файловых угроз. `No` – не использовать исключения Защиты от файловых угроз.
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию о незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию о проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию о необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (значение по умолчанию) – включить эвристический анализатор. `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка, минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) – рекомендуемое значение.

Параметр	Описание	Значения
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.
`DeviceNameMasks.item_#`	Список имен устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску имени устройства.	`AllObjects` – проверять загрузочные секторы всех устройств. `<device name mask>` – проверять загрузочные секторы устройств, имена которых содержат указанную маску. Значение по умолчанию: `/**` – любой набор символов в имени устройства, включая символ `/`.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: `All objects`. Пример `AreaDesc="Mail bases scan"`
`UseScanArea`	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	`Yes` (значение по умолчанию) – проверять указанную область. `No` – не проверять указанную область.
`AreaMask.item_#`	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (проверять все объекты). Пример `AreaMask.item_0000=*doc`
`Path`	Путь к директории с проверяемыми объектами.	`<path to local directory>` – проверять объекты в указанной директории. `Shared:NFS` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. `Shared:SMB` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. `Mounted:NFS` – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `AllShared` – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. `<file system type>` – проверять все ресурсы указанной файловой системы устройства.
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры.		
`AreaDesc`	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из проверки.	`Yes` (значение по умолчанию) – исключать указанную область. `No` – не исключать указанную область.
`AreaMask.item_#`	Ограничение области исключения из проверки. В области исключения приложение исключает только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать все объекты).

Параметр	Описание	Значения
`Path`	Путь к директории с исключаемыми объектами.	`<path to local directory>` – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать маски. В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида `/.snapshots/*/snapshot/`. По умолчанию указан путь `/` – приложение исключает из проверки все директории локальной файловой системы. `Mounted:NFS` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `<file system type>` – исключать из проверки все ресурсы указанной файловой системы устройства. Удаленные директории исключаются из проверки приложением, только если они были смонтированы до запуска задачи. Удаленные директории, смонтированные после запуска задачи, из проверки не исключаются.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Задача Выборочная проверка

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Выборочная проверка (`Scan_File`).

Параметр	Описание	Значения
`ScanFiles`	Включение проверки файлов.	`Yes` (по умолчанию) – проверять файлы. `No` – не проверять файлы.
`ScanBootSectors`	Включение проверки загрузочных секторов.	`Yes` – проверять загрузочные секторы. `No` (по умолчанию) – не проверять загрузочные секторы.
`ScanComputerMemory`	Включение проверки памяти процессов и памяти ядра.	`Yes` – проверять память процессов и память ядра. `No` (по умолчанию) – не проверять память процессов и память ядра.
`ScanStartupObjects`	Включение проверки объектов автозапуска.	`Yes` – проверять объекты автозапуска. `No` (по умолчанию) – не проверять объекты автозапуска.
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	`Yes` (по умолчанию) – проверять архивы. Если для параметра `ActionOnThreat` указано значение `DisinfectDeleteIfNotPossible` и лечение невозможно, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` (по умолчанию) – проверять самораспаковывающиеся архивы. `No` – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других.	`Yes` – проверять файлы почтовых баз. `No` (по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронной почты в текстовом формате. `No` (по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
`QueueScanTasks`	Отложенный запуск задач проверки, запланированных по расписанию, если запущенная ранее проверка по расписанию еще выполняется. Kaspersky Endpoint Security ставит запланированные задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, запланировано запускать задачу проверки в 18:00 и в 20:00. Задача проверки, которая должна запуститься в 20:00, будет отложена, если задача проверки, запущенная в 18:00, еще выполняется. Задача запустится после завершения задачи, запущенной в 18:00.	`Yes` – ставить в очередь задачи проверки, запланированные по расписанию, если текущая проверка еще выполняется. `No` (значение по умолчанию) – запускать запланированные задачи проверки по расписанию, даже если текущая проверка еще не завершена.

Параметр	Описание	Значения
`ActionOnThreat`	Выбор действия, которое приложение будет выполнять над зараженными объектами.	`DisinfectDeleteIfNotPossible` (лечить; удалять, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. `DisinfectInformIfNotPossible` (лечить; информировать, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение сохраняет в журнале информацию об этом. `Inform` (информировать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Включение исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.	Значение по умолчанию не задано.
		Пример
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Включение исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats.item_#`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.
`UseOASExclusions`	Включение использования исключений Защиты от файловых угроз при проверке.	`Yes` (по умолчанию) – использовать исключения Защиты от файловых угроз. `No` – не использовать исключения Защиты от файловых угроз.

Параметр	Описание	Значения
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию о незараженных объектах. `No` (по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию о проверке объектов в составе архивов. `No` (по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию о необработанных объектах. `No` (по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (по умолчанию) – включить эвристический анализатор. `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка, минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (по умолчанию) – рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.
`DeviceNameMasks.item_#`	Список имен устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску имени устройства.	`AllObjects` – проверять загрузочные секторы всех устройств. `<device name mask>` – проверять загрузочные секторы устройств, имена которых содержат указанную маску. Значение по умолчанию: `/**` – любой набор символов в имени устройства, включая символ `/`.

Задача Проверка важных областей

В таблице ниже описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Проверка важных областей (`Critical_Areas_Scan`).

Параметры задачи Проверка важных областей

Параметр	Описание	Значения
`ScanFiles`	Включение проверки файлов.	`Yes` – проверять файлы. `No` (значение по умолчанию) – не проверять файлы.
`ScanBootSectors`	Включение проверки загрузочных секторов.	`Yes` (значение по умолчанию) – проверять загрузочные секторы. `No` – не проверять загрузочные секторы.

Параметр	Описание	Значения
`ScanComputerMemory`	Включение проверки памяти процессов и памяти ядра.	`Yes` (значение по умолчанию) – проверять память процессов и память ядра. `No` – не проверять память процессов и память ядра.
`ScanStartupObjects`	Включение проверки объектов автозапуска.	`Yes` (значение по умолчанию) – проверять объекты автозапуска. `No` – не проверять объекты автозапуска.
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	`Yes` (значение по умолчанию) – проверять архивы. Если для параметра `ActionOnThreat` указано значение `DisinfectDeleteIfNotPossible` и лечение невозможно, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` (значение по умолчанию) – проверять самораспаковывающиеся архивы. `No` – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронной почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
`QueueScanTasks`	Отложенный запуск задач проверки, запланированных по расписанию, если запущенная ранее проверка по расписанию еще выполняется. Kaspersky Endpoint Security ставит запланированные задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, запланировано запускать задачу проверки в 18:00 и в 20:00. Задача проверки, которая должна запуститься в 20:00, будет отложена, если задача проверки, запущенная в 18:00, еще выполняется. Задача запустится после завершения задачи, запущенной в 18:00.	`Yes` – ставить в очередь задачи проверки, запланированные по расписанию, если текущая проверка еще выполняется. `No` (значение по умолчанию) – запускать запланированные задачи проверки по расписанию, даже если текущая проверка еще не завершена.

Параметр	Описание	Значения
`ActionOnThreat`	Выбор действия, которое приложение будет выполнять над зараженными объектами.	`DisinfectDeleteIfNotPossible` (лечить; удалять, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. `DisinfectInformIfNotPossible` (лечить; информировать, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение сохраняет в журнале информацию об этом. `Inform` (информировать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Включение исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.
	Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Включение исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats.item_#`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (значение по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.
`UseOASExclusions`	Включение использования исключений Защиты от файловых угроз при проверке.	`Yes` (значение по умолчанию) – использовать исключения Защиты от файловых угроз. `No` – не использовать исключения Защиты от файловых угроз.

Параметр	Описание	Значения
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию о незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию о проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию о необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (значение по умолчанию) – включить эвристический анализатор. `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка, минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) – рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.
`DeviceNameMasks.item_#`	Список имен устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску имени устройства.	`AllObjects` – проверять загрузочные секторы всех устройств. `<device name mask>` – проверять загрузочные секторы устройств, имена которых содержат указанную маску. Значение по умолчанию: `/**` – любой набор символов в имени устройства, включая символ `/`.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области проверки, содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: `All objects`. Пример `AreaDesc="Mail bases scan"`
`UseScanArea`	Включение проверки указанной области. Для выполнения задачи требуется включить проверку хотя бы одной области.	`Yes` (значение по умолчанию) – проверять указанную область. `No` – не проверять указанную область.
`AreaMask.item_#`	Ограничение области проверки. В области проверки приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (проверять все объекты). Пример `AreaMask.item_0000=*doc`

Параметр	Описание	Значения
`Path`	Путь к директории с проверяемыми объектами.	`<path to local directory>` – проверять объекты в указанной директории. `Shared:NFS` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. `Shared:SMB` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. `Mounted:NFS` – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `AllShared` – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. `<file system type>` – проверять все ресурсы указанной файловой системы устройства.
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из проверки.	`Yes` (значение по умолчанию) – исключать указанную область. `No` – не исключать указанную область.
`AreaMask.item_#`	Ограничение области исключения из проверки. В области исключения приложение исключает только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать все объекты).

Параметр	Описание	Значения
`Path`	Путь к директории с исключаемыми объектами.	`<path to local directory>` – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать маски. В системах с файловой системой btrfs и включенными активными снимками для оптимизации работы задач проверки рекомендуется добавить в исключения путь со снимками, смонтированными системой в режиме "только чтение". Например, в системах на базе SUSE/OpenSUSE вы можете добавить исключение вида `/.snapshots/*/snapshot/`. По умолчанию указан путь `/` – приложение исключает из проверки все директории локальной файловой системы. `Mounted:NFS` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `<file system type>` – исключать из проверки все ресурсы указанной файловой системы устройства. Удаленные директории исключаются из проверки приложением, только если они были смонтированы до запуска задачи. Удаленные директории, смонтированные после запуска задачи, из проверки не исключаются.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Задача Проверка съемных дисков

В командной строке вы можете управлять проверкой съемных дисков с помощью предустановленной задачи Проверка съемных дисков (`Removable_Drives_Scan`).

По умолчанию задача *Проверка съемных дисков* не запущена. Вы можете запускать и останавливать эту задачу вручную. Вы можете настраивать параметры проверки, изменяя параметры этой задачи.

Если задача запущена, приложение контролирует подключение съемных дисков к устройству и при подключении съемного диска создает и запускает временную задачу проверки загрузочных секторов (задачу типа `ODS`). Эту задачу остановить невозможно. После завершения выполнения задачи приложение автоматически ее удаляет.

Если в параметрах задачи *Проверка съемных дисков* вы включили проверку файлов, приложение также запускает одну или несколько временных задач выборочной проверки файлов (задачи типа `ODS`). Если требуется, пользователь с правами администратора может останавливать выполнение таких задач.

При изменении параметров задачи *Проверка съемных дисков* новые значения не применяются к уже запущенным временным задачам. При остановке задачи *Проверка съемных дисков* уже запущенные временные задачи не останавливаются.

Параметры задачи Проверка съемных дисков

Параметр	Описание	Значения
`ScanRemovableDrives`	Включение проверки съемных дисков при подключении к устройству. Этот параметр не применяется к CD/DVD-приводам и дискам Blu-ray (см. параметр `ScanOpticalDrives`).	`DetailedScan` – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и дисков Blu-ray). Детализированная проверка выполняется с параметрами, которые заданы по умолчанию для задачи `Scan_File` (ID:3). `QuickScan` – проверять на съемных дисках (за исключением CD/DVD-приводов и дисков Blu-ray) только файлы **определенных типов**. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи `Critical_Areas_Scan` (ID:4). `NoScan` (значение по умолчанию) – не проверять съемные диски при подключении.
`ScanOpticalDrives`	Включение проверки CD/DVD-приводов и дисков Blu-ray при подключении к устройству.	`DetailedScan` – проверять все файлы на CD/DVD-приводах и дисках Blu-ray. Детализированная проверка выполняется с параметрами, которые заданы по умолчанию для задачи `Scan_File` (ID:3). `QuickScan` – проверять на CD/DVD-приводах и дисках Blu-ray только файлы **определенных типов**. На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи `Critical_Areas_Scan` (ID:4). `NoScan` (значение по умолчанию) – не проверять CD/DVD-приводы и диски Blu-ray при подключении.
`BlockDuringScan`	Включение блокировки файлов на подключенном диске при проверке. При проверке загрузочных секторов файлы не блокируются.	`Yes` – блокировать файлы при проверке. `No` (значение по умолчанию) – не блокировать файлы при проверке.

Проверка контейнеров

В командной строке вы можете выполнять проверку контейнеров и образов следующими способами:

- С помощью предустановленной задачи Проверка контейнеров (`Container_Scan`). Вы можете запускать и останавливать эту задачу вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры проверки, изменяя параметры этой задачи.

- С помощью пользовательских задач проверки контейнеров (задач типа `ContainerScan`). Вы можете запускать и останавливать пользовательские задачи вручную и настраивать расписание запуска задач.

- С помощью следующей команды вы можете выполнять *выборочную проверку* указанных контейнеров и образов:

```
kesl-control --scan-container
```

Параметры проверки контейнеров

В таблице ниже описаны параметры проверки контейнеров, которые используются при проверке пространств имен и контейнеров в реальном времени.

Общие параметры проверки контейнеров и пространств имен

Параметр	Описание	Значения
`OnAccessContainerScanAction`	Действие над контейнером при обнаружении зараженного объекта. Этот параметр доступен при использовании приложения по лицензии, которая включает эту функцию. При проверке объектов внутри контейнера используются параметры задачи Защита от файловых угроз.	`StopContainerIfFailed` (значение по умолчанию) – остановить контейнер, если не удалось вылечить или удалить зараженный объект. Если выбрано это значение, выполнямое над контейнером действие также зависит от заданного значения параметра `ActionOnThreat` задачи Защита от файловых угроз. Если для параметра `ActionOnThreat` задано значение `DisinfectDeleteIfNotPossible` и при выполнении действия приложению не удалось вылечить или удалить зараженный объект, контейнер будет остановлен. `StopContainer` – остановить контейнер при обнаружении зараженного объекта. `Skip` – не выполнять никаких действий над контейнерами при обнаружении зараженного объекта.
`UseDocker`	Использование системы управления контейнерами Docker.	`Yes` (значение по умолчанию) – использовать систему управления контейнерами Docker. `No` – не использовать систему управления контейнерами Docker.
`DockerSocket`	Путь или URI (универсальный идентификатор ресурса) Docker-сокета.	Значение по умолчанию: /var/run/docker.sock.
`UseCrio`	Использование среды CRI-O.	`Yes` (значение по умолчанию) – использовать среду CRI-O. `No` – не использовать среду CRI-O.
`CrioConfigFilePath`	Путь к конфигурационному файлу CRI-O.	Значение по умолчанию: /etc/crio/crio.conf.

Параметр	Описание	Значения
`UsePodman`	Использование утилиты Podman.	`Yes` (значение по умолчанию) – использовать утилиту Podman. `No` – не использовать утилиту Podman.
`PodmanBinaryPath`	Путь к исполняемому файлу утилиты Podman.	Значение по умолчанию: /usr/bin/podman.
`PodmanRootFolder`	Путь к корневой директории хранилища контейнеров.	Значение по умолчанию: /var/lib/containers/storage.
`UseRunc`	Использование утилиты runc.	`Yes` (значение по умолчанию) – использовать утилиту runc. `No` – не использовать утилиту runc.
`RuncBinaryPath`	Путь к исполняемому файлу утилиты runc.	Значение по умолчанию: /usr/bin/runc.
`RuncRootFolder`	Путь к корневой директории хранилища состояний контейнеров.	Значение по умолчанию: /run/runc.

Задача Проверка контейнеров

В таблице описаны все доступные значения и значения по умолчанию для всех параметров задачи Проверка контейнеров (`Container_Scan`).

Параметры задачи Проверка контейнеров

Параметр	Описание	Значения
`ScanContainers`	Проверка контейнеров, заданных по маске. Вы можете указать маски с помощью параметра `ContainerNameMask`.	`Yes` (значение по умолчанию) – проверять контейнеры, заданные по маске. `No` – не проверять контейнеры, заданные по маске.

`ContainerNameMask`	Имя или маска имени проверяемого контейнера.
	Маски указываются в формате командной оболочки. Вы можете использовать символы ? и *.
	Прежде чем указать этот параметр, убедитесь, что значение параметра `ScanContainers=Yes`.
		Значение по умолчанию: * (выполнять проверку всех контейнеров).
		`Пример проверки контейнера с именем my_container`
		`ContainerNameMask=my_container`
		`Пример проверки всех контейнеров, имена которых начинаются с my_container`
		`ContainerNameMask=my_container*`
		`Пример проверки всех контейнеров, имена которых начинаются с my_, затем содержат пять любых символов, затем слово _container и заканчиваются любой последовательностью символов`
		`ContainerNameMask=my_?????_container*`

`ScanImages`	Проверка образов, заданных по маске. Вы можете указать маски с помощью параметра `ImageNameMask`.	`Yes` (значение по умолчанию) – проверять образы, заданные по маске. `No` – не проверять образы, заданные по маске.

`ImageNameMask`	Имя или маска имени проверяемых образов.
	Прежде чем указать этот параметр, убедитесь, что для параметра `ScanImages` выбрано значение `Yes`.
	Маски указываются в формате командной оболочки.
	Если вы хотите указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом.
		Значение по умолчанию: * (выполнять проверку всех образов).
		`Пример проверки образов с именем my_image и значением тега latest`
		`ImageNameMask=my_image:latest`
		`Пример проверки всех образов, имена которых начинаются с my_image_, имеющих любое значение тега`
		`ImageNameMask=my_image*`

`DeepScan`	Проверка всех слоев образов и запущенных контейнеров.	`Yes` – проверять все слои. `No` (значение по умолчанию) – не проверять все слои.

Параметр	Описание	Значения
`ContainerScanAction`	Действие над контейнером при обнаружении зараженного объекта. Действия над зараженным объектом внутри контейнера описаны ниже.	`StopContainerIfFailed` (значение по умолчанию) – приложение останавливает контейнер, если не удалось вылечить или удалить зараженный объект. Если выбрано это значение, выполняемое над контейнером действие также зависит от заданного значения параметра `ActionOnThreat`, которое применяется к объектам внутри контейнеров и образов (см. таблицу ниже). Если для параметра `ActionOnThreat` задано значение `DisinfectDeleteIfNotPossible` и при выполнении действия приложению не удалось вылечить или удалить зараженный объект, контейнер будет остановлен. Из-за особенностей работы среды CRI-O зараженный объект не лечится и не удаляется в контейнере в среде CRI-O. Рекомендуется выбирать действие `StopContainer`. `StopContainer` – приложение останавливает контейнер при обнаружении зараженного объекта. `Skip` – приложение не выполняет никаких действий над контейнерами при обнаружении зараженного объекта.
`ImageAction`	Действие над образом при обнаружении зараженного объекта. Действия над зараженным объектом внутри образа описаны ниже.	`Skip` (значение по умолчанию) – приложение не выполняет никаких действий над образами при обнаружении зараженного объекта. `Delete` – приложение удаляет образ при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.

Ниже описаны параметры, которые применяются к объектам внутри контейнеров и образов.

Параметры задачи Проверка контейнеров

Параметр	Описание	Значения
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	`Yes` (значение по умолчанию) – проверять архивы. Если для параметра `ActionOnThreat` указано значение `DisinfectDeleteIfNotPossible` и лечение невозможно, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` (значение по умолчанию) – проверять самораспаковывающиеся архивы. `No` – не проверять самораспаковывающиеся архивы.
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронной почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.

Параметр	Описание	Значения
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
`ActionOnThreat`	Выбор действия, которое приложение будет выполнять над зараженными объектами.	`DisinfectDeleteIfNotPossible` (лечить; удалять, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. `DisinfectInformIfNotPossible` (лечить; информировать, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение сохраняет в журнале информацию об этом. `Inform` (информировать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Использование исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.	Значение по умолчанию не задано.
		Пример
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Использование исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats.item_#`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (значение по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.

Параметр	Описание	Значения
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию о незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию о проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию о необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (значение по умолчанию) – включить эвристический анализатор; `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка, минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) – рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.
`QueueScanTasks`	Отложенный запуск задач проверки, запланированных по расписанию, если запущенная ранее проверка по расписанию еще выполняется. Kaspersky Endpoint Security ставит запланированные задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, запланировано запускать задачу проверки в 18:00 и в 20:00. Задача проверки, которая должна запуститься в 20:00, будет отложена, если задача проверки, запущенная в 18:00, еще выполняется. Задача запустится после завершения задачи, запущенной в 18:00.	`Yes` – ставить в очередь задачи проверки, запланированные по расписанию, если текущая проверка еще выполняется. `No` (значение по умолчанию) – запускать запланированные задачи проверки по расписанию, даже если текущая проверка еще не завершена.

Интеграция с Jenkins

Kaspersky Endpoint Security поддерживает интеграцию с Jenkins. Плагины Jenkins Pipeline можно использовать для проверки Docker-образов на разных этапах. Например, можно проверять Docker-образы в репозитории в процессе разработки или перед публикацией.

Чтобы интегрировать Kaspersky Endpoint Security с Jenkins:

1. Установите Kaspersky Endpoint Security на узле Jenkins.
2. Установите Docker Engine на узле Jenkins.

   Дополнительная информация приведена в документации Docker Engine.

3. Предоставьте пользователю Jenkins права администратора приложения Kaspersky Endpoint Security:

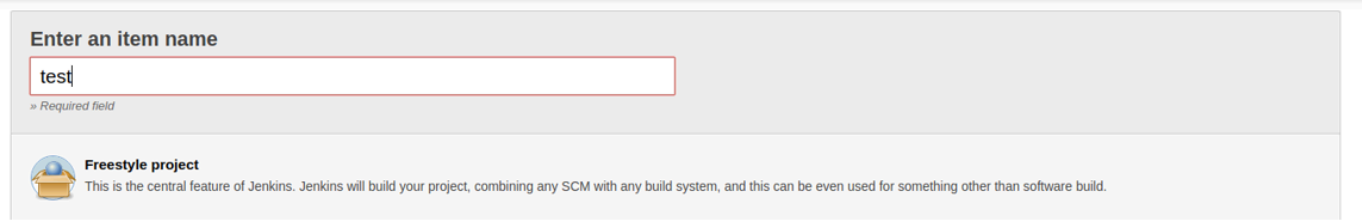
```
kesl-control --grant-role admin <Jenkins user name>
```

4. Добавьте пользователя Jenkins в группу docker:

```
sudo usermod -aG docker <Jenkins user name>
```

Обычно используется имя jenkins.

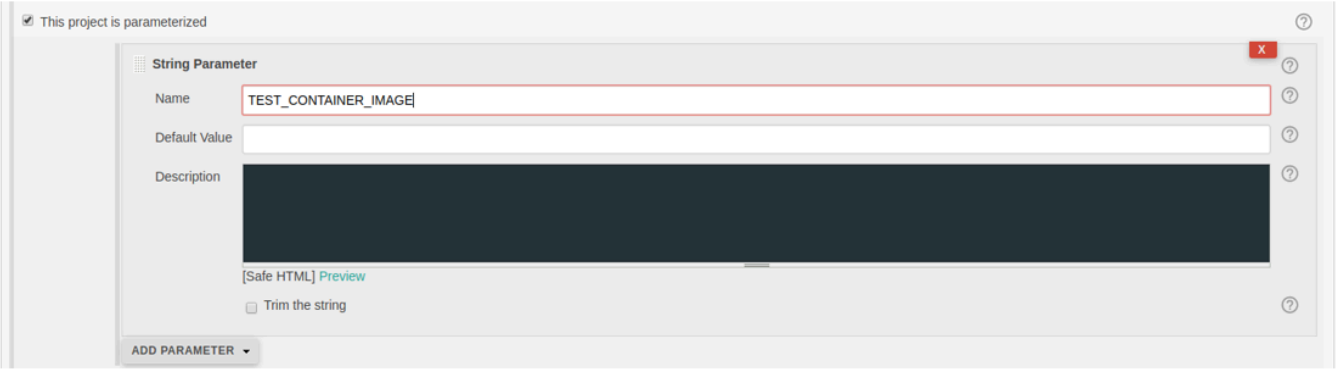
5. В Jenkins создайте новое задание на сборку с названием `test` (**New Item** → **Enter an item name**).



6. Настройте проект в соответствии с вашими требованиями. Предполагается, что в результате настройки вы получите образ или запущенный контейнер, который нужно проверить.

7. Чтобы запустить Docker-контейнер, добавьте следующий скрипт в процедуру сборки Jenkins. Если вы используете плагины Jenkins или другой способ запуска Docker-контейнеров, сохраните идентификатор запущенного Docker-контейнера в файл /tmp/kesl_cs_info для дальнейшей проверки:

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
CONTAINER_ID=$(docker run -d -v /storage:/storage ${TEST_CONTAINER_IMAGE} /storage/docker_process.sh)
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
exit 1
fi
echo "${CONTAINER_ID}" > ${TMP_FILE}
exit ${EXIT_CODE}
```



8. После создания артефактов добавьте следующий сценарий к шагам создания jenkins.

   Этот скрипт поддерживает проверку одного контейнера. Если требуется, измените скрипт в соответствии с вашими требованиями.

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep 'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
echo "ATTENTION! ${THREATS_AMOUNT} threats detected at: '${CONTAINER_ID}'"
EXIT_CODE=1
else
echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

9. Чтобы выполнить проверку Docker-образа из репозитория, выполните следующий скрипт:

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
echo "Dockerfile not fetched"
exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container ${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. Сохраните задание на сборку.

Задача Защита от шифрования

В командной строке вы можете управлять защитой от шифрования с помощью задачи Защита от шифрования (`Anti_Cryptor`).

По умолчанию задача Защита от шифрования не запущена. Вы можете запускать и останавливать эту задачу вручную.

Вы можете настраивать параметры защиты от шифрования, изменяя параметры предустановленной задачи Защита от шифрования.

Параметр	Описание	Значения
`ActionOnDetect`	Включение блокировки недоверенных устройств.	`Block` (значение по умолчанию) – включить блокировку недоверенных устройств. `Notify` – выключить блокировку недоверенных устройств.
`BlockTime`	Длительность блокировки недоверенного устройства в минутах. Изменение параметра `BlockTime` не влияет на длительность блокировки ранее заблокированных скомпрометированных устройств. Длительность блокировки не является динамическим значением и рассчитывается на момент блокировки.	Целое значение от 1 до 4294967295. Значение по умолчанию: 30.
`UseExcludeMasks`	Включение исключения из области защиты объектов, указанных параметром `ExcludeMasks.item_#`. Этот параметр работает, только если указано значение параметра `ExcludeMasks.item_#`.	`Yes` – исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области защиты. `No` (значение по умолчанию) – не исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области защиты.
`ExcludeMasks.item_#`	Исключение из области защиты объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области защиты отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`. Если вы хотите указать несколько масок, указывайте каждую маску в новой строке с новым индексом.	Значение по умолчанию не задано.
Секция **[ScanScope.item_#]** содержит области, защищаемые приложением. Для задачи Защита от шифрования требуется указать хотя бы одну область защиты, можно указывать только общие директории. Вы можете указать несколько секций [ScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области защиты, содержит дополнительную информацию об области защиты.	Значение по умолчанию: `All shared directories`.
`UseScanArea`	Включение защиты указанной области. Для выполнения задачи требуется включить защиту хотя бы одной области.	`Yes` (значение по умолчанию) – защищать указанную область. `No` – не защищать указанную область.
`AreaMask.item_#`	Ограничение области защиты. В области защиты приложение защищает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (защищать все объекты).
`Path`	Путь к директории с защищаемыми объектам.	`< путь к локальной директории >` – защищать локальную директорию, доступную через SMB/NFS. Для указания пути вы можете использовать маски. `AllShared` (значение по умолчанию) – защищать все ресурсы, доступные через SMB/NFS. `Shared:SMB` – защищать ресурсы, доступные через SMB. `Shared:NFS` – защищать ресурсы, доступные через NFS.
Секция **[ExcludedFromScanScope.item_#]** содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#]. Объекты, удовлетворяющие правилам любой из секций [ExcludedFromScanScope.item_#], не проверяются. Формат секции [ExcludedFromScanScope.item_#] аналогичен формату секции [ScanScope.item_#]. Вы можете указать несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области исключения из защиты, содержит дополнительную информацию об области исключения.	Значение по умолчанию: `All objects`.

Параметр	Описание	Значения
`UseScanArea`	Исключение указанной области из защиты.	`Yes` (значение по умолчанию) – исключать указанную область из защиты. `No` – не исключать указанную область из защиты.
`AreaMask.item_#`	Ограничение области исключения из защиты. В области исключения приложение исключает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (исключать все объекты).
`Path`	Путь к директории с объектами, исключаемыми из защиты.	`< путь к локальной директории >` – исключать из защиты объекты в указанной директории. Для указания пути вы можете использовать маски. `Mounted:NFS` – исключать из защиты удаленные директории, смонтированные на клиентском устройстве по протоколу NFS. `Mounted:SMB` – исключать из защиты удаленные директории, смонтированные на клиентском устройстве по протоколу Samba. `AllRemoteMounted` – исключать из защиты все удаленные директории, смонтированные на клиентском устройстве с помощью протоколов Samba и NFS.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Задача Анализ поведения

В командной строке вы можете управлять анализом поведения приложений в операционной системе с помощью предустановленной задачи Анализ поведения (`Behavior_Detection`).

Задача Анализ поведения по умолчанию запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры анализа поведения, изменяя параметры предустановленной задачи Анализ поведения.

Параметр	Описание	Значения
`UseTrustedPrograms`	Исключение процессов из проверки.	`Yes` – исключать из проверки активность указанных процессов. `No` (значение по умолчанию) – проверять все процессы.
`TaskMode`	Действие, выполняемое приложением при обнаружении вредоносной активности в операционной системе.	`Block` (значение по умолчанию) – завершать процесс приложения, осуществляющего вредоносную активность. `Notify` – не завершать процесс, осуществляющий вредоносную активность, только регистрировать обнаружение вредоносной активности в журнале событий.
TelemetrySource	Дополнительные параметры сбора телеметрии, отправляемой решениям Detection and Response при интеграции с ними. Параметр `UseTelemetryMonopolyMode` применяется, только если для параметра `TelemetrySource` установлено значение `Default`.	`Default` (значение по умолчанию) – использовать для сбора телеметрии технологию eBPF и службу auditd. `OnlyEBPF` – использовать для сбора телеметрии только технологию eBPF.
UseTelemetryMonopolyMode	Параметр неприменим для устройств с процессором Эльбрус.	`True` (значение по умолчанию) – приложение Kaspersky Endpoint Security использует службу auditd в монопольном режиме. `False` – служба auditd используется в режиме многоадресной рассылки.
Секция **[TrustedPrograms.item_#]** содержит процессы, которые исключаются из проверки компонентом Анализ поведения. Приложение Kaspersky Endpoint Security не контролирует активность указанных процессов.		
`ProgramPath`	Путь к исключаемому процессу.	`< полный путь к процессу >` – исключать из проверки процесс в указанной локальной директории. Для указания пути вы можете использовать маски.
`ApplyToDescendants`	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром `ProgramPath`.	`Yes` – исключать из проверки указанный процесс и все его дочерние процессы. `No` (значение по умолчанию) – исключать из проверки только указанный процесс, не исключать из проверки дочерние процессы.
`ProgramDesc`	Описание исключаемого процесса.	
`UseTrustedProgram`	Использование исключения активности указанного процесса из проверки.	`Yes` (значение по умолчанию) – использовать исключение из проверки активности указанного процесса. `No` – не использовать исключение активности указанного процесса из проверки.

Параметр	Описание	Значения
`UseTrustedProgramForDetects`	Исключение активности процесса из проверки при работе компонента Анализ поведения.	`Yes` – исключать активность указанного процесса из проверки при работе компонента Анализ поведения. `No` (значение по умолчанию) – не исключать активность указанного процесса из проверки при работе компонента Анализ поведения.
`UseTrustedProgramForMDRAndEDR`	Исключение активности процесса из телеметрии, которую собирают компоненты MDR и EDR Expert (on-premises). Параметр неприменим для устройств с процессором Эльбрус.	`Yes` – исключать активность указанного процесса из телеметрии, которую собирают компоненты MDR и EDR Expert (on-premises). `No` (значение по умолчанию) – не исключать активность указанного процесса из телеметрии.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Защита от эксплойтов

В командной строке вы можете управлять защитой от эксплойтов с помощью параметров предустановленной задачи Анализ поведения (`Behavior_Detection`).

Вы можете настраивать параметры защиты от эсклойтов, изменяя параметры предустановленной задачи Анализ поведения (см. таблицу ниже).

Параметры Защиты от эксплойтов

Параметр	Описание	Значения
`UseAEP`	Включение компонента Защита от эксплойтов.	`Yes` – включить Защиту от эксплойтов. `No` (значение по умолчанию) – выключить Защиту от эксплойтов.
`AEPMode`	Действие, выполняемое приложением при обнаружении эксплойта.	`Block` (значение по умолчанию) – блокировать вредоносные действия эксплойта и записывать в журнал событий информацию об этом. `Notify` – не блокировать действия эксплойта, а только записывать в журнал событий информацию об обнаружении эксплойта.

Параметр	Описание	Значения
Секция **[AEPExclusions.item_#]** содержит исключения из проверки компонентом Защита от эксплойтов.		
`Enabled`	Включение использования исключения из проверки в работе компонента Защита от эксплойтов.	`Yes` (значение по умолчанию) – использовать исключение из проверки Защитой от эксплойтов. `No` – не использовать исключение из проверки Защитой от эксплойтов.
`DetectName`	Исключение из проверки объекта по названию обнаруженной в объекте угрозы. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseDetectName`.	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным. Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
`Hash`	Исключение из проверки файла, в котором обнаружена угроза, по его хеш-сумме. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseHash`.	
`HashType`	Тип хеш-суммы файла, по которой вы хотите исключить файл из проверки с помощью параметра `Hash`.	`Md5` – тип хеш-суммы MD5. `Sha256` – тип хеш-суммы SHA256.
`Path`	Исключение из проверки файла, в котором обнаружена угроза, по пути к нему. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UsePath`.	`< полный путь к файлу или локальной директории >` – исключать из проверки файл или объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать символы `*` и `?`.
`UseDetectName`	Включение исключения из проверки объектов с угрозами, указанными параметром `DetectName`.	`Yes` (значение по умолчанию) – исключать из проверки объекты, которые содержат угрозы, указанные параметром `DetectName`. `No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `DetectName`.
`UseHash`	Включение исключения из проверки файл, в котором обнаружена угроза, по его хеш-сумме. Хеш-сумма файла указывается с помощью параметра `Hash`.	`Yes` (значение по умолчанию) – исключать из проверки файл, в котором обнаружена угроза, по его хеш-сумме. `No` – не исключать из проверки файл, в котором обнаружена угроза, по его хеш-сумме.
`UsePath`	Включение исключения из проверки файла, в котором обнаружена угроза, по пути к нему. Путь к файлу указывается с помощью параметра `Path`.	`Yes` (значение по умолчанию) – исключать из проверки файл, в котором обнаружена угроза, по пути к нему. `No` – не исключать из проверки файл, в котором обнаружена угроза, по пути к нему.

Использование Kaspersky Security Network

В командной строке вы можете включать и выключать использование Kaspersky Security Network с помощью параметра `UseKSN` из общих параметров приложения.

Вы можете изменять значение параметра `UseKSN` с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Чтобы включить использование Kaspersky Security Network с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-app-settings UseKSN=<Extended/Basic> --accept-ksn
```

где:

`<Extended/Basic>` – режим использования Kaspersky Security Network.

`--accept-ksn` – ключ, означающий, что вы соглашаетесь с условиями, изложенными в Положении о Kaspersky Security Network. Вы подтверждаете, что полностью прочитали, понимаете и принимаете условия Положения о Kaspersky Security Network.

Файл ksn_license.<ID языка> с текстом Положения о Kaspersky Security Network находится в директории /opt/kaspersky/kesl/doc/.

Чтобы выключить использование Kaspersky Security Network с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-app-settings UseKSN=No
```

Чтобы включить или выключить использование Kaspersky Security Network с помощью конфигурационного файла, выполните следующую команду:

```
kesl-control --set-app-settings --file <path to the configuration file> [--json] [--accept-ksn]
```

где:

`--file <path to the configuration file>` – полный путь к конфигурационному файлу с общими параметрами приложения, в котором настроено нужное значение параметра `UseKSN`.

`--json` – укажите этот ключ, если вы импортируете параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

`--accept-ksn` – ключ, означающий, что вы соглашаетесь с условиями, изложенными в Положении о Kaspersky Security Network. Ключ требуется указать, если вы включаете использование Kaspersky Security Network.

Если приложение Kaspersky Endpoint Security, установленное на клиентском устройстве, работает под управлением политики Kaspersky Security Center, значение параметра `UseKSN` можно изменить только в Kaspersky Security Center. Когда приложение Kaspersky Endpoint Security, установленное на клиентском устройстве, прекращает работать под управлением политики, параметру присваивается значение `UseKSN=No`.

Подключение к Kaspersky Security Network

Чтобы проверить подключение к Kaspersky Security Network, выполните следующую команду:

```
kesl-control --app-info
```

В строке **Использование Kaspersky Security Network** отображается статус подключения к Kaspersky Security Network:

- Если отображается статус *Расширенный режим KSN*, приложение Kaspersky Endpoint Security использует Kaspersky Security Network, можно получать информацию из базы знаний, отправляется анонимная статистика и информация о типах и источниках угроз.

- Если отображается статус *Стандартный режим KSN*, приложение Kaspersky Endpoint Security использует Kaspersky Security Network, можно получать информацию из базы знаний, но анонимная статистика и информация о типах и источниках угроз не отправляется.

- Если отображается статус *KSN не используется*, приложение Kaspersky Endpoint Security не использует Kaspersky Security Network.

В строке **Инфраструктура Kaspersky Security Network** отображается информация об инфраструктурном решении, которое используется для работы с репутационными базами "Лаборатории Касперского": *KSN* или *KPSN*.

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Устройство пользователя не подключено к интернету.

- Использование Kaspersky Security Network не включено.

- Приложение не активировано, или срок действия лицензии истек.

- Выявлены проблемы, связанные с лицензионным ключом. Например, ключ находится в списке запрещенных ключей.

Включение и выключение облачного режима

Облачный режим – это режим работы приложения Kaspersky Endpoint Security, при котором используется облегченная версия баз вредоносного ПО.

> Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, работа с облегченными базами вредоносного ПО не поддерживается. Приложение получает от Сервера защиты специальные базы, необходимые для работы Легкого агента.

В командной строке вы можете включать и выключать облачный режим с помощью параметра `CloudMode=Yes/No` из общих параметров приложения.

Вы можете изменять значение параметра `CloudMode` с помощью конфигурационного файла, который содержит все общие параметры приложения, или с помощью ключей командной строки.

> Облачный режим работы приложения доступен, если включено использование Kaspersky Security Network.

Задача Защита от атак BadUSB

В командной строке вы можете управлять защитой от атак BadUSB с помощью предустановленной задачи Защита от атак BadUSB (`Bad_USB`).

Задача Защита от атак BadUSB не запущена по умолчанию. Вы можете запускать и останавливать эту задачу вручную.

> Для запуска и остановки задачи Защита от атак BadUSB из командной строки требуются права роли Администратор.

Вы можете настраивать параметры защиты от атак BadUSB, изменяя параметры предустановленной задачи Защита от атак BadUSB.

В таблице ниже описаны доступные значения и значения по умолчанию для параметров, которые вы можете указать для задачи Защита от атак BadUSB.

Параметры задачи Защита от атак BadUSB

Параметр	Описание	Значения
`MaxAuthAttempts`	Максимальное количество попыток авторизации USB-устройства, после исчерпания которых приложение блокирует USB-устройство и дальнейшие попытки авторизации USB-устройства на время, указанное с помощью параметра `TimeoutAfterAttempts`.	Возможные значения: 1–10. Значение по умолчанию: 5.
`TimeoutAfterAttempts`	Время блокировки USB-устройства после заданного с помощью параметра `MaxAuthAttempts` количества неудачных попыток ввода кода авторизации.	Возможные значения: 1–180 (мин). Значение по умолчанию: 5 минут.
`ProhibitOnScreenKeyboard`	Включение или выключение запрета на использование экранной клавиатуры для авторизации USB-устройств.	`Yes` – приложение запрещает использование экранной клавиатуры для авторизации USB-устройств, с которых невозможно ввести код авторизации. `No` (по умолчанию) – приложение разрешает использование экранной клавиатуры для авторизации USB-устройств, с которых невозможно ввести код авторизации.
`ProhibitBarcodeScanner`	Включение или выключение вывода кода авторизации в виде штрихкода для авторизации USB-устройств, с которых невозможно ввести код авторизации.	`Yes` (по умолчанию) – приложение запрещает вывод кода авторизации в виде штрихкода. `No` – приложение разрешает вывод кода авторизации в виде штрихкода.

Защита сетевых соединений и средств коммуникации

Задача Защита от веб-угроз

В командной строке вы можете управлять защитой от веб-угроз с помощью предустановленной задачи Защита от веб-угроз (`Web_Threat_Protection`).

Задача запускается автоматически, если в системе обнаружен один из поддерживаемых браузеров и на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в свойствах политики не установлен). Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры защиты от веб-угроз, изменяя параметры предустановленной задачи Защита от веб-угроз.

Параметры задачи Защита от веб-угроз

Параметр	Описание	Значения
`ActionOnDetect`	Действия, выполняемые при обнаружении зараженного объекта в веб-трафике.	`Notify` – разрешить загрузку обнаруженного объекта, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте. `Block` (значение по умолчанию) – запретить доступ к обнаруженному объекту, показать уведомление о заблокированной попытке доступа, записать в журнал информацию о зараженном объекте.
`CheckMalicious`	Проверка ссылок по базе вредоносных веб-адресов.	`Yes` (значение по умолчанию) – проверять ссылки на вхождение в базу вредоносных веб-адресов. `No` – не проверять ссылки на вхождение в базу вредоносных веб-адресов.
`CheckPhishing`	Проверка ссылок по базе фишинговых веб-адресов.	`Yes` (значение по умолчанию) – проверять ссылки на вхождение в базу фишинговых веб-адресов. `No` – не проверять ссылки на вхождение в базу фишинговых веб-адресов.
`UseHeuristicForPhishing`	Использование эвристического анализа для проверки веб-страниц на наличие фишинговых ссылок. Параметр неприменим для устройств с процессором Эльбрус.	`Yes` (значение по умолчанию) – использовать эвристический анализ для обнаружения фишинговых ссылок. Если выбрано это значение, используется поверхностный уровень эвристического анализа – `Light` (наименее тщательная проверка, минимальная загрузка системы). Для задачи Защита от веб-угроз невозможно изменить уровень эвристического анализа. `No` – не использовать эвристический анализ для обнаружения фишинговых ссылок.
`CheckAdware`	Проверка ссылок по базе рекламных веб-адресов.	`Yes` – проверять ссылки на вхождение в базу рекламных веб-адресов. `No` (значение по умолчанию) – не проверять ссылки на вхождение в базу рекламных веб-адресов.
`CheckOther`	Проверка ссылок по базе веб-адресов, содержащих легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.	`Yes` – проверять ссылки на вхождение в базу веб-адресов, содержащих легальные приложения, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным. `No` (значение по умолчанию) – не проверять ссылки на вхождение в базу веб-адресов, содержащих легальные приложения, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным.
`UseTrustedAddresses`	Использование списка доверенных веб-адресов. Приложение не проверяет доверенные веб-адреса на вирусы и другие вредоносные объекты. Вы можете указать доверенные веб-адреса с помощью параметра `TrustedAddresses.item_#`.	`Yes` (значение по умолчанию) – использовать список доверенных веб-адресов. `No` – не использовать список доверенных веб-адресов.
`TrustedAddresses.item_#`	Доверенные веб-адреса.	Значение по умолчанию не задано. Для указания веб-адресов вы можете использовать маски. Использование масок для указания IP-адресов не поддерживается.

Полезные статьи

Как задавать маски

При создании маски адреса вы можете использовать символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html).

Проверка сетевого трафика

В командной строке для управления параметрами проверки сетевого трафика предусмотрены специальные команды управления. С помощью команд управления параметрами проверки сетевого трафика вы можете:

- Настраивать параметры проверки сетевого трафика.
- Просматривать исключения из проверки зашифрованных соединений.
- Очищать список доменов, которые приложение автоматически исключило из проверки.
- Настраивать список доверенных корневых сертификатов, который приложение использует при проверке зашифрованных соединений.
- Настраивать и просматривать исключения из перехвата трафика.

Просмотр и изменение параметров проверки сетевого трафика

С помощью специальных команд управления параметрами проверки сетевого трафика вы можете:

- Выводить текущие значения параметров проверки сетевого трафика в консоль или в конфигурационный файл. Этот файл вы можете использовать для изменения параметров.
- Изменять все параметры проверки сетевого трафика, используя конфигурационный файл. Вы можете получить конфигурационный файл с помощью команды вывода параметров проверки сетевого трафика.
- Изменять отдельные параметры, используя ключи командной строки в формате `< имя параметра >= < значение параметра >`. Текущие значения параметров вы можете получить с помощью команды вывода параметров проверки сетевого трафика.

Чтобы вывести в консоль текущие значения параметров проверки сетевого трафика, выполните следующую команду:

```
kesl-control --get-net-settings [--json]
```

где `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Чтобы вывести в файл текущие значения параметров проверки сетевого трафика, выполните следующую команду:

```
kesl-control --get-net-settings --file <path to configuration file> [--json]
```

где:

- `--file <path to the configuration file>` – путь к файлу, в который будут сохранены параметры проверки сетевого трафика. Если вы укажете имя файла, не указав путь к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, файл не будет создан.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Чтобы изменить значения параметров проверки сетевого трафика с помощью конфигурационного файла:

1. Выведите параметры проверки сетевого трафика в конфигурационный файл, как описано выше.
2. Измените значения нужных параметров в файле и сохраните изменения.
3. Выполните команду:

   ```
   kesl-control --set-net-settings --file <path to the configuration file> [--json]
   ```

   где:

   - `--file <path to the configuration file>` – полный путь к конфигурационному файлу с параметрами проверки сетевого трафика.
   - `--json` – импортировать в приложение параметры из конфигурационного файла формата JSON. Если вы не укажете ключ `--json`, приложение попытается выполнить импорт из файла формата INI. При невозможности импорта отображается ошибка.

   Все значения параметров проверки сетевого трафика, заданные в файле, будут импортированы в приложение.

Чтобы изменить значения параметров проверки сетевого трафика с помощью командной строки, выполните следующую команду:

```
kesl-control --set-net-settings <parameter name>=<parameter value> [<parameter name>=<parameter value>]
```

где `<parameter name>=<parameter value>` – имя и значение одного из параметров проверки сетевого трафика.

Значения указанных параметров будут изменены.

Просмотр исключений из проверки зашифрованных соединений

Вы можете просматривать следующие списки исключений из проверки зашифрованных соединений:

- список исключений, добавленных пользователем;
- список исключений, добавленных приложением;
- список исключений, полученных из баз приложения.

Чтобы просмотреть список исключений из проверки зашифрованных соединений, добавленных пользователем, выполните следующую команду:

```
kesl-control -N --query user
```

Чтобы просмотреть список исключений из проверки зашифрованных соединений, добавленных приложением, выполните следующую команду:

```
kesl-control -N --query auto
```

Чтобы просмотреть список исключений из проверки зашифрованных соединений, полученных из баз приложения, выполните следующую команду:

```
kesl-control -N --query kl
```

Чтобы очистить список доменов, которые приложение автоматически исключило из проверки, выполните следующую команду:

```
kesl-control [-N] --clear-web-auto-excluded
```

Управление списком доверенных корневых сертификатов

Чтобы добавить сертификат в список доверенных корневых сертификатов, выполните следующую команду:

```
kesl-control --add-certificate <path to the certificate>
```

где:

`<path to the certificate>` – путь к файлу сертификата, который вы хотите добавить, в формате PEM или DER.

Чтобы удалить сертификат из списка доверенных корневых сертификатов, выполните следующую команду:

```
kesl-control --remove-certificate <subject of the certificate>
```

Чтобы просмотреть список доверенных корневых сертификатов, выполните следующую команду:

```
kesl-control --list-certificates
```

Для каждого сертификата отображается следующая информация:

- субъект сертификата;
- серийный номер;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- отпечаток сертификата SHA256.

Настройка и просмотр исключений из перехвата трафика

Чтобы добавить исключение из перехвата трафика, выполните команду:

```
kesl-control --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port <destination port>
```

где:

- `<in|out>` – направление трафика в исключаемом соединении. Вы можете настроить исключение для входящего трафика или для исходящего трафика.
- `<remote IP address>` – адрес удаленного устройства в формате IPv4 или IPv6. В зависимости от направления трафика будет исключаться трафик с указанного IP-адреса (исключение для входящего трафика) или трафик на указанный IP-адрес (исключение для исходящего трафика).
- `<destination port>` – в зависимости от направления трафика:
  - Порт на защищенном устройстве (исключение для входящего трафика). Из перехвата будет исключаться трафик на этот порт с удаленных устройств.
  - Порт на удаленном устройстве (исключение для исходящего трафика). Из перехвата будет исключаться трафик на этот порт с защищенного устройства.

Вы можете указать в исключении только IP-адрес удаленного устройства или только порт назначения.

Если в исключении для входящего трафика вы указываете только IP-адрес удаленного устройства (без указания порта на защищенном устройстве), весь трафик с удаленного устройства исключается из перехвата. Настраивать такое исключение рекомендуется только для трафика с устройств, которым вы доверяете.

Чтобы просмотреть список настроенных исключений из перехвата трафика, выполните команду:

```
kesl-control --list-bypass-endpoints
```

Для каждого исключения отображается следующая информация:

- порядковый номер исключения;
- направление трафика в соединении;
- IP-адрес удаленного устройства;
- номер порта.

Чтобы удалить исключение из перехвата трафика, выполните команду:

```
kesl-control --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

где:

- `<in|out>` – направление трафика в исключаемом соединении.
- `<remote IP address>` – адрес удаленного устройства в формате IPv4 или IPv6, трафик на который или с которого исключается из перехвата (в зависимости от направления трафика).
- `<destination port>` – порт на защищенном устройстве (исключение для входящего трафика) или порт на удаленном устройстве (исключение для исходящего трафика).

Задача Защита от сетевых угроз

В командной строке вы можете управлять защитой от сетевых угроз с помощью предустановленной задачи Защита от сетевых угроз (`Network_Threat_Protection`).

По умолчанию задача Защита от сетевых угроз не запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры защиты от сетевых угроз, изменяя параметры предустановленной задачи Защита от сетевых угроз.

Параметр	Описание	Значения
`ActionOnDetect`	Действие, выполняемое при обнаружении сетевой активности, характерной для сетевых атак. При изменении значения этого параметра с `Block` на `Notify` список заблокированных устройств очищается.	`Notify` – разрешить сетевую активность, записать в журнал информацию об обнаруженной сетевой активности. Если указано это значение, значение параметра `BlockAttackingHosts` не учитывается. `Block` (значение по умолчанию) – заблокировать сетевую активность и записать в журнал информацию об этом.
`BlockAttackingHosts`	Блокировка сетевой активности со стороны атакующих устройств.	`Yes` (значение по умолчанию) – заблокировать сетевую активность атакующего устройства. `No` – не блокировать сетевую активность атакующего устройства. Если указано это значение, а для параметра `ActionOnDetect` указано значение `Block`, приложение блокирует сетевую активность со стороны атакующего устройства, но не вносит это устройство в список заблокированных устройств.
`BlockDurationMinutes`	Продолжительность блокировки атакующих устройств (в минутах).	1 – 32768 Значение по умолчанию: 60.
`UseExcludeIPs`	Использование списка IP-адресов, сетевую активность которых не требуется блокировать при обнаружении сетевой атаки. Приложение записывает в журнал информацию о вредоносной активности со стороны этих устройств. Вы можете добавить IP-адреса в список исключений с помощью параметра `ExcludeIPs.item_#`.	`Yes` – использовать список исключений IP-адресов. `No` (значение по умолчанию) – не использовать список исключений IP-адресов.
`ExcludeIPs.item_#`	IP-адреса, сетевая активность которых не блокируется приложением. По умолчанию список пуст.	`d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255. `d.d.d.d/p` – подсеть адресов IPv4, где p – число от 0 до 32. `x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. `x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64. Значение по умолчанию не задано.

Управление сетевым экраном

В командной строке вы можете настраивать управление сетевым экраном с помощью предустановленной задачи Управление сетевым экраном (`Firewall_Management`).

По умолчанию задача Управление сетевым экраном не запущена. Вы можете запускать и останавливать эту задачу вручную.

Вы можете настраивать параметры управления сетевым экраном, изменяя параметры предустановленной задачи Управление сетевым экраном.

Вы также можете настраивать параметры управления сетевым экраном с помощью команд управления сетевым экраном:

- Создавать и удалять сетевые пакетные правила и изменять приоритет их выполнения.
- Формировать список IP-адресов или подсетей в сетевых зонах.
- Просматривать созданные в приложении правила сетевого экрана с помощью команды:

```
kesl-control -F --query
```

Параметр	Описание	Значения
`DefaultIncomingAction`	Действие по умолчанию, применяемое ко входящему соединению, если другие сетевые правила не применяются к этому виду соединения.	`Allow` (значение по умолчанию) – разрешать входящие соединения. `Block` – запрещать входящие соединения.
`DefaultIncomingPacketAction`	Действие по умолчанию, применяемое ко входящему пакету, если другие сетевые пакетные правила не применяются к этому виду соединения.	`Allow` (значение по умолчанию) – разрешать входящие пакеты. `Block` – запрещать входящие пакеты.
`OpenNagentPorts`	Добавление динамических правил для Агента администрирования в пакетные правила.	`Yes` (значение по умолчанию) – добавлять динамические правила для Агента администрирования в пакетные правила. `No` – не добавлять динамические правила для Агента администрирования в пакетные правила.
Секция **[PacketRules.item_#]** содержит сетевые пакетные правила для задачи Управление сетевым экраном. Вы можете указать несколько секций `[PacketRules.item_#]` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Каждая секция `[PacketRules.item_#]` содержит следующие параметры:		
`Name`	Имя сетевого пакетного правила.	Значение по умолчанию: `Packet rule #<n>`, где n – это индекс.
`FirewallAction`	Действие, применяемое к соединениям, указанным в сетевом пакетном правиле.	`Allow` (значение по умолчанию) – разрешать сетевые соединения. `Block` – запрещать сетевые соединения.

`Protocol`	Тип протокола, для которого необходим мониторинг сетевой активности.	`Any` (значение по умолчанию) – задача Управление сетевым экраном контролирует всю сетевую активность.
		`TCP`
		`UDP`
		`ICMP`
		`ICMPv6`
		`IGMP`
		`GRE`

`RemotePorts`	Номера портов удаленных устройств, соединение между которыми отслеживается. Вы можете указать значение в виде целого числа или в виде интервала. Этот параметр можно указать, только если для параметра `Protocol` установлено значение `TCP` или `UDP`.	`Any` (значение по умолчанию) – контролировать все удаленные порты. `0 – 65535`.
`LocalPorts`	Номера портов локальных устройств, соединение между которыми отслеживается. Вы можете указать значение в виде целого числа или в виде интервала. Этот параметр можно указать, только если для параметра `Protocol` установлено значение `TCP` или `UDP`.	`Any` (значение по умолчанию) – контролировать все локальные порты. `0 – 65535`.
`ICMPType`	Тип пакета ICMP. Этот параметр можно указать, только если для параметра `Protocol` установлено значение `ICMP` или `ICMPv6`.	`Any` (значение по умолчанию) – контролировать все типы пакетов ICMP. Целое число согласно спецификации протокола передачи данных.
`ICMPCode`	Код пакета ICMP. Этот параметр можно указать, только если для параметра `Protocol` установлено значение `ICMP` или `ICMPv6`.	`Any` (значение по умолчанию) – контролировать все коды пакетов ICMP. Целое число согласно спецификации протокола передачи данных.

Параметр	Описание	Значения
`Direction`	Направление отслеживаемой сетевой активности.	`IncomingOutgoing` или `InOut` (значение по умолчанию) – контролировать как входящие, так и исходящие соединения. `Incoming` или `In` – контролировать только входящие соединения. `Outgoing` или `Out` – контролировать только исходящие соединения. `IncomingPacket` или `InPacket` – контролировать только входящие пакеты. `OutgoingPacket` или `OutPacket` – контролировать только исходящие пакеты. `IncomingOutgoingPacket` или `InOutPacket` – контролировать как входящие, так и исходящие пакеты.
`RemoteAddress`	Сетевые адреса удаленных устройств, которые могут передавать и получать сетевые пакеты.	`Any` (значение по умолчанию) – контролируется отправка и / или получение сетевых пакетов удаленными устройствами с любым IP-адресом. `Trusted` – заданная сетевая зона для доверенных сетей. `Local` – заданная сетевая зона для локальных сетей. `Public` – заданная сетевая зона для публичных сетей. `d.d.d.d` – адрес версии IPv4, где d – десятичное число от 0 до 255. `d.d.d.d – d.d.d.d` – диапазон адресов версии IPv4. `d.d.d.d/p` – подсеть адресов версии IPv4, где p – число от 0 до 32. `x:x:x:x:x:x:x:x` – адрес версии IPv6, где x – шестнадцатеричное число от 0 до ffff. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` – диапазон адресов версии IPv6. x:x:x:x:x:x:x:x/p – подсеть адресов версии IPv6, где p – число от 0 до 128, можно использовать **::** для сокращения.
`LocalAddress`	Сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты.	`Any` (значение по умолчанию) – контролируется отправка и / или получение сетевых пакетов локальными устройствами с любым IP-адресом. `d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255. `d.d.d.d – d.d.d.d` – диапазон адресов версии IPv4. `d.d.d.d/p` – подсеть адресов версии IPv4, где p – число от 0 до 32. `x:x:x:x:x:x:x:x` – адрес версии IPv6, где x – шестнадцатеричное число от 0 до ffff. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` – диапазон адресов версии IPv6. x:x:x:x:x:x:x:x/p – подсеть адресов версии IPv6, где p – число от 0 до 128, можно использовать **::** для сокращения.
`LogAttempts`	Включение записи в отчет действия сетевого правила.	`Yes` – записывать действия в отчет. `No` (значение по умолчанию) – не записывать действия в отчет.
Секция **[NetworkZonesPublic]** содержит сетевые адреса, связанные с публичными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		

Параметр	Описание	Значения
`Address.item_#`	Указывает IP-адрес или IP-подсеть.	`d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255. `d.d.d.d/p` – подсеть адресов IPv4, где p – число от 0 до 32. `x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. `x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64. Значение по умолчанию: "" (в этой зоне нет сетевых адресов).
Секция **[NetworkZonesLocal]** содержит сетевые адреса, связанные с локальными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		
`Address.item_#`	Указывает IP-адрес или IP-подсеть.	`d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255. `d.d.d.d/p` – подсеть адресов IPv4, где p – число от 0 до 32. `x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. `x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64. Значение по умолчанию: `""` (в этой зоне нет сетевых адресов).
Секция **[NetworkZonesTrusted]** содержит сетевые адреса, связанные с доверенными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		
`Address.item_#`	Указывает IP-адрес или IP-подсеть.	`d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255. `d.d.d.d/p` – подсеть адресов IPv4, где p – число от 0 до 32. `x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. `x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64. Значение по умолчанию: `""` (в этой зоне нет сетевых адресов).

Настройка списка сетевых пакетных правил

Чтобы добавить сетевое пакетное правило, выполните следующую команду:

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

где:

- `--name <rule name>` – название сетевого пакетного правила.
- `--action <Allow|Block>` – действие, применяемое к соединениям, указанным в сетевом пакетном правиле.
- `--protocol <protocol>` – тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность.
- `--direction <direction>` – направление отслеживаемой сетевой активности.

- `--remote <remote address>:<port>` – сетевой адрес удаленного устройства. Вы можете указать имя предустановленной сетевой зоны в качестве удаленного адреса.

- `--local <local address>:<port>` – сетевой адрес устройства с установленным приложением Kaspersky Endpoint Security.

- `--at <index>` – индекс правила в списке сетевых пакетных правил. Если ключ `--at` не указан или его значение больше количества правил в списке, новое правило добавляется в конец списка.

Для параметров, значения которых вы не указали в команде, устанавливаются значения по умолчанию.

Пример создания правила, блокирующего все входящие и создаваемые соединения по протоколу TCP через порт 23

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
any
```

Пример создания правила, блокирующего входящие и создаваемые соединения по протоколу TCP через порт 23 для сетевой зоны Публичные

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
Public
```

Чтобы удалить сетевое пакетное правило, выполните одну из следующих команд:

```
kesl-control --del-rule --name <rule name>
```

либо

```
kesl-control --del-rule --index <current index>
```

где:

- `--name <rule name>` – название сетевого пакетного правила.

- `--index <current index>` – текущий индекс правила в списке сетевых пакетных правил.

Если список сетевых пакетных правил содержит несколько правил с одинаковым именем или не содержит правило с указанным именем или индексом, происходит ошибка.

Чтобы изменить приоритет выполнения сетевого пакетного правила, выполните одну из следующих команд:

```
kesl-control --move-rule --name <rule name> --at < new index>
```

либо

```
kesl-control --move-rule --index <current index> --at <new index>
```

где:

- `--name <rule name>` – название сетевого пакетного правила.
- `--index <current index>` – текущий индекс правила в списке сетевых пакетных правил.
- `--at <new index>` – новый индекс правила в списке сетевых пакетных правил.

Настройка сетевых зон

Чтобы добавить сетевой адрес в зону, выполните следующую команду:

```
kesl-control --add-zone <zone> --address <address>
```

где:

- `<zone>` – предустановленное имя сетевой зоны. Возможные значения: `Public`, `Local`, `Trusted`.
- `<address>` – сетевой адрес или подсеть.

Чтобы удалить сетевой адрес из зоны, выполните одну из следующих команд:

```
kesl-control --del-zone <zone> --address <address>
```

либо

```
kesl-control --del-zone <zone> --index <address index in the zone>
```

Если зона содержит несколько элементов с одинаковым сетевым адресом, команда `--del-zone` не будет выполнена.

Если указанный сетевой адрес или индекс не существует, отображается сообщение об ошибке.

Контроль безопасности

Задача Контроль устройств

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Контроль устройств (`Device_Control`).

Параметр	Описание	Значения
`OperationMode`	Режим работы приложения при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств.	`Block` (значение по умолчанию) – приложение применяет режим доступа, заданный для устройства или шины. `Notify` – приложение тестирует выбранный режим доступа и формирует событие об обнаружении попытки доступа к устройству.
`AllowToRequestTemporaryAccess`	Разрешение запрашивать временный доступ к заблокированному устройству. Предоставление доступа к заблокированному устройству доступно, только если в организации развернуто приложение Kaspersky Security Center 16.1 и клиентское устройство имеет возможность установить связь с Сервером администрирования.	`Yes` – разрешить пользователю запрашивать временный доступ к заблокированному устройству в графическом интерфейсе или командной строке приложения. `No` (значение по умолчанию) – запретить пользователю запрашивать временный доступ к заблокированному устройству.
Секция **[DeviceClass]** содержит режимы доступа к устройствам в зависимости от их типа.		
`HardDrive`	Режим доступа к жестким дискам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к жестким дискам. `DependsOnBus` (значение по умолчанию) – доступ к жесткому диску зависит от режима доступа для шины подключения, по которой подключен диск. `Block` – пользователям запрещен доступ ко всем жестким дискам (за исключением системных жестких дисков, которые Контроль устройств не блокирует). `ByRule` – доступ к жестким дискам зависит от правил доступа. `ReadOnly` – пользователям разрешен доступ к жестким дискам только на чтение, запись запрещена.
`RemovableDrive`	Режим доступа к съемным дискам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к съемным дискам. `DependsOnBus` (значение по умолчанию) – доступ к съемному диску зависит от режима доступа для шины подключения, по которой подключен диск. `Block` – пользователям запрещен доступ к съемным дискам. `ByRule` – доступ к съемным дискам зависит от правил доступа. `ReadOnly` – пользователям разрешен доступ к съемным дискам только на чтение, запись запрещена.
`FloppyDrive`	Режим доступа к дискетам, подключенным к клиентскому устройству. Приложение не блокирует дискеты, подключенные к клиентскому устройству с помощью шины ISA.	`Allow` – пользователям разрешен доступ к дискетам. `DependsOnBus` (значение по умолчанию) – доступ к дискете зависит от режима доступа для шины подключения, по которой подключена дискета. `Block` – пользователям запрещен доступ к дискетам. `ByRule` – доступ к дискетам зависит от правил доступа. `ReadOnly` – пользователям разрешен доступ к дискетам только на чтение, запись запрещена.

Параметр	Описание	Значения
`OpticalDrive`	Режим доступа к CD/DVD-приводам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к CD/DVD-приводам. `DependsOnBus` (значение по умолчанию) – доступ к CD/DVD-приводу зависит от режима доступа для шины подключения, по которой подключен CD/DVD-привод. `Block` – пользователям запрещен доступ к CD/DVD-приводам. `ByRule` – доступ к CD/DVD-приводам зависит от правил доступа. `ReadOnly` – пользователям разрешен доступ к CD/DVD-приводам только на чтение, запись запрещена.
`SerialPortDevice`	Режим доступа к устройствам, подключенным к клиентскому устройству через последовательный порт. Приложение не блокирует устройства, подключенные к клиентскому устройству через последовательный порт с помощью шины ISA.	`Allow` – пользователям разрешен доступ к устройствам, подключенным через последовательный порт. `DependsOnBus` (значение по умолчанию) – доступ к устройству, подключенному через последовательный порт, зависит от режима доступа для шины подключения. `Block` – пользователям запрещен доступ к устройствам, подключенным через последовательный порт.
`ParallelPortDevice`	Режим доступа к устройствам, подключенным к клиентскому устройству через параллельный порт.	`Allow` – пользователям разрешен доступ к устройствам, подключенным через параллельный порт. `DependsOnBus` (значение по умолчанию) – доступ к устройству, подключенному через параллельный порт, зависит от режима доступа для шины подключения. `Block` – пользователям запрещен доступ к устройствам, подключенным через параллельный порт.
`Printer`	Режим доступа к принтерам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к принтерам. `DependsOnBus` (значение по умолчанию) – доступ к принтеру зависит от режима доступа для шины подключения, по которой подключен принтер. `Block` – пользователям запрещен доступ к принтерам.
`Modem`	Режим доступа к модемам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к модемам. `DependsOnBus` (значение по умолчанию) – доступ к модему зависит от режима доступа для шины подключения, по которой подключен модем. `Block` – пользователям запрещен доступ к модемам.
`TapeDrive`	Режим доступа к стримерам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к стримерам. `DependsOnBus` (значение по умолчанию) – доступ к стримеру зависит от режима доступа для шины подключения, по которой подключен стример. `Block` – пользователям запрещен доступ к стримерам.
`MultifuncDevice`	Режим доступа к мультифункциональным устройствам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к мультифункциональным устройствам. `DependsOnBus` (значение по умолчанию) – доступ к мультифункциональному устройству зависит от режима доступа для шины подключения, по которой подключено устройство. `Block` – пользователям запрещен доступ к мультифункциональным устройствам.

Параметр	Описание	Значения
`SmartCardReader`	Режим доступа к устройствам чтения смарт-карт, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к устройствам чтения смарт-карт. `DependsOnBus` (значение по умолчанию) – доступ к устройству чтения смарт-карт зависит от режима доступа для шины подключения, по которой подключено устройство. `Block` – пользователям запрещен доступ к устройствам чтения смарт-карт.
`WiFiAdapter`	Режим доступа к Wi-Fi-адаптерам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к Wi-Fi-адаптерам. `DependsOnBus` (значение по умолчанию) – доступ к Wi-Fi-адаптеру зависит от режима доступа для шины подключения. `Block` – пользователям запрещен доступ к Wi-Fi-адаптерам.
`NetworkAdapter`	Режим доступа к внешним сетевым адаптерам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к внешним сетевым адаптерам. `DependsOnBus` (значение по умолчанию) – доступ к внешнему сетевому адаптеру зависит от режима доступа для шины подключения, по которой подключен адаптер. Контроль устройств не позволяет запрещать доступ к внешним сетевым адаптерам во избежание отключения клиентского устройства от сети.
`PortableDevice`	Режим доступа к портативным устройствам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к портативным устройствам. `DependsOnBus` (значение по умолчанию) – доступ к портативному устройству зависит от режима доступа для шины подключения, по которой подключено устройство. `Block` – пользователям запрещен доступ к портативным устройствам.
`BluetoothDevice`	Режим доступа к Bluetooth-устройствам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к Bluetooth-устройствам. `DependsOnBus` (значение по умолчанию) – доступ к Bluetooth-устройству зависит от режима доступа для шины подключения, по которой подключено устройство. `Block` – пользователям запрещен доступ к Bluetooth-устройствам.
`ImagingDevice`	Режим доступа к устройствам обработки изображений, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к устройствам обработки изображений. `DependsOnBus` (значение по умолчанию) – доступ к устройству обработки изображений зависит от режима доступа для шины подключения, по которой подключено устройство. `Block` – пользователям запрещен доступ к устройствам обработки изображений.
`SoundAdapter`	Режим доступа к звуковым адаптерам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к звуковым адаптерам. `DependsOnBus` (значение по умолчанию) – доступ к звуковому адаптеру зависит от режима доступа для шины подключения, по которой подключено устройство. `Block` – пользователям запрещен доступ к звуковым адаптерам.

Параметр	Описание	Значения
`InputDevice`	Режим доступа к устройствам ввода, подключенным к клиентскому устройству (клавиатура, мышь, тачпад и другие).	`Allow` – пользователям разрешен доступ к устройствам ввода. `DependsOnBus` (значение по умолчанию) – доступ к устройству ввода зависит от режима доступа для шины подключения, по которой подключено устройство. `Block` – пользователям запрещен доступ к устройствам ввода.
Секция **[DeviceBus]** содержит режимы доступа для шин подключения.		
`USB`	Режим доступа для устройств, подключенных к клиентскому устройству через USB-интерфейс.	`Allow` (значение по умолчанию) – пользователям разрешен доступ к USB-устройствам. `Block` – пользователям запрещен доступ к USB-устройствам.
`FireWire`	Режим доступа для устройств, подключенных к клиентскому устройству через интерфейс FireWire.	`Allow` (значение по умолчанию) – пользователям разрешен доступ к устройствам, подключенным через интерфейс FireWire. `Block` – пользователям запрещен доступ к устройствам, подключенным через интерфейс FireWire.
Секция **[TrustedDevices.item_#]** содержит доверенные устройства.		
`DeviceId`	Идентификатор или маска идентификатора доверенного устройства.	Вы можете использовать маски * (любая последовательность символов) или ? (один любой символ), чтобы указать идентификатор устройства. Примеры: *Чтобы запретить доступ ко всем USB-устройствам, кроме указанного, укажите следующие параметры:* В секции `[DeviceBus]` параметр `USB=Block` В секции `[TrustedDevices.item_#]` параметр `DeviceId=<device ID>` *Чтобы запретить доступ ко всем USB-устройствам, но разрешить доступ ко всем USB-накопителям, укажите следующие параметры:* В секции `[DeviceBus]` параметр `USB=Block` В секции `[TrustedDevices.item_#]` параметр `DeviceId=USBSTOR*`
`Comment`	Комментарий к указанному доверенному устройству.	—
Секция **[TrustedDevices.item_#.Principals.item_#]** содержит правила доступа к доверенннному устройству.		
`Principal`	Пользователь или группа пользователей, для которых устройство будет доверенным. Если для устройства назначен тип доступа "только чтение", при назначении доверенного устройства на определенного пользователя, назначенный пользователь игнорируется и устройство становится доступным для записи всем пользователям.	`\Everyone` (значение по умолчанию) – устройство будет доверенным для всех пользователей. `<user name>` – имя локального или доменного пользователя (без указания полного имени с доменом, если система допускает ввод имен пользователей в таком формате, или в формате <domain name>\`<user name>` или `<user name>`@<domain name>), для которого устройство будет доверенным. `@<group name>` – название группы пользователей (локальной или доменной), для которых устройство будет доверенным.
Секция **[Schedules.item_#]** содержит расписание доступа для устройств. Вы можете настраивать расписание только для жестких дисков, съемных дисков, дискет и CD/DVD-приводов.		
`ScheduleName`	Название расписания. Название расписания должно быть уникальным.	Значение по умолчанию: `Default`. Расписание `Default` (по умолчанию) обеспечивает полный доступ к устройствам для всех пользователей в любое время, если для соответствующего типа устройства разрешен доступ по шине подключения. Расписание `Default` удалить нельзя.

Параметр	Описание	Значения
DaysHours	Интервалы времени для расписания.	All (значение по умолчанию) – расписание действует 24/7 (без ограничений по времени). <weekday> – дни недели. Вы можете использовать как полные названия дней недели, так и аббревиатуры (например, для понедельника можно указать Mo, Mon или Monday). Для дней недели можно указывать либо интервалы, либо конкретные дни. Неделя начинается с воскресенья. <hour> – часы [0:24]. Для часов можно указывать только интервалы. Пример расписания schedule_1, действующего с воскресенья по субботу с 0 до 11, с 12 до 15 и с 16 до 24 [Schedules.item_0001] ScheduleName=schedule_1 DaysHours=Su-Sa:0..11,12..15,16..24 Пример расписания schedule_2, действующего по четвергам с 12 до 14 и по пятницам с 2 до 15 и с 16 до 24 [Schedules.item_0002] ScheduleName=schedule_2 DaysHours=Th:12..14;Fr:2..15,16..24 Пример расписания schedule_3, действующего 24 часа 7 дней в неделю [Schedules.item_0003] ScheduleName=schedule_3 DaysHours=All
Секция **[HardDrivePrincipals.item_#]** содержит правила доступа к жестким дискам. Для жестких дисков должно быть включено хотя бы одно расписание. Вы можете назначить несколько правил доступа к жесткому диску. Также для пользователя или группы пользователей можно указать несколько расписаний. Если возникает конфликт правила доступа для пользователя или группы, предоставляются минимальные права доступа.		
Principal	Пользователь или группа пользователей, к которым применяется правило доступа.	\Everyone (значение по умолчанию) – правило доступа применяется для всех пользователей. <user name> – имя локального пользователя, для которого применяется правило доступа. @<group name> – название группы пользователей, для которых применяется правило доступа.
[HardDrivePrincipals.item_#.AccessRules.item_#] содержит параметры правил доступа.		
UseRule	Показывает, включено или выключено правило.	Yes (значение по умолчанию) – правило доступа включено. No – правило доступа выключено.
ScheduleName	Расписание, указанное в секции [Schedules.item_#].	Значение по умолчанию: Default.
Access	Тип доступа.	Allow (значение по умолчанию) – доступ к жестким дискам разрешен. Block – доступ к жестким дискам запрещен.
Секция **[RemovableDrivePrincipals.item_#]** содержит правила доступа к съемным дискам. Для съемных дисков должно быть включено хотя бы одно расписание. Вы можете назначить несколько правил доступа к съемному диску. Также для пользователя или группы пользователей можно указать несколько расписаний. Если возникает конфликт правила доступа для пользователя или группы, предоставляются минимальные права доступа.		
Principal	Пользователь или группа пользователей, к которым применяется правило доступа.	\Everyone (значение по умолчанию) – правило доступа применяется для всех пользователей. <user name> – имя локального пользователя, для которого применяется правило доступа. @<group name> – название группы пользователей, для которых применяется правило доступа.
[RemovableDrivePrincipals.item_#.AccessRules.item_#] содержит параметры правил доступа.		
UseRule	Показывает, включено или выключено правило.	Yes (значение по умолчанию) – правило доступа включено. No – правило доступа выключено.
ScheduleName	Расписание, указанное в секции [Schedules.item_#].	Значение по умолчанию: Default.

Параметр	Описание	Значения
`Access`	Тип доступа.	`Allow` (значение по умолчанию) – доступ к съемным дискам разрешен. `Block` – доступ к съемным дискам запрещен.
Секция **[FloppyDrivePrincipals.item_#]** содержит правила доступа к дискетам. Для дискет должно быть включено хотя бы одно расписание. Вы можете назначить несколько правил доступа к дискете. Также для пользователя или группы пользователей можно указать несколько расписаний. Если возникает конфликт правила доступа для пользователя или группы, предоставляются минимальные права доступа.		
`Principal`	Пользователь или группа пользователей, к которым применяется правило доступа.	`\Everyone` (значение по умолчанию) – правило доступа применяется для всех пользователей. `<user name>` – имя локального пользователя, для которого применяется правило доступа. `@<group name>` – название группы пользователей, для которых применяется правило доступа.
`[FloppyDrivePrincipals.item_#.AccessRules.item_#]` содержит параметры правил доступа.		
`UseRule`	Показывает, включено или выключено правило.	`Yes` (значение по умолчанию) – правило доступа включено. `No` – правило доступа выключено.
`ScheduleName`	Расписание, указанное в секции `[Schedules.item_#]`.	Значение по умолчанию: `Default`.
`Access`	Тип доступа.	`Allow` (значение по умолчанию) – доступ к дискетам разрешен. `Block` – доступ к дискетам запрещен.
Секция **[OpticalDrivePrincipals.item_#]** содержит правила доступа к CD/DVD-приводам. Для CD/DVD-приводов должно быть включено хотя бы одно расписание. Вы можете назначить несколько правил доступа к CD/DVD-приводу. Также для пользователя или группы пользователей можно указать несколько расписаний. Если возникает конфликт правила доступа для пользователя или группы, предоставляются минимальные права доступа.		
`Principal`	Пользователь или группа пользователей, к которым применяется правило доступа.	`\Everyone` (значение по умолчанию) – правило доступа применяется для всех пользователей. `<user name>` – имя локального пользователя, для которого применяется правило доступа. `@<group name>` – название группы пользователей, для которых применяется правило доступа.
`[OpticalDrivePrincipals.item_#.AccessRules.item_#]` содержит параметры правил доступа.		
`UseRule`	Показывает, включено или выключено правило.	`Yes` (значение по умолчанию) – правило доступа включено. `No` – правило доступа выключено.
`ScheduleName`	Расписание, указанное в секции `[Schedules.item_#]`.	Значение по умолчанию: `Default`.
`Access`	Тип доступа.	`Allow` (значение по умолчанию) – доступ к CD/DVD-приводам разрешен. `Block` – доступ к CD/DVD-приводам запрещен.

Веб-Контроль

В командной строке вы можете управлять Веб-Контролем с помощью предустановленной задачи Веб-Контроль (`Web_Control`).

Задача Веб-Контроль по умолчанию остановлена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры Веб-Контроля, изменяя параметры предустановленной задачи Веб-Контроль.

Вы также можете просматривать и настраивать параметры Веб-Контроля с помощью команд управления Веб-Контролем.

Задача Веб-Контроль

В таблице ниже описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Веб-Контроль (`Web_Control`).

Параметры задачи Веб-Контроль

Параметр	Описание	Значения
`WebControlDefaultAction`	Правило по умолчанию, то есть действие, которое Веб-Контроль будет выполнять при обнаружении попытки доступа к веб-ресурсам, которые не попадают под действие других правил.	`Allow` (значение по умолчанию) – разрешать доступ к веб-ресурсам. `Block` – запрещать доступ к веб-ресурсам.
`ComplaintRecipient`	Адрес электронной почты администратора для оправки ему сообщения об ошибочной блокировке веб-ресурса.	
Секция **[Rules.item_#]** содержит следующие параметры:		
`Name`	Название правила доступа к веб-ресурсам. Название правила должно быть уникальным.	
`WebControlAction`	Действие правила, которое Веб-Контроль будет выполнять при обнаружении попытки доступа к веб-ресурсу, удовлетворяющему правилу.	`Allow` (значение по умолчанию) – разрешать доступ к веб-ресурсу. `Block` – запрещать доступ к веб-ресурсу. `Notify` – выводить предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.
`Enabled`	Статус работы правила доступа к веб-ресурсам.	`Yes` – правило включено, Веб-Контроль применяет это правило во время работы. `No` (значение по умолчанию) – правило выключено и не используется во время работы Веб-Контроля.
`ScheduleId`	Идентификатор расписания, который используется в секции `[Schedules.item_#]`.	
`UseUrls`	Использование в правиле фильтра адресов веб-ресурса.	`Yes` – использовать в правиле фильтр адресов веб-ресурсов. `No` (значение по умолчанию) – не использовать фильтр адресов веб-ресурсов, применять правило ко всем адресам веб-ресурсов.
`Urls.item_#`	Адрес веб-ресурса, доступ к которому регулирует правило.	Для указания адреса веб-ресурса вы можете использовать маски.
`UseCategories`	Использование в правиле фильтров по категориям содержания и по категориям типов данных.	`None` (значение по умолчанию) – не использовать фильтр содержимого веб-ресурсов. `ContentOnly` – использовать в правиле фильтр по категориям содержания. `FormatOnly` – использовать в правиле фильтр категориям типов данных. `ContentAndFormat` – использовать в правиле фильтр по категориям содержания и категориям типов данных.
`[Rules.item_#.ContentCategories.item_#]`	Секция для указания категории содержания.	–

Параметр	Описание	Значения
ContentCategory	Категория содержания.	AdultContent, AlcoholTobaccoNarcotics, Violence, Profanity, Weapons, ChatForum, WebMail, OnlineShops, SocialNets, Recruitment, HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweepstakes, InternetCommunicationMedia, CryptocurAndMining, LegislationBE, ECommerce, ComputerGames, Religions, News, Torrents, FileSharing, AudioAndVideo, BankSites, Blogs, DatingSites, LegislationRF, LegislationGlobal, SexuallyExplicit, Sexuality, AITools
[Rules.item_#.FormatCategories.item_#]	Секция для указания категории типов данных.	–
FormatCategory	Категория типов данных.	Video – Видео Audio – Звуковые данные OfficeDocument – Файлы офисных приложений Executable – Исполняемые файлы Archives – Архивы Images – Графические файлы Scripts – Скрипты
UsePrincipals	Использование фильтра пользователей, на которых распространяется правило доступа к веб-ресурсам.	Yes – использовать в правиле фильтр пользователей. No (значение по умолчанию) – не использовать фильтр пользователей, применять правило ко всем пользователям.
[Rules.item_#.Principals.item_#]	Секция для указания пользователей, на которых распространяется правило доступа к веб-ресурсам.	
Name	Пользователь или группа пользователей, на которых распространяется правило доступа к веб-ресурсам.	<username> – имя пользователя, для которого применяется правило. @<groupname> – название группы пользователей, для которых применяется правило. Значение по умолчанию: правило доступа к веб-ресурсам применяется для всех пользователей.
Секция **[UrlCategories.item_#]** содержит следующие параметры:		
Name	Название группы адресов веб-ресурсов, доступ к которым регулирует правило.	
Urls.item_#	Адрес веб-ресурса, входящего в группу.	Для указания адреса веб-ресурса вы можете использовать маски.
Секция **[Schedules.item_#]** содержит расписание работы правила.		
Id	Идентификатор расписания, который используется в секции [Rules.item_#].	1 – 999999 0 – идентификатор расписания Default (по умолчанию), которое обеспечивает работу правила без ограничений по времени, то есть в любое время.

Параметр	Описание	Значения
`Name`	Название расписания.	
`DaysHours`	Интервалы времени для расписания.	`<weekday>` – дни недели. Вы можете использовать как полные названия дней недели, так и аббревиатуры (например, для понедельника можно указать `Mo`, `Mon` или `Monday`). Для дней недели можно указывать либо интервалы, либо конкретные дни. Неделя начинается с воскресенья. `<hour>` – часы [0:24]. Для часов вы можете указывать только интервалы.

Просмотр и изменение параметров Веб-Контроля

Чтобы просмотреть параметры Веб-Контроля, выполните следующую команду:

```
kesl-control --get-settings 26 [--file <path to the configuration file>] [--json]
```

где:

`--file <path to the configuration file>` – полный путь к конфигурационному файлу, в который будут выведены параметры.

`--json` – выводить данные в формате JSON.

Чтобы изменить параметры Веб-Контроля, выполните следующую команду:

```
kesl-control --set-settings 26 [--file <path to the configuration file>] [--json]
```

где:

`--file <path to the configuration file>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры.

`--json` – импорт данных из файла в формате JSON.

Чтобы удалить настроенные параметры и восстановить значения параметров Веб-Контроля до правила по умолчанию, выполните следующую команду:

```
kesl-control --set-settings 26 --set-to-default
```

Контроль приложений

В командной строке вы можете управлять контролем приложений с помощью предустановленной задачи Контроль приложений (`Application_Control`).

По умолчанию задача Контроль приложений не запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры контроля приложений на устройстве, изменяя параметры предустановленной задачи Контроль приложений.

Если вы меняете список разрешенных приложений или запрещаете запуск всех приложений и/или приложений, влияющих на работу Kaspersky Endpoint Security, то при изменении параметров задачи с помощью конфигурационного файла или с помощью ключей командной строки требуется запускать следующую команду:

```
kesl-control --set-settings --accept
```

Вы также можете настраивать параметры Контроля приложений с помощью команд управления Контролем приложений:

- Создавать и изменять списки категорий.
- Просматривать список созданных в приложении категорий.
- Настраивать список правил контроля приложений.

Задача Контроль приложений

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Контроль приложений (`Application_Control`).

Параметры задачи Контроль приложений

Параметр	Описание	Значения
`AppControlMode`	Режим работы компонента Контроль приложений.	`AllowList` – Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. `DenyList` (значение по умолчанию) – Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.
`AppControlRulesAction`	Действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам.	`ApplyRules` (значение по умолчанию) – Kaspersky Endpoint Security применяет правила контроля приложений и выполняет заданное в правилах действие. `TestRules` – Kaspersky Endpoint Security тестирует правила и формирует событие об обнаружении приложения, удовлетворяющего правилу.
Секция **[Categories.item_#]** содержит следующие параметры:		
`Name`	Название категории приложений, для которой будет применяться правило.	
`UseIncludes`	Использование включающих условий для срабатывания правила.	`Yes` – применять правило к приложению, если приложение соответствует хотя бы одному включающему условию. `No` (значение по умолчанию) – не применять правило к приложению, даже если приложение соответствует включающему условию.
`IncludeFileNames.item_#`	Имя исполняемого файла, на которое срабатывает правило.	Для указания имени файла вы можете использовать маски.
`IncludeFolders.item_#`	Имя директории с исполняемым файлом приложения, на которое срабатывает правило.	Для указания имени директории вы можете использовать маски.
`IncludeHashes.item_#`	Хеш SHA256 исполняемого файла, на который срабатывает правило.	Допускается использование только SHA256.

Параметр	Описание	Значения
`UseExcludes`	Использование исключающих условий для срабатывания правила.	`Yes` – не применять правило к приложению, если приложение соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию. `No` (значение по умолчанию) – применять правило к приложению, даже если приложение соответствует исключающему условию.
`ExcludeFileNames.item_#`	Имя исполняемого файла, на которое срабатывает правило.	Для указания имени файла вы можете использовать маски.
`ExcludeFolders.item_#`	Имя директории с исполняемым файлом приложения, на которое срабатывает правило.	Для указания имени директории вы можете использовать маски.
`ExcludeHashes.item_#`	Хеш SHA256 исполняемого файла, на который срабатывает правило.	Допускается использование только SHA256.
Секция **[AllowListRules.item_#]** содержит список правил контроля приложений для режима работы *Список разрешенных* (*AllowList*). Каждая секция [AllowListRules.item_#] содержит следующие параметры:		
`Description`	Описание правила контроля приложений.	
`AppControlRuleStatus`	Статус работы правила контроля приложений.	`On` (значение по умолчанию) – правило включено, Kaspersky Endpoint Security применяет это правило для контроля приложений. `Off` – правило не используется для контроля приложений. `Test` – Kaspersky Endpoint Security разрешает запуск приложений, на которые распространяется действие правила, но фиксирует информацию о запуске этих приложений в отчете.
`Category`	Название категории приложений, для которой применяется правило. Вы можете указать в качестве категории категорию "Golden Image".	
Секция **[AllowListRules.item_#.ACL.item_#]** содержит список пользователей, которым разрешен или запрещен запуск приложений.		
`Access`	Тип доступа, назначаемый пользователю или группе пользователей.	`Allow` (значение по умолчанию) – разрешать запуск приложений. `Block` – запрещать запуск приложений.
`Principal`	Пользователь или группа пользователей, на которых распространяется правило контроля приложений.	`\Everyone` (значение по умолчанию) – правило применяется для всех пользователей. `< имя пользователя >` – имя пользователя, для которого применяется правило. `@< название группы >` – название группы пользователей, для которых применяется правило.
Секция **[DenyListRules.item_#]** содержит список правил контроля приложений для режима работы *Список запрещенных* (*DenyList*). Каждая секция [DenyListRules.item_#] содержит следующие параметры:		
`Description`	Описание правила контроля приложений.	
`AppControlRuleStatus`	Статус работы правила контроля приложений.	`On` (значение по умолчанию) – правило включено, Kaspersky Endpoint Security применяет это правило для контроля приложений. `Off` – правило не используется для контроля приложений. `Test` – Kaspersky Endpoint Security разрешает запуск приложений, на которые распространяется действие правила, но фиксирует информацию о запуске этих приложений в отчете.
`Category`	Название созданной категории приложений, для которой применяется правило. Вы можете указать в качестве категории список приложений "Golden Image".	
Секция **[DenyListRules.item_#.ACL.item_#]** содержит список пользователей, которым разрешен или запрещен запуск приложений.		

Параметр	Описание	Значения
`Access`	Тип доступа, назначаемый пользователю или группе пользователей.	`Allow` – разрешать запуск приложений. `Block` (значение по умолчанию) – запрещать запуск приложений.
`Principal`	Пользователь или группа пользователей, на которых распространяется правило контроля приложений.	`\Everyone` (значение по умолчанию) – правило применяется для всех пользователей. `< имя пользователя >` – имя пользователя, для которого применяется правило. `@< название группы >` – название группы пользователей, для которых применяется правило.

Полезные статьи

Как задавать маски

Вы можете использовать символ * (любая последовательность символов) или символ ? (один любой символ) для формирования маски имени файла или директории.

Вы можете указать символ * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/*/file*/` или `/dir/file*/`.

Вы можете указать символ ? вместо любого одного символа (включая символ `/`) в имени файла или директории.

Создание и изменение списка категорий

Вы можете создать новую категорию двумя способами:

- с помощью команды kesl --set-settings и конфигурационного файла параметров задачи Контроль приложений (`Application_Control`);
- с помощью команды kesl --set-categories и конфигурационного файла параметров категории.

Чтобы создать категории приложений, выполните следующую команду:

```
kesl-control --set-categories --file <path to the configuration file>
```

где:

`--file <path to the configuration file>` – путь к конфигурационному файлу с параметрами категорий.

Файл с параметрами категорий должен иметь такую структуру:

```
[
   {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
```

```
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "Name" : "<category name 2>"
   }
]
```

Для указания имени файла в полях `Exclude` и `Include` вы можете использовать маски.

Параметр `Name` обязательный, если вы не укажете название категории, она не будет создана или будет удалена. Параметр `GUID` также обязательный, если вы его не укажете, отобразится сообщение об ошибке и категория не будет создана. Параметр `GUID` требуется указывать без дефисов.

Чтобы изменить список созданных категорий приложений, выполните следующую команду:

```
kesl-control --set-categories [--names <category name 1> <category name 2> ... <category name N>] --file <path to the configuration file>
```

где:

- `<category name 1> <category name 2> ... <category name N>` – названия категорий, информацию о которых вы хотите изменить. Если вы хотите изменить информацию о нескольких категориях, укажите названия категорий через пробел. Если вы не укажете название категории, существующие категории будут удалены и будут созданы новые категории из указанного файла.
- `--file <path to the configuration file>` – путь к конфигурационному файлу с параметрами категорий.

Полезные статьи

Как задавать маски

Вы можете использовать символ * (любая последовательность символов) или символ ? (один любой символ) для формирования маски имени файла или директории.

Вы можете указать символ * вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ /. Например, `/dir/*/file*/` или `/dir/file*/`.

Вы можете указать символ ? вместо любого одного символа (включая символ `/`) в имени файла или директории.

Просмотр списка категорий

В командной строке вы можете просматривать список созданных категорий приложений с помощью команды управления контролем приложений `kesl-control --get-categories`.

Список созданных категорий содержит следующие категории:

- категории, созданные в Kaspersky Security Center;
- категории, добавленные в параметрах задачи Контроль приложений через командную строку;
- категория "GoldenImage", созданная с помощью задачи Инвентаризация (в Kaspersky Security Center или через командную строку).

Чтобы просмотреть список всех созданных категорий приложений, выполните следующую команду:

```
kesl-control --get-categories [--file <path to the configuration file>] [--json]
```

где:

- `--file <path to the configuration file>` – полный путь к конфигурационному файлу, в который будут выведены параметры.
- `--json` – выводить параметры в формате JSON.

Kaspersky Endpoint Security отобразит следующую информацию о каждой категории приложений:

- уникальный идентификатор (GUID) категории;
- название категории;
- список включающих условий для срабатывания правила;
- список исключающих условий для срабатывания правила.

Чтобы просмотреть список отдельных категорий приложений, выполните следующую команду:

```
kesl-control --get-categories [--names <category name 1> <category name 2> ... <category name N>] [--file <path to
the configuration file>] [--json]
```

где:

- `<category name 1> <category name 2> ... <category name N>` – названия категорий, информацию о которых вы хотите просмотреть. Если вы хотите просмотреть информацию о нескольких категориях, укажите названия категорий через пробел.
- `--file <path to the configuration file>` – полный путь к конфигурационному файлу формата JSON, в который будут выведен список категорий.
- `--json` – выводить параметры в формате JSON.

Если в параметрах задачи Контроль приложений в секции `[Categories.item_#]` для включающих или исключающих условий срабатывания правила вы указали символические ссылки на файл приложения или на директорию с исполняемыми файлами, то при просмотре списка категорий для этих условий будет отображаться исходный путь, на который ссылается символическая ссылка.

Настройка списка правил контроля приложений

Чтобы просмотреть список правил контроля приложений, выполните следующую команду:

```
kesl-control --get-settings 21 [--file <path to the configuration file>] [--json]
```

где:

- `--file <path to the configuration file>` – полный путь к конфигурационному файлу, в который будут выведены параметры.
- `--json` – выводить данные в формате JSON.

Kaspersky Endpoint Security отобразит следующую информацию о правилах контроля приложений:

- режим работы компонента Контроль приложений;
- действие, которое Контроль приложений будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенному правилу;
- описание правила контроля приложений (если есть);
- статус работы правила контроля приложений;
- название категории приложений, для которой применяется правило;
- тип доступа, назначенный пользователю или группе пользователей;
- пользователь или группа пользователей, на которых распространяется правило контроля приложений.

Чтобы изменить список категорий приложений и правил контроля приложений, выполните следующую команду:

```
kesl-control --set-settings 21 [--file <path to the configuration file>] [--json]
```

где:

- `--file <path to the configuration file>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры.
- `--json` – импорт данных из файла в формате JSON.

Чтобы удалить список категорий приложений и правил контроля приложений, выполните следующую команду:

```
kesl-control --set-settings 21 --set-to-default
```

Настройка инвентаризации

В командной строке вы можете выполнять инвентаризацию приложений защищаемого устройства следующими способами:

- С помощью предустановленной задачи Инвентаризация (`Inventory_Scan`). Вы можете запускать и останавливать эту задачу вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры проверки, изменяя параметры этой задачи.

- С помощью пользовательских задач инвентаризации (задач типа `InventoryScan`). Вы можете запускать, останавливать, приостанавливать и возобновлять пользовательские задачи вручную и настраивать расписание запуска задач.

Вы можете просматривать список приложений, обнаруженных на устройстве в результате выполнения задачи Инвентаризация, с помощью команд управления контролем приложений.

Задача Инвентаризация

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Инвентаризация (`Inventory_Scan`).

Параметры задачи Инвентаризация

Параметр	Описание	Значения
`ScanScripts`	Включение проверки скриптов.	`Yes` (значение по умолчанию) – проверять скрипты. `No` – не проверять скрипты.
`ScanBinaries`	Включение проверки бинарных файлов (elf, java и pyc).	`Yes` (значение по умолчанию) – проверять бинарные файлы. `No` – не проверять бинарные файлы.
`ScanAllExecutable`	Включение проверки файлов с исполняемым битом.	`Yes` (значение по умолчанию) – проверять файлы с исполняемым битом. `No` – не проверять файлы с исполняемым битом.
`GoldenImageAction`	Действие, которое приложение Kaspersky Endpoint Security выполняет с категорией приложений "Золотой образ" (Golden Image) по завершении задачи Инвентаризация: Вы можете использовать категорию приложений "Золотой образ" в правилах контроля приложений.	`DoNothing` (значение по умолчанию) – не изменять категорию приложений "Золотой образ" (Golden Image) после выполнения инвентаризации. `Create` – добавлять обнаруженные приложения в категорию приложений "Золотой образ" (Golden Image). Если категория отсутствует, она будет создана. Если категория существует, список приложений в ней будет обновлен. `Remove` – очистить категорию приложений "Золотой образ" (Golden Image). Приложение очищает категорию сразу после запуска задачи без инвентаризации файлов на устройстве.
Секция **[ScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области инвентаризации. Максимальная длина строки, задаваемой этим параметром: 4096 символов.	Значение по умолчанию: `All objects`.
`UseScanArea`	Включение проверки указанной области инвентаризации. Для выполнения задачи требуется включить проверку хотя бы одной области инвентаризации.	`Yes` (значение по умолчанию) – проверять указанную область инвентаризации. `No` – не проверять указанную область инвентаризации.

Параметр	Описание	Значения
`AreaMask.item_#`	Ограничение области инвентаризации. В области инвентаризации приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области инвентаризации. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (проверять все объекты).
`Path`	Путь к директории с проверяемыми объектами.	`< путь к локальной директории >` – проверять объекты в указанной директории. Значение по умолчанию: `/usr/bin`
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры.		
`AreaDesc`	Описание области исключения из инвентаризации.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из инвентаризации.	`Yes` (значение по умолчанию) – исключать указанную область. `No` – не исключать указанную область.
`AreaMask.item_#`	Ограничение области исключения из инвентаризации по маскам в формате shell. Если параметр не указан, приложение исключает все объекты в области инвентаризации. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать все объекты).
`Path`	Путь к директории с исключаемыми объектами.	`< путь к локальной директории >` – исключать из проверки объекты в указанной директории. Для указания пути вы можете использовать маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Просмотр списка обнаруженных приложений

Чтобы просмотреть список приложений, обнаруженных на устройстве, выполните следующую команду:

```
kesl-control --get-app-list [--json]
```

где `--json` – выводить данные в формате JSON.

Kaspersky Endpoint Security отобразит следующую информацию об обнаруженных приложениях:

- **Дата и время инвентаризации**. Дата и время выполнения задачи Инвентаризация.
- **Количество приложений**. Количество приложений, обнаруженных на устройстве.
- Список приложений, содержащий следующую информацию:
  - **Путь**. Путь к приложению.
  - **Хеш**. Хеш-сумма приложения.
  - **Тип**. Тип приложения. Например: `Script`, `Executable`.
  - **Категории**. Категории, к которым принадлежит приложение (если они были созданы ранее). Вы можете просмотреть список созданных категорий приложений с помощью следующей команды:

    ```
    kesl-control --get-categories
    ```

При добавлении новой категории информация о ней в списке приложений автоматически не обновляется. Для обновления списка приложений требуется повторный запуск задачи Инвентаризация.

Задача Контроль целостности системы

В командной строке вы можете управлять контролем целостности системы в реальном времени с помощью предустановленной задачи Контроль целостности системы (`System_Integrity_Monitoring`). Тип задачи – `OAFIM`.

Задача Контроль целостности системы по умолчанию не запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры контроля целостности системы на устройстве, изменяя параметры предустановленной задачи Контроль целостности системы.

Параметры задачи Контроль целостности системы при доступе

Параметр	Описание	Значения
`UseExcludeMasks`	Включение исключения из области мониторинга объектов, указанными параметром `ExcludeThreats.item_#`. Этот параметр работает, только если указано значение параметра `ExcludeMasks.item_#`.	`Yes` – исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области мониторинга. `No` (значение по умолчанию) – не исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области мониторинга.
`ExcludeMasks.item_#`	Исключение из мониторинга объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`. Вы можете указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом.	Значение по умолчанию не задано.

Параметр	Описание	Значения
Секция [ScanScope.item_#] содержит области мониторинга для задачи Контроль целостности системы. Для задачи должна быть указана минимум одна область мониторинга. Вы можете указать несколько секций [ScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области мониторинга, содержит дополнительную информацию об области мониторинга.	Значение по умолчанию не задано.
`UseScanArea`	Включение мониторинга указанной области.	`Yes` (значение по умолчанию) – контролировать указанную область. `No` – не контролировать указанную область.
`Path`	Путь к директории для мониторинга.	Для указания пути вы можете использовать маски. Значение по умолчанию: /opt/kaspersky/kesl/
`AreaMask.item_#`	Ограничение области мониторинга. В области мониторинга приложение проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (контролировать все объекты).
Секция **[ExcludedFromScanScope.item_#]** содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#].Вы можете указать несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области исключения из мониторинга, содержит дополнительную информацию об области исключения из мониторинга.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из мониторинга.	`Yes` (значение по умолчанию) – исключать указанную область из мониторинга. `No` – не исключать указанную область из мониторинга.
`Path`	Путь к директории с объектами, исключаемыми из мониторинга.	Для указания пути вы можете использовать маски. Значение по умолчанию не задано.
`AreaMask.item_#`	Ограничение области исключения из мониторинга. В области исключения из мониторинга приложение исключает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (исключать из мониторинга все объекты).

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Задача Проверка целостности системы

В командной строке вы можете выполнять проверку целостности системы на устройстве с помощью пользовательских задач Проверка целостности системы (`System_Integrity_Monitoring`). Тип задачи – `ODFIM`.

Вы можете запускать, останавливать, приостанавливать и возобновлять пользовательские задачи вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры проверки целостности системы, изменяя параметры этих задач.

Параметры задачи Проверка целостности системы

Параметр	Описание	Значения
`RebuildBaseline`	Включение обновления снимка состояния системы после завершения задачи *Проверка целостности системы*.	`Yes` – обновлять снимок состояния системы каждый раз после завершения задачи *Проверка целостности системы*. `No` (значение по умолчанию) – не обновлять снимок состояния системы каждый раз после завершения задачи *Проверка целостности системы*.
`CheckFileHash`	Использовать хеш файла (SHA256) в качестве критерия, по которому выполняется сравнение текущего состояния контролируемого файла с исходным состоянием.	`Yes` – проверять хеш. `No` (значение по умолчанию) – выключить проверку хеша. Если проверка выключена, приложение сравнивает только размер файла (если размер файла не изменился, время изменения не считается критическим параметром).
`TrackDirectoryChanges`	Включение мониторинга директорий.	`Yes` – контролировать директории во время выполнения проверки целостности системы. `No` (значение по умолчанию) – не контролировать директории.
`TrackLastAccessTime`	Включение проверки времени последнего доступа к файлу. В операционных системах Linux это параметр `noatime`.	`Yes` – проверять время последнего доступа к файлу. `No` (значение по умолчанию) – не проверять время последнего доступа к файлу.
`UseExcludeMasks`	Включение исключения из области мониторинга объектов, указанными параметром `ExcludeMasks.item_#`. Этот параметр работает, только если указано значение параметра `ExcludeMasks.item_#`.	`Yes` – исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области мониторинга. `No` (значение по умолчанию) – не исключать объекты, указанные параметром `ExcludeMasks.item_#`, из области мониторинга.
`ExcludeMasks.item_#`	Исключение из мониторинга объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell. Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`. Вы можете указать несколько масок, каждая маска должна быть указана в новой строке с новым индексом.	Значение по умолчанию не задано.
Секция [ScanScope.item_#] содержит области мониторинга для задачи *Проверка целостности системы*. Для задачи должна быть указана минимум одна область мониторинга. Вы можете указать несколько секций [ScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области мониторинга, содержит дополнительную информацию об области мониторинга.	Значение по умолчанию не задано.

Параметр	Описание	Значения
`UseScanArea`	Включение мониторинга указанной области.	`Yes` (значение по умолчанию) – контролировать указанную область. `No` – не контролировать указанную область.
`Path`	Путь к директории для мониторинга.	Для указания пути вы можете использовать маски. Значение по умолчанию: /opt/kaspersky/kesl/
`AreaMask.item_#`	Ограничение области мониторинга. В области мониторинга приложение проверяет только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (контролировать все объекты).
Секция **[ExcludedFromScanScope.item_#]** содержит объекты, которые требуется исключить из всех секций [ScanScope.item_#]. Вы можете указать несколько секций [ExcludedFromScanScope.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Секция [ExcludedFromScanScope.item_#] содержит следующие параметры:		
`AreaDesc`	Описание области исключения из мониторинга, содержит дополнительную информацию об области исключения из мониторинга.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из мониторинга.	`Yes` (значение по умолчанию) – исключать указанную область из мониторинга. `No` – не исключать указанную область из мониторинга.
`Path`	Путь к директории с объектами, исключаемыми из мониторинга.	Для указания пути вы можете использовать маски. Значение по умолчанию не задано.
`AreaMask.item_#`	Ограничение области исключения из мониторинга. В области исключения из мониторинга приложение исключает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (исключать из мониторинга все объекты).

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Защита от сложных угроз и целевых атак

Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)

В командной строке вы можете управлять интеграцией приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (on-premises) на платформе OSMP с помощью предустановленной задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* (`KATAEDR`).

> Задача также позволяет настраивать параметры интеграции с компонентом Kaspersky Endpoint Detection and Response (KATA). Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) в параметрах задачи вам нужно выбрать режим интеграции *EDR Expert (on-premises)* и настроить нужные параметры интеграции.

Вы можете настраивать параметры интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises), изменяя параметры предустановленной задачи.

По умолчанию задача *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* не запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете управлять сертификатами, которые используются для подключения к серверам OSMP, с помощью команд управления компонентом EDR Expert (on-premises).

Параметры интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises)

В таблице ниже описаны параметры предустановленной задачи Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises) (`KATAEDR`), которые вы можете настраивать при интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises).

> Задача также позволяет настраивать параметры интеграции с компонентом Kaspersky Endpoint Detection and Response (KATA). Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) в параметрах задачи вам нужно выбрать режим интеграции *EDR Expert (on-premises)* (параметр `Mode=EDRExpertOnPrem`).

Параметры интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises)

Параметр	Описание	Значение
`Mode`	Режим интеграции. Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) приложение Kaspersky Endpoint Security взаимодействует с серверами на платформе OSMP. Для интеграции с Kaspersky Endpoint Detection and Response (KATA) приложение Kaspersky Endpoint Security взаимодействует с серверами на платформе Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (значение по умолчанию) – режим интеграции EDR (KATA). Позволяет включить интеграцию с Kaspersky Endpoint Detection and Response (KATA), компонентом Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` – режим интеграции EDR Expert (on-premises). Позволяет включить интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premises).
`UseClientPinnedCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу действий по реагированию OSMP. Если двусторонняя аутентификация включена на стороне сервера действий по реагированию OSMP, вам нужно включить двустороннюю аутентификацию в параметрах задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* и добавить сертификат клиента перед запуском задачи.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу действий по реагированию OSMP. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`SynchronizationPeriod`	Периодичность отправки запросов на синхронизацию на сервер действий по реагированию OSMP в минутах.	Значение по умолчанию: `5`.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером действий по реагированию OSMP в секундах.	Значение по умолчанию: `10`.
`RequestTimeout`	Максимальное время ожидания ответа от сервера действий по реагированию OSMP в секундах.	Значение по умолчанию: `10`.
`EnableTelemetry`	Отправка данных о событиях на устройствах (телеметрии) на сервер сбора телеметрии OSMP.	`Yes` (значение по умолчанию) – отправлять телеметрию на сервер сбора телеметрии OSMP. `No` – не отправлять телеметрию.
Секция **[Endpoints.item_#]** содержит адрес и порт сервера действий по реагированию OSMP. Вы можете добавить несколько серверов.		
`Address`	Адрес сервера действий по реагированию OSMP. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера.	Значение по умолчанию: `127.0.0.1`.
`Port`	Порт для подключения к серверу действий по реагированию OSMP.	Значение по умолчанию: `443`.
Секция **[TelemetrySettings]** содержит общие параметры подключения к серверам сбора телеметрии OSMP.		
`UseClientPinnedCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу сбора телеметрии OSMP. Если двусторонняя аутентификация включена на стороне сервера сбора телеметрии OSMP, вам нужно включить двустороннюю аутентификацию в параметрах задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert* и добавить сертификат клиента перед*(on-premises)* запуском задачи.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу сбора телеметрии OSMP. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером сбора телеметрии OSMP в секундах.	Значение по умолчанию: `10`.
`RequestTimeout`	Максимальное время ожидания ответа от сервера сбора телеметрии OSMP в секундах.	Значение по умолчанию: `10`.

Параметр	Описание	Значение
`OnlyTaggedEvents`	Отправка телеметрии только с IOA. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию *потоковой проверки*, которая позволяет отслеживать такие события в режиме реального времени.	`Yes` – отправлять только телеметрию с индикатором атаки (Indicator of Attack, IOA). `No` (значение по умолчанию) – отправлять всю телеметрию.
Секция **[TelemetrySettings.Endpoints.item_#]** содержит адрес и порт сервера сбора телеметрии OSMP. Вы можете добавить несколько серверов.		
`Address`	Адрес сервера сбора телеметрии OSMP. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера.	Значение по умолчанию: `127.0.0.1`.
`Port`	Порт для подключения к серверу сбора телеметрии OSMP.	Значение по умолчанию: `443`.
Секция **[TelemetrySettings.EventTransferSettings]** содержит параметры передачи данных на сервер сбора телеметрии OSMP.		
`MaximumDataTransferTime`	Максимальная задержка отправки событий на сервер сбора телеметрии OSMP в секундах.	Значение по умолчанию: `30`.
`UseRequestCountLimits`	Регулирование количества запросов. Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события.	`Yes` (значение по умолчанию) – регулировать количество отправляемых событий. `No` – не регулировать количество событий.
`MaximumNumberOfEventsInHour`	Максимальное количество событий в час.	Значение по умолчанию: `3000`.
`MaximumNumberOfEventsInPackage`	Максимальное количество событий в одном пакете.	Значение по умолчанию: `1024`.
`EventLimitExceededPercentage`	Процент превышения ограничения на количество событий. Передача событий ограничивается, если соотношение событий одного типа к общему количеству событий превышает установленное ограничение в процентах.	Значение по умолчанию: `15`.

Управление сертификатами для подключения к серверам OSMP EDR Expert (on-premises)

Для управления сертификатами требуются права пользователя с ролью Администратор (admin).

Вы можете управлять сертификатами, которые используются для подключения к серверам OSMP, с помощью команд. Вы можете выполнять следующие действия с сертификатами:

- добавлять или заменять сертификаты серверов OSMP: сервера действий по реагированию и сервера сбора телеметрии;
- выводить информацию о сертификатах серверов;
- удалять сертификаты серверов;
- добавлять или заменять сертификаты клиента, используемые для защиты подключения к серверам OSMP: серверу действий по реагированию и серверу сбора телеметрии;

- выводить информацию о сертификатах клиента;
- удалять сертификаты клиента.

Управление сертификатами для подключения к серверу действий по реагированию OSMP

Чтобы добавить или заменить сертификат сервера действий по реагированию, выполните следующую команду:

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
```

где `<file>` – путь к файлу, содержащему сертификат сервера.

Чтобы добавить или заменить сертификат клиента, используемый для защиты подключения к серверу действий по реагированию:

1. Выполните следующую команду:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
   ```

   где `<file>` – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

2. Введите пароль от криптоконтейнера.

> Сертификат клиента используется для дополнительной защиты соединения с сервером OSMP, если в параметрах сервера OSMP включена проверка сертификата клиента и в параметрах задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* для параметра `UseClientPinnedCertificate` в секции `[KATAEDR]` установлено значение `yes`.

Чтобы вывести информацию о сертификате сервера действий по реагированию, выполните следующую команду:

```
kesl-control [-R] --query-kataedr-server-certificate --server-type response
```

Чтобы вывести информацию о сертификате клиента, используемого для защиты подключения к серверу действий по реагированию, выполните следующую команду:

```
kesl-control [-R] --query-kataedr-client-certificate --server-type response
```

В результате выполнения команды выводится следующая информация о сертификате:

- серийный номер сертификата;
- субъект сертификата;
- издатель сертификата;
- дата начала срока действия сертификата;

- дата окончания срока действия сертификата;
- SHA1 и SHA256 отпечатки сертификата.

Чтобы удалить сертификат сервера действий по реагированию, выполните следующую команду:

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type response
```

Чтобы удалить сертификат клиента, используемый для защиты подключения к серверу действий по реагированию, выполните следующую команду:

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type response
```

Управление сертификатами для подключения к серверу сбора телеметрии OSMP

Чтобы добавить или заменить сертификат сервера сбора телеметрии, выполните следующую команду:

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

где `<file>` – путь к файлу, содержащему сертификат сервера.

Чтобы добавить или заменить сертификат клиента, используемый для защиты подключения к серверу сбора телеметрии:

1. Выполните следующую команду:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
   ```

   где `<file>` – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

2. Если криптоконтейнер защищен паролем, введите пароль по запросу.

Сертификат клиента используется для дополнительной защиты соединения с сервером OSMP, если в параметрах сервера OSMP включена проверка сертификата клиента и в параметрах задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* для параметра `UseClientPinnedCertificate` в секции `[TelemetrySettings]` установлено значение `yes`.

Чтобы вывести информацию о сертификате сервера сбора телеметрии, выполните следующую команду:

```
kesl-control [-R] --query-kataedr-server-certificate --server-type telemetry
```

Чтобы вывести информацию о сертификате клиента, используемого для защиты подключения к серверу сбора телеметрии, выполните следующую команду:

```
kesl-control [-R] --query-kataedr-client-certificate --server-type telemetry
```

В результате выполнения команды выводится следующая информация о сертификате:

- серийный номер сертификата;
- субъект сертификата;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- SHA1 и SHA256 отпечатки сертификата.

Чтобы удалить сертификат сервера сбора телеметрии, выполните следующую команду:

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type telemetry
```

Чтобы удалить сертификат клиента, используемый для защиты подключения к серверу сбора телеметрии, выполните следующую команду:

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type telemetry
```

Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud)

В командной строке вы можете управлять интеграцией приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (cloud) на платформе OSMP с помощью предустановленной задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud)*.

Вы можете настраивать параметры интеграции с Kaspersky Endpoint Detection and Response Expert (cloud), изменяя параметры предустановленной задачи.

По умолчанию задача *Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud)* не запущена. Вы можете запускать и останавливать задачу вручную.

Параметры интеграции с Kaspersky Endpoint Detection and Response Expert (cloud)

В таблице ниже описаны параметры предустановленной задачи Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud) (`EDRExpertCloud`).

Как получить текущие значения параметров задачи

```
kesl-control --get-settings 39
```

Как настроить параметры задачи

```
kesl-control --set-settings 39 <parameter>=<value>
```

Параметр	Описание
Параметры интеграции с сервером реагирования	
`UseTunnel`	Использование TCP-туннеля для подключения к серверу реагирования. TCP-туннель нужен для подключения к серверам, если политика безопасности в вашей инфраструктуре не позволяет подключаться к серверам напрямую. По умолчанию использование TCP-туннеля выключено (`No`).
`TunnelAddress`	Адрес сервера (IPv4, IPv6) для подключения к туннелю.
`TunnelPort`	Порт сервера для подключения к туннелю.
`SynchronizationPeriod`	Периодичность отправки запросов на синхронизацию на сервер действий по реагированию OSMP в минутах. Значение по умолчанию: `5`.
Параметры интеграции с сервером сбора телеметрии Секция `[TelemetrySettings]` содержит общие параметры подключения к серверам сбора телеметрии OSMP.	
`EnableTelemetry`	Отправка данных о событиях на устройствах (телеметрии) на сервер сбора телеметрии OSMP. По умолчанию отправка телеметрии включена (`Yes`).
`OnlyTaggedEvents`	Отправка телеметрии только с IOA. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию *потоковой проверки*, которая позволяет отслеживать такие события в режиме реального времени. По умолчанию отправка телеметрии только с IOA выключена (`No`).
`UseTunnel`	Использование TCP-туннеля для подключения к серверу сбора телеметрии. TCP-туннель нужен для подключения к серверам, если политика безопасности в вашей инфраструктуре не позволяет подключаться к серверам напрямую. По умолчанию использование TCP-туннеля выключено (`No`).
`TunnelAddress`	Адрес сервера (IPv4, IPv6) для подключения к туннелю.
`TunnelPort`	Порт сервера для подключения к туннелю.
Секция `[TelemetrySettings.EventTransferSettings]` содержит общие параметры подключения к серверам сбора телеметрии OSMP.	
`UseRequestCountLimits`	Регулирование количества запросов. Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события. По умолчанию функция включена.
`MaximumDataTransferTime`	Максимальная задержка отправки событий в секундах. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд.
`MaximumNumberOfEventsInHour`	Максимальное количество событий в час. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.
`MaximumNumberOfEventsInPackage`	Максимальное количество пакетов событий. Приложение выполняет синхронизацию с сервером при заполнении буфера событиями. По умолчанию установлено значение 1024 события.
`EventLimitExceededPercentage`	Процент превышения лимита событий. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Endpoint Security восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.

Управление сертификатами для подключения к серверам OSMP EDR Expert (cloud)

Для управления сертификатами требуются права пользователя с ролью Администратор (admin).

Приложение получает адреса серверов и сертификаты для установки доверенного соединения автоматически после принятия условий Соглашения об обработке данных Kaspersky Endpoint Detection and Response Expert (cloud). Поэтому добавлять или удалять сертификаты с помощью команд невозможно. В командной строке вы можете только выводить информацию о сертификатах.

Управление сертификатами для подключения к серверу действий по реагированию OSMP

Вывод информации о сертификате сервера действий по реагированию

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type response
```

Вывод информации о сертификате клиента, используемого для защиты подключения к серверу действий по реагированию

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type response
```

В результате выполнения команды выводится следующая информация о сертификате:

- серийный номер сертификата;
- субъект сертификата;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- SHA1 и SHA256 отпечатки сертификата.

Управление сертификатами для подключения к серверу сбора телеметрии OSMP

Вывод информации о сертификате сервера сбора телеметрии

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type telemetry
```

Вывод информации о сертификате клиента, используемого для защиты подключения к серверу сбора телеметрии

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type telemetry
```

В результате выполнения команды выводится следующая информация о сертификате:

- серийный номер сертификата;
- субъект сертификата;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- SHA1 и SHA256 отпечатки сертификата.

Интеграция с Kaspersky Endpoint Detection and Response (KATA)

В командной строке вы можете управлять интеграцией приложения Kaspersky Endpoint Security с компонентом Kaspersky Endpoint Detection and Response (KATA) с помощью предустановленной задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* (`KATAEDR`).

> Задача также позволяет настраивать параметры интеграции с решением Kaspersky Endpoint Detection and Response Expert (on-premises). Для интеграции с Kaspersky Endpoint Detection and Response (KATA) в параметрах задачи вам нужно выбрать режим интеграции EDR (KATA) и настроить нужные параметры интеграции.

Вы можете настраивать параметры интеграции с Kaspersky Endpoint Detection and Response (KATA), изменяя параметры предустановленной задачи.

По умолчанию задача *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* не запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете управлять сертификатами, которые используются для подключения к серверам KATA, с помощью команд управления компонентом EDR Expert (on-premises).

Параметры интеграции с Kaspersky Endpoint Detection and Response (KATA)

В таблице ниже описаны параметры предустановленной задачи Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises) (`KATAEDR`), которые вы можете настраивать при интеграции с Kaspersky Endpoint Detection and Response (KATA).

> Задача также позволяет настраивать параметры интеграции с решением Kaspersky Endpoint Detection and Response Expert (on-premises). Для интеграции с компонентом Kaspersky Endpoint Detection and Response (KATA) в параметрах задачи вам нужно выбрать режим интеграции *EDR (KATA)* (параметр `Mode=EDRKATA`).

Параметры интеграции с Kaspersky Endpoint Detection and Response (KATA)

Параметр	Описание	Значение
`Mode`	Режим интеграции. Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) приложение Kaspersky Endpoint Security взаимодействует с серверами на платформе OSMP. Для интеграции с Kaspersky Endpoint Detection and Response (KATA) приложение Kaspersky Endpoint Security взаимодействует с серверами на платформе Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (значение по умолчанию) – режим интеграции EDR (KATA). Позволяет включить интеграцию с Kaspersky Endpoint Detection and Response (KATA), компонентом Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` – режим интеграции EDR Expert (on-premises). Позволяет включить интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premises).
`UseClientPinnedCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу KATA. Если двусторонняя аутентификация включена на стороне сервера KATA, вам нужно включить двустороннюю аутентификацию в параметрах задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* и добавить сертификат клиента перед запуском задачи.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу KATA. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.

Параметр	Описание	Значение
`SynchronizationPeriod`	Периодичность отправки запросов на синхронизацию на сервер KATA в минутах.	Значение по умолчанию: `5`.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером KATA в секундах.	Значение по умолчанию: `10`.
`RequestTimeout`	Максимальное время ожидания ответа от сервера KATA в секундах.	Значение по умолчанию: `10`.
`EnableTelemetry`	Отправки данных о событиях на устройствах (телеметрии) на KATA.	`Yes` (значение по умолчанию) – отправлять телеметрию на сервер KATA. `No` – не отправлять телеметрию.
Секция **[Endpoints.item_#]** содержит адрес и порт сервера KATA. Вы можете добавить несколько серверов.		
`Address`	Адрес сервера KATA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера.	Значение по умолчанию: `127.0.0.1`.
`Port`	Порт для подключения к серверу KATA.	Значение по умолчанию: `443`.
Секция **[EventTransferSettings]** содержит параметры передачи данных на сервер KATA.		
`MaximumDataTransferTime`	Максимальная задержка отправки событий на сервер KATA в секундах.	Значение по умолчанию: `30`.
`UseRequestCountLimits`	Включение и выключение регулирования количества событий, отправляемых на сервер KATA.	`Yes` (значение по умолчанию) – регулировать количество отправляемых событий. `No` – не регулировать количество событий.
`MaximumNumberOfEventsInHour`	Максимальное количество событий в час.	Значение по умолчанию: `3000`.
`MaximumNumberOfEventsInPackage`	Максимальное количество событий в одном пакете.	Значение по умолчанию: `1024`.
`EventLimitExceededPercentage`	Процент превышения ограничения на количество событий. Передача событий ограничивается, если соотношение событий одного типа к общему количеству событий превышает установленное ограничение в процентах.	Значение по умолчанию: `15`.

Управление сертификатами для подключения к серверу KATA

Для управления сертификатами требуются права пользователя с ролью Администратор (admin).

Вы можете управлять сертификатами, которые используются для подключения к серверу KATA, с помощью команд. Вы можете выполнять следующие действия с сертификатами:

- добавлять или заменять сертификат сервера KATA;
- выводить информацию о сертификате сервера;
- удалять сертификат сервера;
- добавлять или заменять сертификат клиента, используемый для защиты подключения к серверу KATA;
- выводить информацию о сертификате клиента;
- удалять сертификат клиента.

Чтобы добавить или заменить сертификат сервера, выполните следующую команду:

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

где `<file>` – путь к файлу, содержащему сертификат сервера.

Чтобы добавить или заменить сертификат клиента:

1. Выполните следующую команду:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file>
   ```

   где `<file>` – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

2. Введите пароль от криптоконтейнера.

Сертификат клиента используется для дополнительной защиты соединения с сервером KATA, если в параметрах сервера KATA включена проверка сертификата клиента и в параметрах задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises)* для параметра `UseClientPinnedCertificate` установлено значение `yes`.

Чтобы вывести информацию о сертификате сервера, выполните следующую команду:

```
kesl-control [-R] --query-kataedr-server-certificate
```

Чтобы вывести информацию о сертификате клиента, выполните следующую команду:

```
kesl-control [-R] --query-kataedr-client-certificate
```

В результате выполнения команды выводится следующая информация о сертификате:

- серийный номер сертификата;
- субъект сертификата;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- SHA1 и SHA256 отпечатки сертификата.

Чтобы удалить сертификат сервера, выполните следующую команду:

```
kesl-control [-R] --remove-kataedr-server-certificate
```

Чтобы удалить сертификат клиента, выполните следующую команду:

```
kesl-control [-R] --remove-kataedr-client-certificate
```

Интеграция с Kaspersky Network Detection and Response (KATA)

В командной строке вы можете управлять интеграцией приложения Kaspersky Endpoint Security с компонентом Kaspersky Network Detection and Response (KATA) с помощью предустановленной задачи *Интеграция с Kaspersky Network Detection and Response (KATA)* (`KATANDR`):

По умолчанию задача *Интеграция с Kaspersky Network Detection and Response (KATA)* не запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры интеграции с Kaspersky Network Detection and Response (KATA), изменяя параметры предустановленной задачи.

Вы можете управлять сертификатами, которые используются для подключения к серверам NDR, с помощью команд управления компонентом NDR (KATA).

Параметры интеграции с Kaspersky Network Detection and Response (KATA)

В таблице ниже описаны все доступные параметры и значения по умолчанию для всех параметров, которые вы можете указать для задачи Интеграция с Kaspersky Network Detection and Response (KATA) (`KATANDR`).

Параметры задачи Интеграция с Kaspersky Network Detection and Response (KATA)

Параметр	Описание	Значение
`UseClientPinnedCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу NDR. Если проверка сертификата клиента включена на стороне сервера NDR, вам нужно включить использование сертификата клиента и добавить сертификат клиента перед запуском задачи *Интеграция с Kaspersky Network Detection and Response (KATA)*.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу NDR. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`SynchronizationPeriod`	Периодичность отправки запросов на синхронизацию на сервер NDR в минутах.	Значение по умолчанию: `5`.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером NDR в секундах.	Значение по умолчанию: `10`.
`RequestTimeout`	Максимальное время ожидания ответа от сервера NDR в секундах.	Значение по умолчанию: `10`.
Секция **[Endpoints.item_#]** содержит адрес и порт сервера NDR.		
`Address`	Адрес сервера NDR. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера.	Значение по умолчанию: `127.0.0.1`.
`Port`	Порт для подключения к серверу NDR.	Значение по умолчанию: `8081`.
Секция **[EventTransferSettings]** содержит параметры передачи событий на сервер NDR.		
`MaximumDataTransferTime`	Максимальная задержка отправки событий на сервер NDR в секундах.	Значение по умолчанию: `30`.
`MaximumNumberOfEventsInPackage`	Максимальное количество событий в одном пакете.	Значение по умолчанию: `1024`.

Параметр	Описание	Значение
`UseRequestCountLimits`	Включение и выключение регулирования количества событий, отправляемых на сервер NDR.	`Yes` (значение по умолчанию) – регулировать количество отправляемых событий. `No` – не регулировать количество событий.
`MaximumNumberOfEventsInHour`	Максимальное количество событий в час.	Значение по умолчанию: `3000`.
`EventLimitExceededPercentage`	Процент превышения лимита событий. Передача событий ограничивается, если соотношение событий одного типа к общему количеству событий превышает установленное ограничение в процентах.	Значение по умолчанию: `15`.
`PingPeriod`	Периодичность опроса серверов NDR в секундах.	Значение по умолчанию: `450`.

Управление сертификатами для подключения к серверу NDR

Для управления сертификатами требуются права пользователя с ролью Администратор (admin).

Вы можете управлять сертификатами, которые используются для подключения к серверу NDR, с помощью команд. Вы можете выполнять следующие действия с сертификатами:

- добавлять или заменять сертификат сервера NDR;
- выводить информацию о сертификате сервера;
- удалять сертификат сервера;
- добавлять или заменять сертификат клиента, используемый для защиты подключения к серверу NDR;
- выводить информацию о сертификате клиента;
- удалять сертификат клиента.

Чтобы добавить или заменить сертификат сервера, выполните следующую команду:

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

где `<file>` – путь к файлу, содержащему сертификат сервера.

Чтобы добавить или заменить сертификат клиента:

1. Выполните следующую команду:

   ```
   kesl-control [-R] --add-katandr-client-certificate <file>
   ```

   где `<file>` – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

2. Введите пароль от криптоконтейнера.

Сертификат клиента используется для дополнительной защиты соединения с сервером NDR, если в параметрах сервера NDR включена проверка сертификата клиента и в параметрах задачи *Интеграция с Kaspersky Network Detection and Response (KATA)* для параметра `UseClientPinnedCertificate` установлено значение `yes`.

Чтобы вывести информацию о сертификате сервера, выполните следующую команду:

```
kesl-control [-R] --query-katandr-server-certificate
```

Чтобы вывести информацию о сертификате клиента, выполните следующую команду:

```
kesl-control [-R] --query-katandr-client-certificate
```

В результате выполнения команды выводится следующая информация о сертификате:

- серийный номер сертификата;
- субъект сертификата;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- SHA1 и SHA256 отпечатки сертификата.

Чтобы удалить сертификат сервера, выполните следующую команду:

```
kesl-control [-R] --remove-katandr-server-certificate
```

Чтобы удалить сертификат клиента, выполните следующую команду:

```
kesl-control [-R] --remove-katandr-client-certificate
```

Интеграция с Sandbox

В командной строке вы можете управлять интеграцией приложения Kaspersky Endpoint Security с Sandbox с помощью предустановленной задачи *Интеграция с Sandbox*.

По умолчанию задача *Интеграция с Sandbox* не запущена. Вы можете запускать и останавливать эту задачу вручную.

Чтобы запустить задачу Интеграция с Sandbox, выполните следующую команду:

```
kesl-control --start-task 29
```

Запуск задачи *Интеграция с Sandbox* невозможен, если не добавлен сертификат сервера.

Если задача *Интеграция с Sandbox* запущена и выбран режим, который позволяет отправлять файлы на проверку вручную (`Manual` или `AutoAndManual`), вы можете отправлять файлы в Sandbox на проверку в командной строке.

Как отправить файлы в Sandbox на проверку

```
kesl-control [-X] --sandbox <path>
```

где `<path>` – путь к файлу или директории, которые вы хотите проверить. Вы можете указать несколько путей, разделяя их пробелами.

Вы можете настраивать параметры интеграции с Sandbox, изменяя параметры предустановленной задачи.

С помощью команд управления параметрами интеграции с Sandbox вы можете управлять сертификатами, которые используются для подключения к серверам, обеспечивающим взаимодействие с Sandbox.

Параметры интеграции с Sandbox

В таблице ниже описаны все доступные параметры и значения по умолчанию для всех параметров, которые вы можете указать для задачи Интеграция с Sandbox (`Standalone_Sandbox`).

Как настроить параметры интеграции с Sandbox

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port> [<setting name>=
<setting value>]
```

Параметр	Описание	Значение
`UseClientCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу Sandbox. Если проверка сертификата клиента включена на стороне сервера Sandbox, вам нужно включить использование сертификата клиента и добавить сертификат клиента перед запуском задачи *Интеграция с Sandbox*.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу Sandbox. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером в секундах.	Значение по умолчанию: `10`.
`RequestTimeout`	Максимальное время ожидания ответа от сервера в секундах.	Значение по умолчанию: `10`.
`SendingMode`	Режим отправки файла на проверку в Sandbox.	`AutoOnly` (значение по умолчанию) – автоматическая отправка файлов на проверку при обращении к файлу. `Manual` – ручная отправка файлов на проверку. `AutoAndManual` – автоматическая и ручная отправка файлов на проверку.
`QuarantineFile`	Помещение файла на карантин при обнаружении угрозы.	`Yes` (значение по умолчанию) – при обнаружении угрозы исходный файл удалить, копию файла поместить на карантин. `No` – не помещать файл на карантин при обнаружении угрозы.
`ScanCriticalAreas`	Выполнение проверки важных областей при обнаружении угрозы.	`Yes` (значение по умолчанию) – при обнаружении угрозы запустить проверку важных областей. `No` – не запускать проверку важных областей при обнаружении угрозы.
`CreateIocScanTask`	Создание задачи поиска IOC при обнаружении угрозы.	`Yes` (значение по умолчанию) – при обнаружении угрозы создать задачу поиска IOC. `No` – не создавать задачу поиска IOC при обнаружении угрозы.
`QuarantineFileOnIocDetected`	Помещение объекта на карантин при обнаружении индикатора компрометации.	`Yes` (значение по умолчанию) – при обнаружении индикатора компрометации исходный объект удалить, копию объекта поместить на карантин. `No` – не помещать объект на карантин при обнаружении индикатора компрометации.
`ScanCriticalAreasOnIocDetected`	Выполнение проверки важных областей при обнаружении индикатора компрометации.	`Yes` (значение по умолчанию) – при обнаружении индикатора компрометации запустить проверку важных областей. `No` – не запускать проверку важных областей при обнаружении индикатора компрометации.
`Drives`	Области поиска индикаторов компрометации.	`Critical` (значение по умолчанию) – проверять файлы в пользовательских и системных директориях. `System` – проверять все файлы в пределах корневой файловой системы.
`ScheduleMode`	Режим запуска задачи поиска IOC.	`Manually` (значение по умолчанию) – запускать задачу поиска IOC вручную. `AfterTreatDetected` – запускать задачу поиска IOC после обнаружения угрозы.
Секция **[Servers.item_#]** содержит параметры сервера Sandbox.		

Параметр	Описание	Значение
`Address`	Адрес сервера. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера.	Значение по умолчанию: `127.0.0.1`.
`Port`	Порт для подключения к серверу.	Значение по умолчанию: `443`.
Секция **[SandboxTransferSettings]** содержит параметры передачи файлов на проверку в Sandbox.		
`SandboxQueue`	Максимальный размер директории хранения очереди запросов на проверку в мегабайтах.	Значение по умолчанию: `1024`.

Управление сертификатами для подключения к серверу Sandbox

Для управления сертификатами требуются права пользователя с ролью Администратор (admin).

Вы можете управлять сертификатами, которые используются для подключения к серверам OSMP или серверам с компонентом Central Node, обеспечивающим взаимодействие с Sandbox (далее также к серверам Sandbox), с помощью команд. Вы можете выполнять следующие действия с сертификатами:

- добавлять или заменять сертификат сервера;
- выводить информацию о сертификате сервера;
- удалять сертификат сервера;
- добавлять или заменять сертификат клиента;
- выводить информацию о сертификате клиента;
- удалять сертификат клиента.

Чтобы добавить или заменить сертификат сервера, выполните следующую команду:

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

где `<file>` – путь к файлу, содержащему сертификат сервера.

Чтобы добавить или заменить сертификат клиента:

1. Выполните команду:

   ```
   kesl-control [-X] --add-sandbox-client-certificate <file>
   ```

   где `<file>` – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

2. Введите пароль от криптоконтейнера.

Сертификат клиента используется для дополнительной защиты соединения с сервером Sandbox, если в параметрах сервера Sandbox включена проверка сертификата клиента и в параметрах задачи *Интеграция с Sandbox* для параметра `UseClientCertificate` установлено значение `yes`.

Чтобы вывести информацию о сертификате, выполните следующую команду:

- для сертификата сервера:

  ```
  kesl-control [-X] --query-sandbox-server-certificate
  ```

- для сертификата клиента:

  ```
  kesl-control [-X] --query-sandbox-client-certificate
  ```

  В результате выполнения команды выводится следующая информация о сертификате:

- серийный номер сертификата;
- субъект сертификата;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- SHA1 и SHA256 отпечатки сертификата.

Чтобы удалить сертификат сервера, выполните следующую команду:

```
kesl-control [-X] --remove-sandbox-server-certificate
```

Чтобы удалить сертификат клиента, выполните следующую команду:

```
kesl-control [-X] --remove-sandbox-client-certificate
```

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum

В командной строке вы можете включать и выключать компонент EDR Optimum с помощью параметра `UseEdrOptimum` в общих параметрах приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Чтобы включить компонент EDR Optimum с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

Чтобы выключить компонент EDR Optimum с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-app-settings UseEdrOptimum=No
```

Настройка интеграции с Kaspersky Managed Detection and Response

В командной строке вы можете:

- Включать и выключать компонент MDR.
- Загружать и удалять файл MDR BLOB, который содержит информацию о лицензии Kaspersky Managed Detection and Response.

  Если для активации компонента MDR вы используете лицензионный ключ, загружать файл MDR BLOB не требуется.

Настройку интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response рекомендуется выполнять в Консоли администрирования или в Web Console.

Вы можете включать и выключать компонент MDR с помощью параметра `UseMDR` из общих параметров приложения. Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `UseMDR` может принимать следующие значения:

- `Yes` – включить компонент MDR.
- `No` – выключить компонент MDR.

> Если вы включаете компонент MDR, а Kaspersky Security Network выключен или используется в стандартном режиме, отображается сообщение об ошибке, компонент MDR не включается. Для включения компонента MDR требуется включить использование KSN в расширенном режиме.

Вы можете загружать и удалять файл MDR BLOB с помощью команд управления лицензионными ключами. Файл BLOB находится в ZIP-архиве конфигурационного файла MDR.

Чтобы загрузить файл BLOB, выполните следующую команду

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

Чтобы удалить файл BLOB, выполните следующую команду

```
kesl-control --remove-mdr-blob
```

После включения интеграции в приложении создается служебная задача `Mdr_Autostart_Scan` с режимом запуска один раз в сутки.

Управление сетевой изоляцией устройства

При интеграции с решениями Detection and Response вы можете выполнять следующие действия с помощью командной строки:

- проверять статус сетевой изоляции устройства и просматривать список исключений из сетевой изоляции;
- выключать сетевую изоляцию устройства.

Чтобы выключить сетевую изоляцию устройства, выполните следующую команду:

```
kesl-control [-R] --isolation-off
```

Чтобы проверить статус сетевой изоляции и просмотреть список исключений из сетевой изоляции, выполните следующую команду:

```
kesl-control [-R] --isolation-stat
```

Для сетевой изоляции отображается один из следующих статусов:

- *Сетевая изоляция включена.*
- *Сетевая изоляция выключена.*

Настройка параметров карантина

В командной строке вы можете настраивать параметры карантина с помощью параметров `QuarantineSizeLimit`, `QuarantineFillingNotification` и `QuarantineBackupFolder` в общих параметрах приложения.

Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметры карантина

Параметр	Описание	Значение
`QuarantineFillingNotification`	Процент заполнения карантина, при котором формируется событие о заполнении карантина. Чтобы выключить формирование событий о заполнении карантина, укажите значение 0.	0 – 100 0 – формирование событий о заполнении карантина выключено. Значение по умолчанию: 90.
`QuarantineSizeLimit`	Максимальный размер карантина (в мегабайтах). При достижении максимального размера карантина приложение удаляет самые старые файлы. Чтобы снять ограничение на размер карантина, укажите значение 0.	0 – 4000 0 – размер карантина не ограничен. Значение по умолчанию: 200, если приложение используется в стандартном режиме или в режиме EDR-Агента, и 100, если приложение используется в режиме Легкого агента.
`QuarantineBackupFolder`	Путь к директории, в которой хранятся объекты резервного хранилища и карантина. Вы можете указать директорию, отличную от директории, заданной по умолчанию. В качестве директории для хранения объектов резервного хранилища и карантина можно использовать директории на любых устройствах. Не рекомендуется указывать директории, расположенные на удаленных устройствах, например смонтированных по протоколам Samba и NFS. Если указанной директории не существует или она недоступна, приложение использует директорию, заданную по умолчанию.	Значение по умолчанию: /var/opt/kaspersky/kesl/common/objects-backup/ Для доступа к заданной по умолчанию директории требуются root-права.

Работа с файлами карантина в командной строке

При интеграции с решениями Detection and Response вы можете выполнять следующие действия с помощью команд управления карантином:

- Помещать файлы на карантин (только при интеграции с Kaspersky Endpoint Detection and Response Optimum или с Kaspersky Managed Detection and Response).
- Просматривать информацию о файлах на карантине.
- Удалять из карантина все или только указанные файлы.
- Восстанавливать файлы из карантина.

Восстановление зараженных файлов может привести к заражению устройства.

Помещение файла на карантин

Чтобы поместить файл на карантин, выполните следующую команду:

```
kesl-control [-Q] --put <path to the file> [--md5] [--sha256] [--save-original-file]
```

где:

- `<path to the file>` – путь к файлу, который вы хотите поместить на карантин;
- `--md5` – хеш-сумма MD5 файла, который вы хотите поместить на карантин;
- `--sha256` – хеш-сумма SHA256 файла, который вы хотите поместить на карантин;
- `--save-original-file` – не удалять исходный файл. Если вы не укажете этот ключ, исходный файл будет удален.

  Исходный файл удаляется, только если учетная запись пользователя имеет права на удаление объектов. Если прав недостаточно, отображается сообщение об ошибке удаления файла.

Вы можете использовать эту команду только при интеграции с Kaspersky Endpoint Detection and Response Optimum или с Kaspersky Managed Detection and Response.

Просмотр информации о файлах на карантине

Чтобы просмотреть информацию о файлах карантина, выполните следующую команду:

```
kesl-control -Q --query ["<filter conditions>"] [-n <number of files>] [--json]
```

где:

- `<filter conditions>` – одно или несколько логических выражений в формате `< поле > < операция сравнения > '< значение >'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса. Если вы не укажете условия фильтра, приложение выведет информацию обо всех файлах на карантине.
- `<number of files>` – количество последних файлов на карантине, которые нужно вывести. Если вы не укажете ключ `-n`, будут выведены последние 30 файлов. Чтобы показать все файлы, укажите значение 0.
- `--json` – выводить данные в формате JSON.

В строке `ObjectId` отобразится числовой идентификатор, который приложение присвоило файлу при помещении на карантин. Этот идентификатор используется для выполнения действий над файлом, таких как восстановление или удаление файла из карантина.

Восстановление файлов из карантина

Чтобы восстановить файл из карантина с исходным именем в исходное местоположение, выполните следующую команду:

```
kesl-control -Q --restore <object identifier>
```

где `<object identifier>` – числовой идентификатор, который приложение присвоило файлу при помещении на карантин.

Чтобы восстановить файл с новым именем из карантина в указанную директорию, выполните следующую команду:

```
kesl-control -Q --restore <object identifier> --file <path to the file>
```

где --file `<path to the file>` – новое имя файла и путь к директории, в которой вы хотите сохранить файл.

Вы можете восстановить файл из карантина в другую директорию, только если ваша учетная запись имеет root-права. Если прав недостаточно, файл можно восстановить только в исходное местоположение.

На устройствах с операционной системой Astra Linux в режиме замкнутой программной среды можно восстановить файл только под той учетной записью, под которой он был помещен в резервное хранилище. При восстановлении файла приложение создает директорию с мандатной меткой 3 (флаг cnnr).

Удаление файлов из карантина

Чтобы удалить выбранные файлы из карантина, выполните следующую команду:

```
kesl-control -Q --mass-remove --query "<filter conditions>"
```

где `<filter conditions>` – одно или несколько логических выражений в формате <поле> <операция сравнения> '<значение>', скомбинированных с помощью логического оператора and, для ограничения результатов запроса.

```
Пример удаления файлов, в названии которых или в пути к которым содержится "test"
kesl-control -Q --mass-remove --query "FileName like '%test%'"
```

Чтобы удалить все файлы из карантина, выполните следующую команду:

```
kesl-control -Q --mass-remove
```

Поиск индикаторов компрометации

Вы можете выполнять поиск индикаторов компрометации с помощью задачи поиска IOC в командной строке только при интеграции с Kaspersky Endpoint Detection and Response Optimum. При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) или с Kaspersky Endpoint Detection and Response (KATA) поиск IOC выполняется на стороне соответствующего решения Detection and Response.

Чтобы создать, настроить и запустить задачу Поиск IOC в командной строке, выполните следующую команду:

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

где:

- `--path <path to the directory or file>` – путь к IOC-файлу или директории с IOC-файлами с расширением .IOC или .XML, с помощью которых требуется выполнить проверку.

  Вы можете указать несколько путей, разделяя их пробелами. Вы также можете указать оба типа путей (к файлу и к директории).

- `--process` – включение анализа процессов, запущенных на устройстве.

  Возможные аргументы:

  - `on` – включить анализ процессов, запущенных на устройстве (значение по умолчанию).
  - `off` – выключить анализ процессов, запущенных на устройстве.

  Если вы не укажете ключ `--process`, приложение выполнит анализ процессов, только если в используемом IOC-файле указаны данные этих процессов (`ProcessItem`).

- `--hint <regular expression>` – регулярное выражение, которому соответствует полный путь к файлу (`FileItem`) или исполняемому файлу процесса (`ProcessItem`), который требуется проанализировать.

  Вы можете использовать следующие элементы регулярных выражений:

  - метасимволы: `. ^ $ |`
  - классы символов: digit, alpha, lower, upper, cntrl
  - квантификаторы: `* + ? {n} {n,} {n, m}`
  - отрицание: `[^a-c]`
  - экранируемые символы: `\a \e \f`, `\n \r \t \v \b`

- `--arpentry` – включение анализа записей в ARP-таблице (`ArpEntryItem`).

Возможные аргументы:

- `on` – включить анализ записей в ARP-таблице (значение по умолчанию).
- `off` – выключить анализ записей в ARP-таблице.

Если вы не укажете ключ `--arpentry`, приложение выполнит анализ таблицы ARP, только если в используемом IOC-файле указаны данные этой таблицы (`ArpEntryItem`).

`--ports` – включение анализа портов, открытых для соединения.

Возможные аргументы:

- `on` – включить анализ портов, открытых для соединения и проверять активные соединения на устройстве (значение по умолчанию).
- `off` – выключить анализ портов, открытых для соединения и не проверять активные соединения на устройстве.

Если вы не укажете ключ `--ports`, приложение выполнит анализ портов, только если в используемом IOC-файле указаны данные этих портов (`PortItem`).

- `--system` – включение анализа окружения системы.

  Возможные аргументы:

  - `on` – включить анализ окружения системы (значение по умолчанию).
  - `off` – выключить анализ окружения системы.

  Если вы не укажете ключ `--system`, приложение выполнит анализ окружения системы, только если в используемом IOC-файле указаны данные об окружении системы (`SystemInfoItem`).

- `--files` – включение анализа файлов.

  Возможные аргументы:

  - `on` – включить анализ файлов (значение по умолчанию).
  - `off` – выключить анализ файлов.

  Если вы не укажете ключ `--files`, приложение выполнит анализ файлов, только если в используемом IOC-файле указаны данные этих файлов (`FileItem`).

- `--drives` – области, подлежащие проверке.

  Возможные аргументы:

  - `all` – проверять все доступные файловые области.
  - `system` – проверять все файлы в пределах корневой файловой системы.
  - `critical` – проверять файлы в пользовательских и системных директориях (значение по умолчанию).
  - `custom` – проверять только файлы в указанных вами областях.

  Если вы не укажете ключ `--drives`, приложение выполнит анализ файлов в пользовательских и системных директориях.

- `--excludes <list of exclusions>` – список путей, исключаемых из проверки.

  Исключения, заданные этим ключом, являются глобальными и действуют независимо от типа области или списка директорий. Такие исключения имеют приоритет над другими ключами, включая `--hint` и `--scope`.

  > Исключения задаются в виде путей, но не могут содержать рекурсивные элементы или символы маски (например, `*`).

  Если вы не укажете ключ `--excludes`, проверка выполняется без исключений.

  Вы можете указать несколько исключений, разделяя их пробелом.

- `--scope <list of directories>` – список дополнительных директорий, подлежащих проверке.

  > Этот ключ является обязательным, если для ключа `--drives` вы указали аргумент `custom`.

- `--action` – действие, выполняемое при обнаружении индикаторов компрометации.

  Возможные аргументы:

  - `Skip` – приложение не будет выполнять никаких действий с обнаруженным объектом, но информация о нем сохранится в результатах выполнения задачи (значение по умолчанию).
  - `QuarantineFile` – приложение поместит обнаруженный объект на карантин.
  - `IsolateHost` – приложение изолирует от сети устройство, на котором обнаружен объект.
  - `ScanCriticalAreas` – приложение выполнит проверку важных областей.

    Важные области, которые проверяет Kaspersky Endpoint Security

    - /lib/systemd
    - /lib/udev
    - /lib/dbus-1.0
    - /usr/local/lib/systemd/user
    - /usr/share/dbus-1
    - /usr/share/gdm/autostart
    - /usr/share/gnome/autostart
    - /var/spool/at
    - /var/spool/at/spool
    - /var/spool/anacron
    - /var/spool/cron
    - /boot

- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

Вы можете указать несколько действий, разделяя их запятыми.

> Если вы указали аргумент `Skip`, остальные аргументы добавлять не нужно. Аргумент `Skip` может использоваться только самостоятельно.

Управление запретом запуска объектов

Запрет запуска объектов позволяет контролировать запуск исполняемых файлов и скриптов, а также открытие файлов офисного формата. Запрет запуска объектов управляет доступом пользователей к файлам с помощью правил запрета запуска.

Запрет запуска объектов включает в себя следующие задачи:

- *Запрет запуска объектов (EDR Expert (on-premises))* (`KATAEDR_Prevention`).
- *Запрет запуска объектов (EDR Expert (cloud))* (`EDRExpertCloud_Prevention`).
- *Запрет запуска объектов (EDR Optimum)* (`EDRO_Prevention`).

По умолчанию задачи *Запрет запуска объектов* не запущены. Если вы добавили хотя бы одно правило запрета запуска, то приложение запускает задачу.

Чтобы просмотреть список правил запрета запуска объектов, выполните следующую команду:

```
kesl-control [-T] --get-prevention-state [--kata|cxdr|edro]
```

где:

`--kata` – список правил запрета запуска объектов компонента EDR Expert (on-premises);

`--cxdr` – список правил запрета запуска объектов компонента EDR Expert (cloud);

`--edro` – список правил запрета запуска объектов компонента EDR Optimum.

Настройка интеграции с KUMA

В командной строке вы можете управлять интеграцией приложения Kaspersky Endpoint Security с Kaspersky Unified Monitoring and Analysis Platform с помощью предустановленной задачи *Интеграция с Kaspersky Unified Monitoring and Analysis Platform*.

По умолчанию задача *Интеграция с Kaspersky Unified Monitoring and Analysis Platform* не запущена. Вы можете запускать и останавливать эту задачу вручную.

Вы можете настраивать параметры интеграции с Kaspersky Unified Monitoring and Analysis Platform, изменяя параметры предустановленной задачи.

С помощью команд управления параметрами интеграции с Kaspersky Unified Monitoring and Analysis Platform вы можете управлять сертификатами, которые используются для подключения к серверам KUMA.

Задача Интеграция с Kaspersky Unified Monitoring and Analysis Platform

В таблице ниже описаны все доступные параметры и значения по умолчанию для всех параметров, которые вы можете указать для задачи Интеграция с Kaspersky Unified Monitoring and Analysis Platform (`KUMA`).

Параметр	Описание	Значение
`UseTls`	Включение и выключение проверки сертификата сервера для дополнительной защиты подключения к серверу KUMA.	`Yes` – использовать сертификат для дополнительной защиты подключения к серверу KUMA. `No` (значение по умолчанию) – не использовать сертификат для защиты подключения к серверу KUMA.
`UseClientCertificate`	Включение и выключение двусторонней аутентификации для дополнительной защиты подключения к серверу KUMA. Если проверка сертификата клиента включена на стороне сервера KUMA, вам нужно включить использование сертификата клиента и добавить сертификат клиента перед запуском задачи Интеграция с Kaspersky Unified Monitoring and Analysis Platform.	`Yes` – использовать двустороннюю аутентификацию для дополнительной защиты подключения к серверу KUMA. `No` (значение по умолчанию) – не использовать двустороннюю аутентификацию.
`ConnectionTimeout`	Максимальное время ожидания соединения с сервером KUMA в секундах.	Значение по умолчанию: `5`.
Секция **[Servers.item_#]** содержит параметры сервера KUMA.		
`ServerAddress`	Адрес сервера KUMA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Если вы установили значение параметра `UseTls=Yes`, требуется указать полное доменное имя (FQDN) сервера из сертификата, полученного при приобретении лицензии на использование KUMA.	Значение по умолчанию: `127.0.0.1`.
`ServerPort`	Порт для подключения к серверу KUMA.	Значение по умолчанию: `443`.
`ServerProtocol`	Протокол для подключения к серверу KUMA.	`tcp` (значение по умолчанию) – использовать для подключения к серверу KUMA протокол TCP. `HTTPWithCompression` – использовать для подключения к серверу KUMA протокол HTTP с возможностью сжатия событий при их передаче. `udp` – использовать для подключения к серверу KUMA протокол UDP. При выборе протокола UDP использование сертификатов для обеспечения безопасности соединения не поддерживается (значения параметров `UseTls`, `UseClientCertificate` и `ConnectionTimeout` не учитываются), а также отсутствуют события о соединении с сервером KUMA.
Секция **[KumaTransferSettings]** содержит параметры передачи событий на сервер KUMA.		
`EventTransferTimeMax`	Максимальная задержка отправки событий на сервер KUMA в секундах.	Значение по умолчанию: `30`.

Управление сертификатами для подключения к серверу KUMA

При выборе протокола UDP использование сертификатов для обеспечения безопасности соединения не поддерживается.

Для управления сертификатами требуются права пользователя с ролью Администратор (admin).

Вы можете управлять сертификатами, которые используются для подключения к серверу KUMA, с помощью команд. Вы можете выполнять следующие действия с сертификатами:

- добавлять или заменять сертификат сервера;
- выводить информацию о сертификате сервера;
- удалять сертификат сервера;
- добавлять или заменять сертификат клиента;
- выводить информацию о сертификате клиента;
- удалять сертификат клиента.

Чтобы добавить или заменить сертификат сервера, выполните следующую команду:

```
kesl-control [-M] --add-kuma-server-certificate <path to the file>
```

где `<path to the file>` – путь к файлу формата DER или PEM, содержащему сертификат сервера.

Чтобы добавить или заменить сертификат клиента:

1. Выполните команду:

   ```
   kesl-control [-M] --add-kuma-client-certificate <path to the file>
   ```

   где `<path to the file>` – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

2. Введите пароль от криптоконтейнера.

Сертификат клиента используется для дополнительной защиты соединения с сервером KUMA, если в параметрах сервера KUMA включена проверка сертификата клиента и в параметрах задачи *Интеграция с Kaspersky Unified Monitoring and Analysis Platform* для параметра `UseClientCertificate` установлено значение `yes`.

Чтобы вывести информацию о сертификате, выполните следующую команду:

- для сертификата сервера:

  ```
  kesl-control [-M] --query-kuma-server-certificate
  ```

- для сертификата клиента:

  ```
  kesl-control [-M] --query-kuma-client-certificate
  ```

В результате выполнения команды выводится следующая информация о сертификате:

- серийный номер сертификата;
- субъект сертификата;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- SHA1 и SHA256 отпечатки сертификата.

Чтобы удалить сертификат сервера, выполните следующую команду:

```
kesl-control [-M] --remove-kuma-server-certificate
```

Чтобы удалить сертификат клиента, выполните следующую команду:

```
kesl-control [-M] --remove-kuma-client-certificate
```

Общие параметры

В Консоли администрирования вы можете настраивать общие параметры приложения, которые определяют работу приложения в целом и работу отдельных функций, в свойствах политики (**Общие параметры**).

Общие параметры приложения

В таблице ниже описаны общие параметры приложения, которые определяют работу приложения в целом и работу отдельных функций.

Параметр	Описание	Значения
`SambaConfigPath`	Директория, в которой хранится конфигурационный файл Samba. Конфигурационный файл Samba нужен для обеспечения работы значений `AllShared` или `Shared:SMB` для параметра `Path`. После изменения значения этого параметра требуется перезапустить приложение.	По умолчанию указана стандартная директория конфигурационного файла Samba. Значение по умолчанию: /etc/samba/smb.conf.
`NfsExportPath`	Директория, в которой хранится конфигурационный файл NFS. Конфигурационный файл NFS нужен для обеспечения работы значений `AllShared` или `Shared:NFS` для параметра `Path`. После изменения значения этого параметра требуется перезапустить приложение.	По умолчанию указана стандартная директория конфигурационного файла NFS. Значение по умолчанию: /etc/exports.
`TraceFolder`	Директория, в которой хранятся файлы трассировки приложения. После изменения значения этого параметра требуется перезапустить приложение.	Значение по умолчанию: /var/log/kaspersky/kesl. Для доступа к директории хранения файлов трас заданной по умолчанию, требуются root-права. Е указываете другую директорию, убедитесь, что с разрешена на чтение и запись только для учетно root (права `700` или `rwx--------`).
`TraceLevel`	Включение трассировки приложения и уровень детализации файлов трассировки. Этот параметр включает только создание файла трассировки приложения. Для создания файлов трассировки графического интерфейса и утилиты командной строки kesl-control требуется задать переменную окружения LFS_ENABLE_ALL_COMPONENTS_LOGGING.	`Detailed` – создавать детализированный файл трассировки приложения. `MediumDetailed` – создавать файл трассировки приложения, содержащий информационные соо сообщения об ошибках. `NotDetailed` – создавать файл трассировки пр содержащий сообщения об ошибках. `None` (значение по умолчанию) – не создавать ф трассировки приложения.
`TraceMaxFileCount`	Максимальное количество файлов трассировки приложения. После изменения значения этого параметра требуется перезапустить приложение.	1–10000 Значение по умолчанию: 10.
`TraceMaxFileSize`	Максимальный размер файла трассировки приложения (в мегабайтах). После изменения значения этого параметра требуется перезапустить приложение.	1–1000 Значение по умолчанию: 500.

Параметр	Описание	Значения
`WdTraceLevel`	Включение трассировки Watchdog-сервера и уровень детализации файлов трассировки.	`Detailed` – создавать детализированный файл трассировки Watchdog-сервера. `MediumDetailed` – создавать файл трассировки Watchdog-сервера, содержащий информационн сообщения и сообщения об ошибках. `NotDetailed` – создавать файл трассировки Wa сервера, содержащий сообщения об ошибках. `None` – не создавать файл трассировки Watchdo `Product` (значение по умолчанию) – установить равное значению параметра `TraceLevel`.
`BlockFilesGreaterMaxFileNamePath`	Блокировка доступа к файлам, длина полного пути к которым превышает заданное значение параметра (в байтах). Если длина полного пути к проверяемому файлу превышает значение этого параметра, задачи проверки пропускают такой файл во время проверки. Этот параметр применяется только для операционных систем, не поддерживающих технологию fanotify. После изменения значения этого параметра требуется перезапустить задачу Защита от файловых угроз.	4096–33554432 Значение по умолчанию: 16384.
`DetectOtherObjects`	Включение обнаружения легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.	`Yes` – включить обнаружение легальных прилож которые злоумышленники могут использовать дл нанесения вреда устройствам или данным. `No` (значение по умолчанию) – выключить обнар легальных приложений, которые злоумышленник использовать для нанесения вреда устройствам данным.
`NamespaceMonitoring`	Включение проверки пространств имен и контейнеров. Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен.	`Yes` (значение по умолчанию) – включить провер пространств имен и контейнеров. `No` – выключить проверку пространств имен и ко
`FileBlockDuringScan`	Включение режима перехвата файловых операций с блокированием доступа к файлам во время проверки. Режим перехвата файловых операций влияет на работу компонентов Защита от файловых угроз, Контроль устройств, Запрет запуска объектов и задачи Проверка съемных дисков.	`Yes` (значение по умолчанию) – блокировать дос файлам во время проверки. `No` – не блокировать доступ к файлам во время п Обращение к любому файлу разрешается, прове выполняется в асинхронном режиме. Такой режи перехвата файловых операций оказывает меньш на производительность системы во время работ риск, что угроза в файле не будет вылечена или у Это возможно, если во время проверки процесс с этим файлом, успеет, например, изменить имя принятия приложением решения о статусе этого этом компоненты Защита от файловых угроз, Ко устройств, Запрет запуска объектов и задача Пр съемных дисков работают в режиме информиро независимо от установленного режима работы.
`UseKSN`	Настройка использования Kaspersky Security Network в работе приложения.	`Basic` – включить использование Kaspersky Sec Network в стандартном режиме. `Extended` – включить использование Kaspersky Network в расширенном режиме. `No` (значение по умолчанию) – не использовать K Security Network.

Параметр	Описание	Значения
`CloudMode`	Включение облачного режима работы приложения. Облачный режим доступен, если включено использование KSN. Если вы планируете использовать облачный режим, убедитесь, что KSN доступен на устройстве. Параметр применяется, только если приложение используется в стандартном режиме.	`Yes` (значение по умолчанию) – включить режим при котором приложение Kaspersky Endpoint Sec использует облегченную версию баз вредоносн `No` – использовать полную версию баз вредонос Облачный режим выключается автоматическ выключено использование KSN.
`UseMDR`	Включение компонента Managed Detection and Response для интеграции с Kaspersky Managed Detection and Response. Если вы включаете компонент MDR, а Kaspersky Security Network выключен или используется в стандартном режиме, отображается сообщение об ошибке, компонент MDR не включается. Для включения компонента MDR требуется включить использование KSN в расширенном режиме. Параметр неприменим для устройств с процессором Эльбрус.	`Yes` – включить компонент Managed Detection a Response. `No` (значение по умолчанию) – выключить компо Managed Detection and Response.
`UseEdrOptimum`	Включение компонента EDR Optimum для интеграции с Kaspersky Endpoint Detection and Response Optimum. Параметр неприменим для устройств с процессором Эльбрус.	`Yes` – включить компонент EDR Optimum. `No` (значение по умолчанию) – выключить компо Optimum.
`UseProxy`	Включение использования прокси-сервера компонентами приложения Kaspersky Endpoint Security. Прокси-сервер может использоваться для доступа к серверам активации "Лаборатории Касперского", к источникам обновлений баз и модулей приложения, к Kaspersky Security Network и при проверке сертификатов сайтов компонентом Защита от веб-угроз. Если Kaspersky Endpoint Security используется в режиме Легкого агента, не поддерживается использование прокси-сервера для подключения к Kaspersky Security Network, к SVM и к Серверу интеграции.	`Yes` – включить использование прокси-сервера. `No` (значение по умолчанию) – выключить исполь прокси-сервера.

Параметр	Описание	Значения
`ProxyServer`	Адрес прокси-сервера, используемого для подключения к интернету. Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.	Адрес прокси-сервера в одном из следующих ф • `[<connection protocol>://]<address o proxy server>:<port>`, если для подключе прокси-серверу не требуется аутентификац • `[<connection protocol>://][<user nam [<password>]@]<address of the proxy <port>`, если для подключения к прокси-сер требуется аутентификация. Если вы указыва адрес в формате IPv6, то вводите адрес в ква скобках. Подключение к прокси-серверу по протоколу не поддерживается.
`ProxyBypass`	Список адресов, для подключения к которым прокси-сервер не используется.	Адрес задается в формате `<address>[:<port>` указания адресов вы можете использовать маск `*`) и комментарии после символа `\`.
`ProxyBypassEdr`	Использование прокси-сервера при подключении к серверам, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises). Параметр неприменим для устройств с процессором Эльбрус.	`Yes` – не использовать прокси-сервер при подкл серверам, обеспечивающим интеграцию с Kaspe Endpoint Detection and Response Expert (on-pren `No` (значение по умолчанию) – использовать про при подключении к серверам, обеспечивающим с Kaspersky Endpoint Detection and Response Exp premises).
`ProxyBypassNdr`	Использование прокси-сервера при подключении к серверам, обеспечивающим интеграцию с Kaspersky Network Detection and Response (KATA). Параметр неприменим для устройств с процессором Эльбрус.	`Yes` – не использовать прокси-сервер при подкл серверам, обеспечивающим интеграцию с Kaspe Network Detection and Response (KATA). `No` (значение по умолчанию) – использовать про при подключении к серверам, обеспечивающим с Kaspersky Network Detection and Response (KA
`ProxyBypassSandbox`	Использование прокси-сервера при подключении к серверам, обеспечивающим взаимодействие с Sandbox. Параметр неприменим для устройств с процессором Эльбрус.	`Yes` – не использовать прокси-сервер при подкл серверам, обеспечивающим взаимодействие с S `No` (значение по умолчанию) – использовать про при подключении к серверам, обеспечивающим взаимодействие с Sandbox.
`MaxEventsNumber`	Максимальное количество событий, которые будет хранить приложение. При превышении заданного количества событий приложение удаляет наиболее давние события.	Значение по умолчанию: 500000. Если задано значение 0, то новые события не со а старые события будут удалены.
`LimitNumberOfScanFileTasks`	Максимальное количество задач выборочной проверки, которые непривилегированный пользователь может одновременно запустить на устройстве. Этот параметр не ограничивает количество задач, которые может запустить пользователь с root-правами или с ролью kesladmin.	0–100000 0 – непривилегированный пользователь не може задачи выборочной проверки. Значение по умолчанию: 100.
`UseSyslog`	Включение записи событий приложения в syslog. Для доступа к syslog требуются root-права.	`Yes` – включить запись событий в syslog. `No` (значение по умолчанию) – выключить запись syslog.

Параметр	Описание	Значения
`EventsStoragePath`	Путь к основному файлу базы данных журнала событий. Для доступа к заданной по умолчанию базе данных событий требуются root-права.	Значение по умолчанию: `/var/opt/kaspersky/kesl/private/storage/`
`ExcludedMountPoint.item_#`	Точка монтирования, которую требуется исключить из области проверки. Исключение применяется в работе компонентов Защита от файловых угроз, Защита от шифрования, Мониторинг контейнеров и задачи Проверка съемных дисков, а также настраивается в работе задач проверки (типов ODS и ContainerScan). Вы можете указать несколько точек монтирования, которые требуется исключить из проверки. Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды `mount`. Параметр `ExcludedMountPoint.item_#` по умолчанию не указан.	`AllRemoteMounted` – исключать из перехвата ф операций все удаленные директории, смонтиров устройстве с помощью протоколов SMB и NFS. `Mounted:NFS` – исключать из перехвата файлов операций все удаленные директории, смонтиров устройстве с помощью протокола NFS. `Mounted:SMB` – исключать из перехвата файлов операций все удаленные директории, смонтиров устройстве с помощью протокола SMB. `Mounted:<file system type>` – исключать из файловых операций все смонтированные директ указанным типом файловой системы. `/mnt` – исключать из перехвата объекты, находя точке монтирования /mnt (включая вложенные д используемой в качестве временной точки монт съемных дисков. `<path that contains the /mnt/user*|/mnt/**/user_share>` – исключат перехвата объекты, находящиеся в точках монти имена которых содержат указанную маску.
`MemScanExcludedProgramPath.item_#`	Исключение памяти процесса из проверки. Приложение не будет проверять память указанного процесса.	`<full path to process>` – исключать из пров процесс в указанной локальной директории. Для пути вы можете использовать маски.
`PowerSaveMode`	Отмена запуска запланированных задач на устройстве, работающем от аккумулятора.	`Yes` (значение по умолчанию) – пропускать запу для которых настроено расписание запуска, если устройство работает от аккумулятора. `No` – запускать задачи по расписанию независим источника питания, к которому подключено устр (сеть или аккумулятор).
`UseOnDemandCPULimit`	Включение ограничения на использование ресурсов процессора для задач типа *ODS*, *ContainerScan* и *InventoryScan*.	`Yes` – включить ограничение потребления ресур процессора для задач типа *ODS*, *ContainerScan* и *InventoryScan*. `No` (значение по умолчанию) – выключить огран потребления ресурсов процессора для задач.
`OnDemandCPULimit`	Максимальное значение нагрузки на все ядра процессора (в процентах) при работе задач типа *ODS*, *ContainerScan* и *InventoryScan*.	Целое число в пределах от 10 до 100. Значение по умолчанию: 100.
`BackupSizeLimit`	Максимальный размер резервного хранилища (в мегабайтах). При достижении максимального размера резервного хранилища приложение удаляет самые старые резервные копии файлов. Чтобы снять ограничение на размер резервного хранилища, укажите значение 0.	0 – 4000 0 – размер резервного хранилища не ограничен Значение по умолчанию: 0.
`BackupDaysToLive`	Интервал времени, в течение которого объекты хранятся в резервном хранилище (в сутках). По истечении заданного времени приложение удаляет самые старые резервные копии файлов. Чтобы снять ограничение на время хранения объектов в резервном хранилище, укажите значение 0.	0 – 10000 0 – время хранения объектов в резервном хран ограничено. Значение по умолчанию: 30.

Параметр	Описание	Значения
`QuarantineSizeLimit`	Максимальный размер карантина (в мегабайтах). При достижении максимального размера карантина приложение удаляет самые старые файлы. Чтобы снять ограничение на размер карантина, укажите значение 0. Параметр неприменим для устройств с процессором Эльбрус.	0 – 999999 0 – размер карантина не ограничен. Значение по умолчанию: 200, если приложение используется в стандартном режиме, и 100, если приложение используется в режиме Легкого аге
`QuarantineFillingNotification`	Процент заполнения карантина, при котором формируется событие о заполнении карантина. Чтобы выключить формирование событий о заполнении карантина, укажите значение 0. Параметр неприменим для устройств с процессором Эльбрус.	0 – 100 0 – формирование событий о заполнении карант выключено. Значение по умолчанию: 90.
`QuarantineBackupFolder`	Путь к директории, в которой хранятся резервные копии файлов и файлы, помещенные на карантин. Вы можете изменить директорию, заданную по умолчанию. Если указанной директории не существует или она недоступна, приложение использует директорию, заданную по умолчанию. Параметр неприменим для устройств с процессором Эльбрус. Используется параметр `BackupFolder`.	Значение по умолчанию: `/var/opt/kaspersky/kesl/common/objects-b` Для доступа к заданной по умолчанию директ требуются root-права.
`BackupFolder`	Путь к директории резервного хранилища. Вы можете изменить директорию, заданную по умолчанию. Если указанной директории не существует или она недоступна, приложение использует директорию, заданную по умолчанию.	Значение по умолчанию: `/var/opt/kaspersky/kesl/common/objects-b` Для доступа к заданной по умолчанию директ резервного хранилища требуются root-права
`ShowPopUpNotifications`	Включение отображения всплывающих уведомлений в графическом пользовательском интерфейсе.	`Yes` (значение по умолчанию) – показывать всп уведомления в графическом пользовательском и `No` – не показывать всплывающие уведомления в графическом пользовательском интерфейсе.
`InterceptorMode`	Механизм перехвата системных событий, который приложение Kaspersky Endpoint Security использует в своей работе. Параметр применяется только на устройствах, где операционная система поддерживает технологию fanotify. Параметр неприменим для устройств с процессором Эльбрус.	`UseFanotify` (значение по умолчанию) – исполь технологию fanotify для перехвата системных со `UseUpdatableKernelModule` – использовать об модуль ядра для перехвата системных событий.

Параметр	Описание	Значения
`InterceptorFallbackStrategy`	Действие, которое приложение выполняет, если обновляемый модуль ядра не запускается. Параметр применяется только на устройствах, где операционная система поддерживает технологию fanotify.	`FallbackToFanotify` (значение по умолчанию) использованию технологии fanotify для перехват системных событий. `FallbackToLimitedMode` – не использовать пер системных событий. Если приложение не исполь перехват системных событий, проверка файлов в реального времени не выполняется, уровень заш устройства снижается.
`InterceptorApplyStrategy`	Если приложение переходит к использованию обновляемого модуля ядра, для запуска модуля требуется перезапуск приложения. Параметр позволяет указать, будет ли перезапуск приложения выполняться автоматически или требуется перезапуск приложения вручную. Параметр применяется только на устройствах, где операционная система поддерживает технологию fanotify.	`RestartServiceAutomatically` – автоматичес перезапускать приложение для запуска обновля модуля ядра. Рекомендуется использовать этот п `RestartServiceManually` (значение по умолча запускать обновляемый модуль ядра после пере приложения, выполненного пользователем вручн
`SystemEventsTransmission`	Включение передачи информации о событиях сторонних приложений (не являющихся решениями "Лаборатории Касперского"). Если параметр включен, помимо собственных событий Kaspersky Endpoint Security также отправляет попадающие в systemd-journald события сторонних приложений в журнал событий приложения. Для доступа к systemd-journald требуются root-права.	`Yes` – включить передачу информации о событи сторонних приложений из systemd-journald в жур событий приложения. `No` (значение по умолчанию) – выключить переда информации о событиях сторонних приложений systemd-journald в журнал событий приложения.
`UrgentUpdateRestartEnabled`	Автоматический перезапуск приложения при получении критически важных обновлений по истечении первых суток после установки приложения.	`Yes` – автоматический перезапускать приложени получении критически важных обновлений. `No` (значение по умолчанию) – не перезапускать приложение при получении критически важных с
`CoreDumps`	Включение создания файла дампа при сбое в работе приложения.	`Yes` – создавать файл дампа при сбое в работе приложения. `No` (значение по умолчанию) – не создавать фай сбое в работе приложения.
`CoreDumpsPath`	Путь к директории, в которой хранятся файлы дампов.	Значение по умолчанию: `/var/opt/kaspersky/kesl/common/dumps` Для доступа к директории хранения файлов д заданной по умолчанию, требуются root-прав

Полезные статьи

Как задавать маски

Вы можете использовать символ * (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Расписание задач

В таблице ниже описаны параметры расписания запуска задач, которые вы можете настроить для всех задач приложения.

Параметры расписания запуска задачи

Параметр	Описание
`RuleType`	Расписание запуска задачи. • `Once` – запускать задачу один раз. • `Monthly` – запускать задачу каждый месяц в указанный день и в указанное время. • `Weekly` – запускать задачу каждую неделю в указанный день и в указанное время. • `Daily` – запускать задачу регулярно, с заданным интервалом в днях. • `Hourly` – запускать задачу регулярно, с заданным интервалом в часах, начиная с указанных даты и времени. • `Minutely` – запускать задачу регулярно, с заданным интервалом в минутах, начиная с указанного времени. • `Manual` – запускать задачу вручную. • `PS` – запускать задачу после запуска приложения. • `BR` – запускать задачу после обновления баз приложения.
`StartTime`	Дата и время запуска задачи. Формат параметра зависит от значения `RuleType`. Допустимые значения: • `<year>`: 1970 – 2099; • `<month>`: JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC; • `<day of the month>`: 1 – 31; • `<day of the week>`: Mon, Tue, Wed, Thu, Fri, Sat, Sun; • `<hh>`: 0 – 23; • `<mm>`: 0 – 59; • `<ss>`: 0 – 59; • `<interval between runs (in days)>`: 0 – 364; • `<interval between runs (in hours)>`: 0 – 23; • `<interval between runs (in minutes)>`: 0 – 59.
`RandomInterval`	Запуск задачи на компьютерах случайным образом в течение определенного интервала времени (от 0 до указанного значения). Это позволяет избежать одновременный запуск задач. Значение по умолчанию: 99 минут. Допустимые значения: 0 – 999.
`RunMissedStartRules`	Запуск пропущенной задачи после запуска приложения. • `Yes` (значение по умолчанию) – запуск пропущенной задачи включен. Если во время запуска задачи по расписанию приложение остановлено или компьютер выключен, Kaspersky Endpoint Security запускает задачу сразу после запуска приложения. Это позволяет не пропустить запуск критически важных задач. • `No` – запуск пропущенной задачи выключен. Если во время запуска задачи по расписанию приложение остановлено или компьютер выключен, приложение пропускает запуск этой задачи. Это позволяет избежать повышенной нагрузки при запуске приложения.
`UseWorkingTimeout`	Остановка задачи при достижении максимального времени выполнения задачи, заданного параметром `WorkingTimeout`. Задача будет остановлена, даже если она не завершена. Следующий запуск задачи будет выполнен по расписанию. • `Yes` – останавливать задачу при достижении максимального времени выполнения задачи. • `No` (значение по умолчанию) – не останавливать задачу при достижении максимального времени выполнения задачи.

Параметр	Описание
WorkingTimeout	Максимальное время выполнения задачи (в минутах), при достижении которого приложение останавливает выполнение задачи, если значение параметра UseWorkingTimeout=Yes. Значение по умолчанию: 120 минут. Допустимые значения: 1 – 999.

Настройка параметров прокси-сервера

В командной строке вы можете настраивать использование прокси-сервера компонентами приложения с помощью параметров UseProxy, ProxyServer, ProxyBypass, ProxyBypassEdr, ProxyBypassNdr и ProxyBypassSandbox из общих параметров приложения.

Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр UseProxy может принимать следующие значения:

- Yes – включить использование прокси-сервера.
- No – выключить использование прокси-сервера.

Параметр ProxyServer позволяет задавать параметры прокси-сервера в формате <connection protocol>://[<user>[:<password>]@]<proxy server address>:<port number>, где:

- <user> – имя пользователя для аутентификации на прокси-сервере.
- <password> – пароль пользователя для авторизации на прокси-сервере.
- <proxy server address> – IP-адрес или доменное имя прокси-сервера.
- <port number> – номер порта прокси-сервера.

Подключение к прокси-серверу по протоколу HTTPS не поддерживается.

Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.

Параметр ProxyBypass позволяет задать список адресов, для подключения к которым не будет использоваться прокси-сервер. Адрес задается в формате <address>[:<port number>]. Для указания адресов вы можете использовать маски (символы *) и комментарии (после символа \).

Следующие параметры позволяют настроить использование прокси-сервера в работе компонентов EDR Expert (on-premises), NDR (KATA) и Sandbox, которые обеспечивают интеграцию с решениями Detection and Response:

- параметр `ProxyBypassEdr` позволяет включать и выключать использование прокси-сервера при подключении к серверам, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises) или с Kaspersky Endpoint Detection and Response (KATA);
- параметр `ProxyBypassNdr` позволяет включать и выключать использование прокси-сервера при подключении к серверам, обеспечивающим интеграцию с Kaspersky Network Detection and Response (KATA);
- параметр `ProxyBypassSandbox` позволяет включать и выключать использование прокси-сервера при подключении к серверам, обеспечивающим взаимодействие с Sandbox.

Параметры могут принимать следующие значения:

- `Yes` – включить использование прокси-сервера.
- `No` – выключить использование прокси-сервера.

Настройка параметров резервного хранилища

В командной строке вы можете настраивать параметры резервного хранилища с помощью параметров `BackupDaysToLive, BackupSizeLimit` и `QuarantineBackupFolder` в общих параметрах приложения.

Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметры резервного хранилища

Параметр	Описание	Значение
`BackupDaysToLive`	Интервал времени, в течение которого объекты хранятся в резервном хранилище (в сутках). По истечении заданного времени приложение удаляет самые старые резервные копии файлов. Чтобы снять ограничение на время хранения объектов в резервном хранилище, укажите значение 0.	0 – 10000 0 – время хранения объектов в резервном хранилище не ограничено. Значение по умолчанию: 30.
`BackupSizeLimit`	Максимальный размер резервного хранилища (в мегабайтах). При достижении максимального размера резервного хранилища приложение удаляет самые старые резервные копии файлов. Чтобы снять ограничение на размер резервного хранилища, укажите значение 0.	0 – 4000 0 – размер резервного хранилища не ограничен. Значение по умолчанию: 0.

Параметр	Описание	Значение
`QuarantineBackupFolder`	Путь к директории, в которой хранятся резервные копии файлов и файлы, помещенные на карантин. Вы можете изменить директорию, заданную по умолчанию. Если указанной директории не существует или она недоступна, приложение использует директорию, заданную по умолчанию. Параметр неприменим для устройств с процессором Эльбрус. Используется параметр `BackupFolder`.	Значение по умолчанию: `/var/opt/kaspersky/kesl/common/objects-backup/` Для доступа к заданной по умолчанию директории требуются root-права.
`BackupFolder`	Путь к директории резервного хранилища. Вы можете изменить директорию, заданную по умолчанию. Если указанной директории не существует или она недоступна, приложение использует директорию, заданную по умолчанию.	Значение по умолчанию: `/var/opt/kaspersky/kesl/common/objects-backup/` Для доступа к заданной по умолчанию директории резервного хранилища требуются root-права.

Параметры проверки сетевого трафика

Параметры проверки сетевого трафика

Параметр	Описание	Значения
`EncryptedConnectionsScan`	Включает или выключает проверку зашифрованных соединений. Для FTP-протокола проверка зашифрованных соединений по умолчанию выключена.	`Yes` (значение по умолчанию) – включить проверку зашифрованных соединений. `No` – выключить проверку зашифрованных соединений. Приложение не расшифровывает зашифрованный трафик.
`EncryptedConnectionsScanErrorAction`	Действие, выполняемое приложением при возникновении ошибки проверки зашифрованных соединений на веб-сайте.	`AddToAutoExclusions` (значение по умолчанию) – добавить домен, на котором возникла ошибка, в список доменов с ошибками проверки. Приложение не будет контролировать зашифрованный сетевой трафик при посещении этого домена. `Disconnect` – заблокировать сетевое соединение.
`CertificateVerificationPolicy`	Задает способ проверки сертификатов приложением Kaspersky Endpoint Security. Если сертификат является самоподписанным, приложение не выполняет дополнительную проверку.	`FullCheck` (значение по умолчанию) – приложение использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата. `LocalCheck` – приложение не использует интернет для проверки сертификата.
`UntrustedCertificateAction`	Действие, выполняемое приложением при обнаружении неподтвержденного сертификата.	`Allow` (значение по умолчанию) – разрешить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом. `Block` – запретить сетевые соединения, установленные при посещении домена с неподтвержденным сертификатом.
`ManageExclusions`	Использование исключений при проверке зашифрованного трафика.	`Yes` – не проверять веб-сайты, указанные в секции `[Exclusions.item_#]` (см. ниже). `No` (значение по умолчанию) – проверять все веб-сайты.

Параметр	Описание	Значения
`MonitorNetworkPorts`	Способ контроля сетевых портов приложением Kaspersky Endpoint Security.	`Selected` (значение по умолчанию) – контролировать только сетевые порты, указанные в секции `[NetworkPorts.item_#]` (см. ниже). `All` – контролировать все сетевые порты. Выбор этого значения может значительно увеличить нагрузку на операционную систему.
`NetInterceptorMode`	Режим перехвата трафика приложением Kaspersky Endpoint Security. Параметр неприменим для устройств с процессором Эльбрус.	`UseEBPF` – использовать для перехвата трафика технологию eBPF. `UseIPTables` (значение по умолчанию) – использовать для перехвата трафика утилиту iptables. Для изменения режима перехвата трафика требуется перезапустить приложение. Во время перезапуска происходит разрыв установленных сетевых соединений.
Секция **[Exclusions.item_#]** содержит домены, исключенные из проверки. Приложение не проверяет соединения, установленные при посещении указанных доменов.		
`DomainName`	Имя домена.	Для указания домена вы можете использовать маски.
Секция **[IncomingEndpointsExclusions.item_#]** содержит исключения для входящего трафика.		
`RemoteIp`	IP-адрес удаленного устройства, трафик с которого исключается из перехвата.	
`DestinationPort`	Порт на защищенном устройстве, трафик на который с удаленных устройств исключается из перехвата.	
Секция **[OutgoingEndpointsExclusions.item_#]** содержит исключения для исходящего трафика.		
`RemoteIp`	IP-адрес удаленного устройства, трафик на который исключается из перехвата.	
`DestinationPort`	Порт на удаленном устройстве, трафик на который с защищенного устройства исключается из перехвата.	
Секция **[NetworkPorts.item_#]** содержит сетевые порты, контролируемые приложением.		
`PortName`	Описание сетевого порта.	
`Port`	Номера сетевых портов, контролируемые приложением.	`1 – 65535`. Значение по умолчанию не задано.

Настройка глобальных исключений

В командной строке вы можете настраивать исключения точек монтирования с помощью параметра `ExcludedMountPoint.item_#` из общих параметров приложения.

Вы можете изменять значение параметра с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `ExcludedMountPoint.item_#` может принимать следующие значения:

- `AllRemoteMounted` – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протоколов SMB и NFS.
- `Mounted:NFS` – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протокола NFS.
- `Mounted:SMB` – исключать из перехвата файловых операций все удаленные директории, смонтированные на устройстве с помощью протокола SMB.
- `Mounted:<file system type>` – исключать из перехвата файловых операций все смонтированные директории с указанным типом файловой системы.
- `/mnt` – исключать из перехвата объекты, находящиеся в точке монтирования /mnt (включая вложенные директории), используемой в качестве временной точки монтирования съемных дисков.
- `<path containing the mask /mnt/user* or /mnt/**/user_share>` – исключать из перехвата объекты, находящиеся в точках монтирования, имена которых содержат указанную маску.

Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды `mount`.

Вы можете указать несколько точек монтирования, которые вы хотите исключить из проверки.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Параметры защиты паролем

Вы можете разрешить или отозвать права на управление приложением, изменяя значения параметров с помощью ключей командной строки или с помощью конфигурационного файла.

Параметры защиты паролем

Параметр	Описание	Значение
`StopProtection`	Выключение компонентов защиты.	`Yes` – разрешить пользователю выполнять действие. `No` – запретить пользователю выполнять действие.
`StopSecurityControl`	Выключение компонентов контроля.	
`StartProtection`	Включение компонентов защиты.	
`StartSecurityControl`	Включение компонентов контроля.	
`ApplicationSettings`	Настройка приложения.	
`ViewReports`	Просмотр отчетов.	
`RestoreFromBackup`	Восстановление из резервного хранилища.	
`RemoveLicenseKey`	Удаление ключа.	
`AddLicense`	Добавление ключа.	
`DisablePolicy`	Выключение политики Kaspersky Security Center.	

Параметры приложения в Консоли администрирования

Вы можете настроить параметры Kaspersky Endpoint Security с помощью политики. Подробная информация о компонентах приложения приведена в соответствующих подразделах.

Обновление баз

В Консоли администрирования вы можете выполнять обновление баз приложения с помощью задачи Обновление.

Вы можете создавать и запускать пользовательские задачи обновления. Вы можете настраивать параметры обновления, изменяя параметры задач.

В свойствах задачи Обновление в разделах **Источники обновлений** и **Параметры** вы можете настроить параметры, приведенные в таблице ниже.

Раздел Источники обновлений задачи Обновление

Параметр	Описание

Источники обновлений	Таблица содержит список источников обновлений баз. В процессе обновления приложение обращается к источникам обновлений в том порядке, в котором они указаны в таблице.
	Таблица содержит следующие столбцы:
	• **Адрес источника** – адрес источника обновлений:
	  • **Серверы обновлений "Лаборатории Касперского"**, на которых публикуются обновления баз для приложений "Лаборатории Касперского" (значение по умолчанию).
	  • **Kaspersky Security Center** – Сервер администрирования Kaspersky Security Center.
	  • Другие источники в локальной или глобальной сети, добавленные пользователем – HTTP-, HTTPS- и FTP-серверы или директории на серверах локальной сети.
	• **Статус** показывает, используется ли источник обновлений в задаче (**Используется** или **Не используется**). Вы можете изменить статус, установив или сняв флажок **Использовать этот источник** в окне **Источник обновлений**, которое открывается при нажатии на кнопку **Изменить**.
	Источники обновлений в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Раздел Параметры задачи Обновление

Параметр	Описание
Максимальное время ожидания ответа от источника обновлений (сек.)	Предельный период ожидания ответа на запрос приложения от выбранного источника обновлений (в секундах). При отсутствии ответа по истечении этого времени в журнал выполнения задач записывается событие о нарушении связи с источником обновлений. Доступные значения: 0–120. Если указано значение 0, период ожидания ответа на запрос приложения от выбранного источника не ограничен. Значение по умолчанию: 10 секунд.
Режим загрузки обновлений	В раскрывающемся списке вы можете выбрать режим загрузки автоматически устанавливаемых обновлений приложения (автопатчей): • **Не загружать**. При выборе этого элемента списка автопатчи автоматически не загружаются. • **Только загружать**. При выборе этого элемента списка автопатчи автоматически загружаются, но не устанавливаются на клиентские устройства (значение по умолчанию). • **Загружать и устанавливать**. При выборе этого элемента списка автопатчи автоматически загружаются и устанавливаются на клиентские устройства. После установки автопатча приложение будет автоматически перезапущено.

Защита устройств от угроз

Защита от файловых угроз

В Консоли администрирования вы можете управлять защитой от файловых угроз в свойствах политики (**Базовая защита → Защита от файловых угроз**).

Параметры компонента Защита от файловых угроз

Параметр	Описание
Включить Защиту от файловых угроз	Флажок включает или выключает компонент Защита от файловых угроз на всех управляемых устройствах. По умолчанию флажок установлен.
Режим Защиты от файловых угроз	В раскрывающемся списке вы можете выбрать режим работы компонента Защита от файловых угроз: • **Интеллектуальный режим** (значение по умолчанию) – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен. Если процесс в течение определенного времени многократно обращается к файлу и изменяет его, приложение повторно проверяет файл только при последнем закрытии файла этим процессом. • **При открытии** – проверять файл при попытке открытия на чтение, исполнение или изменение. • **При открытии и изменении** – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки и параметры проверки.
Действия при обнаружении угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Действия при обнаружении угрозы**, в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно **добавлять**, **изменять**, **удалять**, перемещать **вверх** и **вниз**.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно Новая область проверки

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, приложение проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Как использовать теги

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`

- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

Где:

<id> – идентификатор контейнера.

<name> – имя контейнера.

<path to local directory> – путь к локальной директории.

Также вы можете использовать уникальные комбинации из тегов [container-id:<id>], [container-name:<name>], [image-id:<id>] и [image-name:<name>]/path to local directory>.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- [container-name:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

В названиях и идентификаторах можно использовать маски (символы ? и *).

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы Защиты от файловых угроз.

Параметры Защиты от файловых угроз

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, Kaspersky Endpoint Security проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, включив и настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, Kaspersky Endpoint Security не проверяет архивы. По умолчанию флажок снят.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, Kaspersky Endpoint Security проверяет самораспаковывающиеся архивы. Если флажок снят, Kaspersky Endpoint Security не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок снят.

Параметр	Описание
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, Kaspersky Endpoint Security проверяет файлы почтовых баз. Если флажок снят, Kaspersky Endpoint Security не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, Kaspersky Endpoint Security проверяет сообщения в текстовом формате. Если флажок снят, Kaspersky Endpoint Security не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать текстовые файлы	Временное исключение из проверки файлов в текстовом формате. Если флажок установлен, Kaspersky Endpoint Security не будет проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. Параметр позволяет оптимизировать проверку журналов работы приложений. Если флажок снят, Kaspersky Endpoint Security проверяет текстовые файлы. По умолчанию флажок снят. Параметр применяется, если вы используете механизм перехвата системных событий на основе технологии fanotify. При использовании обновляемого модуля ядра проверка оптимизирована за счет применения кеша результатов проверки.
Пропускать файлы журналов баз данных	Временное исключение из проверки файлы журналов баз данных. Если флажок установлен, приложение не будет проверять файл журнала баз данных, если файл журнала повторно используется тем же процессом в течение 10 минут после последней проверки. Параметр позволяет оптимизировать проверку журналов баз данных. Если флажок снят, приложение проверяет файлы журналов баз данных. По умолчанию флажок снят. Параметр применяется, если вы используете механизм перехвата системных событий на основе технологии fanotify. При использовании обновляемого модуля ядра проверка оптимизирована за счет применения кеша результатов проверки.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени Kaspersky Endpoint Security прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 60.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, Kaspersky Endpoint Security проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, Kaspersky Endpoint Security записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, Kaspersky Endpoint Security не записывает в журнал события типа *ObjectProcessed*. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, Kaspersky Endpoint Security записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, Kaspersky Endpoint Security не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.

Параметр	Описание
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, Kaspersky Endpoint Security записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, Kaspersky Endpoint Security не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, Kaspersky Endpoint Security проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, Kaspersky Endpoint Security проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Окно Действия при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Параметры Защиты от файловых угроз

Параметр	Описание
Действия при обнаружении угрозы	Вы можете выбрать действия, которое приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить; удалять, если лечение невозможно** (значение по умолчанию). При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. • **Лечить; блокировать, если лечение невозможно**. При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение блокирует доступ к зараженному объекту. • **Блокировать**. При выборе этого действия приложение блокирует доступ к зараженному объекту. При лечении и удалении копия зараженного объекта будет помещена в резервное хранилище.

Исключения Защиты от файловых угроз

Исключение из защиты – это совокупность условий, при выполнении которых приложение Kaspersky Endpoint Security не проверяет объекты на наличие вирусов и других вредоносных программ. Вы также можете исключать из защиты объекты по маскам и названиям угроз и настраивать исключения для процессов.

В Консоли администрирования вы можете настроить исключения Защиты от файловых угроз в свойствах политики (**Базовая защита** → **Исключения Защиты от файловых угроз**).

Параметры исключений из проверки

Блок параметров	Описание
Исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Области исключения. В этом окне вы можете задать список областей исключения из проверки.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Исключения по маске. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Исключения по названию угрозы. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Исключения по процессам	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Исключения по процессам. В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Области исключения

Окно содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

По умолчанию таблица областей исключения пуста. Элементы в таблице можно добавлять, изменять и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**.

Окно Новая область исключения

В этом окне вы можете добавить или настроить область исключения из проверки.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Как использовать теги

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Где:

`<id>` – идентификатор контейнера.

`<name>` – имя контейнера.

`<path to local directory>` – путь к локальной директории.

Также вы можете использовать уникальные комбинации из тегов `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` и `[image-name:<name>]/path to local directory>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Вы можете включить объединение списка исключений при наследовании в дочерних политиках. Для объединения элементов списка требуется установить флажок **Объединять значения при наследовании**. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

Вы можете включить объединение списка исключений при наследовании в дочерних политиках. Для объединения элементов списка требуется установить флажок **Объединять значения при наследовании**. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.

Окно Исключения по процессам

Окно содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса и файлов, изменяемых указанным процессом, из проверки. По умолчанию список содержит две области исключения, содержащие пути к Агентам администрирования. Вы можете удалить эти исключения, если требуется.

Параметры области исключения по процессам

Параметр	Описание
Объединять значения при наследовании	Флажок включает или выключает объединение списка при наследовании в дочерних политиках. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**.

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Исключения по процессам**. Поле ввода не должно быть пустым.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки. Если для перехвата системных событий используется обновляемый модуль ядра, указанный процесс исключается из перехвата во всех пространствах имен.
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром **Путь к исключаемому процессу**. По умолчанию флажок снят.
Использовать эту область	Флажок включает или выключает исключение этой области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Путь к изменяемым файлам	Блок параметров позволяет задать исключения из проверки для файлов, которые изменяет процесс. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная** или **Общая**, то в раскрывающемся списке протоколов доступа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски. Поле ввода не должно быть пустым.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в блоке **Путь к изменяемым файлам**. Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Поиск вредоносного ПО

В Консоли администрирования вы можете выполнять проверку на наличие вредоносного ПО с помощью задачи *Поиск вредоносного ПО*.

Вы можете запускать автоматически созданную групповую задачу, а также создавать и запускать пользовательские задачи проверки. Вы можете настраивать параметры проверки, изменяя параметры задач.

В свойствах задачи *Поиск вредоносного ПО* в разделе **Параметры** вы можете настроить параметры, приведенные в таблице ниже.

Параметры задачи Поиск вредоносного ПО

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки, параметры области проверки и параметры проверки.
Действия при обнаружении угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Действия при обнаружении угрозы**, в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

В свойствах задачи *Поиск вредоносного ПО* в разделе **Исключения** вы можете настроить области исключения, исключения по маске и по названию угрозы.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно **добавлять**, **изменять**, **удалять**, перемещать **вверх** и **вниз**.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, приложение проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Как использовать теги

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Где:

`<id>` – идентификатор контейнера.

`<name>` – имя контейнера.

`<path to local directory>` – путь к локальной директории.

Также вы можете использовать уникальные комбинации из тегов `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` и `[image-name:<name>]/path to local directory>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

Окно Параметры области проверки

В этом окне вы можете настроить параметры проверки во время работы задачи Поиск вредоносного ПО. Приложение позволяет проверять файлы, загрузочные секторы, память устройства и объекты автозапуска.

Параметры области проверки

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, приложение проверяет файлы. Если флажок снят, приложение не проверяет файлы. По умолчанию флажок установлен.
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, приложение проверяет загрузочные секторы. Если флажок снят, приложение не проверяет загрузочные секторы. По умолчанию флажок снят.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти устройства. Если флажок установлен, приложение проверяет память ядра и запущенные процессы. Если флажок снят, приложение не проверяет память ядра и запущенные процессы. По умолчанию флажок снят.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, приложение проверяет объекты автозапуска. Если флажок снят, приложение не проверяет объекты автозапуска. По умолчанию флажок снят.
Устройства для проверки	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях, во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области проверки

Таблица содержит маски имен устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять и удалять.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.

Параметр	Описание
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.

Параметр	Описание
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.
Не запускать несколько задач проверки одновременно	Отложенный запуск задач проверки, если проверка уже выполняется. Kaspersky Endpoint Security ставит новые задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, приложение запустило задачу полной проверки по расписанию. Если пользователь пытается запустить быструю проверку в интерфейсе приложения, Kaspersky Endpoint Security поставит задачу быстрой проверки в очередь и автоматически запустит ее после завершения полной проверки. По умолчанию флажок снят.

Окно Действия при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Действия при обнаружении угрозы

Параметр	Описание
Действия при обнаружении угрозы	Вы можете выбрать действия, которые приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить; удалять, если лечение невозможно** (значение по умолчанию). При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. • **Лечить; информировать, если лечение невозможно**. При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), то приложение сохраняет в журнал информацию об этом. • **Информировать**. При выборе этого действия приложение сохраняет в журнале информацию о зараженном объекте.

Раздел Исключения

Исключение из проверки – это совокупность условий, при выполнении которых приложение Kaspersky Endpoint Security не проверяет объекты на наличие вирусов и других вредоносных программ. Вы можете также исключать объекты из проверки по маскам и названиям угроз.

Параметры исключений из проверки

Блок параметров	Описание
Области исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**. В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Исключения по маске. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Исключения по названию угрозы. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Окно Области исключения

Окно содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

По умолчанию таблица областей исключения пуста. Элементы в таблице можно добавлять, изменять и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**.

Окно Новая область исключения

В этом окне вы можете добавить или настроить область исключения из проверки.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Как использовать теги

Вы можете использовать специальные теги для указания контейнера или образа:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Где:

`<id>` – идентификатор контейнера.

`<name>` – имя контейнера.

`<path to local directory>` – путь к локальной директории.

Также вы можете использовать уникальные комбинации из тегов `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` и `[image-name:<name>]/path to local directory>`.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`

- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

В названиях и идентификаторах можно использовать маски (символы `?` и `*`).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

Проверка важных областей

В Консоли администрирования вы можете выполнять проверку важных областей операционной системы защищаемого устройства с помощью задачи *Проверка важных областей*.

Вы можете создавать и запускать пользовательские задачи проверки важных областей. Вы можете настраивать параметры проверки, изменяя параметры задач.

В свойствах задачи *Проверка важных областей* в разделе **Параметры** вы можете настроить параметры, приведенные в таблице ниже.

Параметры задачи Проверка важных областей

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки, параметры области проверки и параметры проверки.
Действия при обнаружении угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Действия при обнаружении угрозы**, в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

В свойствах задачи *Проверка важных областей* в разделе **Исключения** вы можете настроить области исключения, исключения по маске и по названию угрозы.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно **добавлять**, **изменять**, **удалять**, перемещать **вверх** и **вниз**.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно Новая область проверки

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна Области проверки. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски и теги. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, приложение проверяет все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область проверки. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Как использовать теги

Вы можете использовать специальные теги для указания контейнера или образа:

- [container-id:<id>]/<path to local directory>
- [container-name:<name>]/<path to local directory>
- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

Где:

<id> – идентификатор контейнера.

<name> – имя контейнера.

<path to local directory> – путь к локальной директории.

Также вы можете использовать уникальные комбинации из тегов [container-id:<id>], [container-name:<name>], [image-id:<id>] и [image-name:<name>]/path to local directory>.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- [container-name:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

В названиях и идентификаторах можно использовать маски (символы ? и *).

Окно Параметры области проверки

В этом окне вы можете настроить параметры проверки во время работы задачи Проверка важных областей. Приложение позволяет проверять файлы, загрузочные секторы, объекты автозапуска, память процесса и память ядра.

Параметры области проверки

Параметр	Описание
Проверять файлы	Флажок включает или выключает проверку файлов. Если флажок установлен, Kaspersky Endpoint Security проверяет файлы. Если флажок снят, Kaspersky Endpoint Security не проверяет файлы. По умолчанию флажок снят.

Параметр	Описание
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, Kaspersky Endpoint Security проверяет загрузочные секторы. Если флажок снят, Kaspersky Endpoint Security не проверяет загрузочные секторы. По умолчанию флажок установлен.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти устройства. Если флажок установлен, Kaspersky Endpoint Security проверяет память ядра и запущенные процессы. Если флажок снят, Kaspersky Endpoint Security не проверяет память ядра и запущенные процессы. По умолчанию флажок установлен.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, Kaspersky Endpoint Security проверяет объекты автозапуска. Если флажок снят, Kaspersky Endpoint Security не проверяет объекты автозапуска. По умолчанию флажок установлен.
Устройства для проверки	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях, во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области проверки

Таблица содержит маски имен устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять и удалять.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок установлен.

Параметр	Описание
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.
Не запускать несколько задач проверки одновременно	Отложенный запуск задач проверки, если проверка уже выполняется. Kaspersky Endpoint Security ставит новые задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, приложение запустило задачу полной проверки по расписанию. Если пользователь пытается запустить быструю проверку в интерфейсе приложения, Kaspersky Endpoint Security поставит задачу быстрой проверки в очередь и автоматически запустит ее после завершения полной проверки. По умолчанию флажок снят.

Окно Действия при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Действия при обнаружении угрозы

Параметр	Описание
Действия при обнаружении угрозы	Вы можете выбрать действия, которые приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить; удалять, если лечение невозможно** (значение по умолчанию). При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. • **Лечить; информировать, если лечение невозможно**. При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), то приложение сохраняет в журнал информацию об этом. • **Информировать**. При выборе этого действия приложение сохраняет в журнале информацию о зараженном объекте.

Раздел Исключения

Исключение из проверки – это совокупность условий, при выполнении которых приложение Kaspersky Endpoint Security не проверяет объекты на наличие вирусов и других вредоносных программ. Вы можете также исключать объекты из проверки по маскам и названиям угроз.

Параметры исключений из проверки

Блок параметров	Описание
Области исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**. В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Окно Области исключения

Окно содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

По умолчанию таблица областей исключения пуста. Элементы в таблице можно добавлять, изменять и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**.

Окно Новая область исключения

В этом окне вы можете добавить или настроить область исключения из проверки.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательский** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ ? вместо любого одного символа в имени файла или директории.

Как использовать теги

Вы можете использовать специальные теги для указания контейнера или образа:

- [container-id:<id>]/<path to local directory>
- [container-name:<name>]/<path to local directory>
- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

Где:

<id> – идентификатор контейнера.

<name> – имя контейнера.

<path to local directory> – путь к локальной директории.

Также вы можете использовать уникальные комбинации из тегов [container-id:<id>], [container-name:<name>], [image-id:<id>] и [image-name:<name>]/path to local directory>.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- [container-name:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

В названиях и идентификаторах можно использовать маски (символы ? и *).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

Мониторинг контейнеров

В Консоли администрирования вы можете управлять работой компонента Мониторинг контейнеров в свойствах политики (**Общие параметры** → **Параметры проверки контейнеров**).

Параметры мониторинга контейнеров

Параметр	Описание
Включить проверку пространств имен и контейнеров	Флажок включает или выключает проверку пространств имен и контейнеров в реальном времени. По умолчанию флажок установлен.
Действие с контейнером при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта: • **Пропустить контейнер** – при обнаружении зараженного объекта приложение не выполняет никаких действий над контейнером. • **Остановить контейнер** – при обнаружении зараженного объекта приложение останавливает контейнер. • **Остановить, если не удалось вылечить** (значение по умолчанию) – если не удалось вылечить зараженный объект, приложение останавливает контейнер. Этот параметр доступен при использовании приложения по лицензии, которая включает эту функцию.
Параметры проверки контейнеров	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Параметры проверки контейнеров.

Окно Параметры проверки контейнеров

В этом окне вы можете настроить параметры интеграции приложения Kaspersky Endpoint Security с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Параметры проверки контейнеров

Параметр	Описание
Использовать Docker	Флажок включает или выключает использование системы управления контейнерами Docker. По умолчанию флажок установлен.
Путь Docker-сокета	Поле ввода пути или URI (универсальный идентификатор ресурса) Docker-сокета. Значение по умолчанию: /var/run/docker.sock.
Использовать CRI-O	Флажок включает или выключает использование среды CRI-O. По умолчанию флажок установлен.

Параметр	Описание
Путь к файлу	Поле ввода пути к конфигурационному файлу CRI-O. Значение по умолчанию: /etc/crio/crio.conf.
Использовать Podman	Флажок включает или выключает использование утилиты Podman. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты Podman. Значение по умолчанию: /usr/bin/podman
Корневая директория	Поле ввода пути к корневой директории хранилища контейнеров. Значение по умолчанию: /var/lib/containers/storage
Использовать runc	Флажок включает или выключает использование утилиты runc. По умолчанию флажок установлен.
Путь к файлу	Поле ввода пути к исполняемому файлу утилиты runc. Значение по умолчанию: /usr/bin/runc
Корневая директория	Поле ввода пути к корневой директории хранилища состояний контейнеров. Значение по умолчанию: /run/runc.

Проверка контейнеров

В Консоли администрирования вы можете выполнять проверку контейнеров и образов с помощью задачи *Проверка контейнеров*.

Вы можете создавать и запускать пользовательские задачи проверки контейнеров. Вы можете настраивать параметры проверки, изменяя параметры задач.

В свойствах задачи *Проверка контейнеров* в разделе **Параметры** вы можете настроить параметры, приведенные в таблице ниже.

Параметры задачи Проверка контейнеров

Параметр	Описание
Проверка	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить параметры проверки контейнеров и общие параметры проверки.
Действия при обнаружении угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Действия при обнаружении угрозы**, в котором вы можете настроить действия, которые приложение будет выполнять над обнаруженным зараженным объектом.

В свойствах задачи *Проверка контейнеров* в разделе **Исключения** вы также можете настроить исключения по маске и по названию угрозы.

Окно Параметры проверки контейнеров

В этом окне вы можете настроить параметры проверки контейнеров и образов.

Параметры проверки контейнеров и образов

Параметр	Описание
Проверять контейнеры	Флажок включает или выключает проверку контейнеров. Если флажок установлен, вы можете указать имя или маску имени проверяемых контейнеров. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых контейнеров. По умолчанию указана маска * – выполняется проверка всех контейнеров.

Параметр	Описание
Действие при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта: • **Пропустить контейнер** – не выполнять никаких действий над контейнером при обнаружении зараженного объекта. • **Остановить контейнер** – остановить контейнер при обнаружении зараженного объекта. • **Остановить, если не удалось вылечить** (значение по умолчанию) – остановить контейнер, если не удалось вылечить зараженный объект или устранить угрозу. Из-за особенностей работы среды CRI-O зараженный объект не лечится и не удаляется в контейнере в среде CRI-O. Рекомендуется выбирать действие **Остановить контейнер**.
Проверять образы	Флажок включает или выключает проверку образов. Если флажок установлен, вы можете указать имя или маску имени проверяемых образов. По умолчанию флажок установлен.
Маска имени	Поле ввода имени или маски имени проверяемых образов. По умолчанию указана маска * – выполняется проверка всех образов.
Действие при обнаружении угрозы	В раскрывающемся списке вы можете выбрать действие, которое приложение будет выполнять над образом при обнаружении зараженного объекта: • **Пропустить образ** (значение по умолчанию) – не выполнять никаких действий над образом при обнаружении зараженного объекта. • **Удалить образ** при обнаружении зараженного объекта (не рекомендуется). Все зависимые объекты также будут удалены. Запущенные контейнеры будут остановлены, а затем удалены.
Проверять каждый слой	Флажок включает или выключает проверку всех слоев образов и запущенных контейнеров. По умолчанию флажок снят.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.

Параметр	Описание
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.
Не запускать несколько задач проверки одновременно	Отложенный запуск задач проверки, если проверка уже выполняется. Kaspersky Endpoint Security ставит новые задачи проверки в очередь, если текущая проверка еще продолжается. Это позволяет оптимизировать нагрузку на компьютер. Например, приложение запустило задачу полной проверки по расписанию. Если пользователь пытается запустить быструю проверку в интерфейсе приложения, Kaspersky Endpoint Security поставит задачу быстрой проверки в очередь и автоматически запустит ее после завершения полной проверки. По умолчанию флажок снят.

Окно Действия при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Endpoint Security будет выполнять над обнаруженным зараженным объектом.

Действия при обнаружении угрозы

Параметр	Описание
Действия при обнаружении угрозы	Вы можете выбрать действия, которые приложение будет выполнять над обнаруженным зараженным объектом: • **Лечить; удалять, если лечение невозможно** (значение по умолчанию). При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. • **Лечить; информировать, если лечение невозможно**. При выборе этого действия приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), то приложение сохраняет в журнал информацию об этом. • **Информировать**. При выборе этого действия приложение сохраняет в журнале информацию о зараженном объекте.

Раздел Исключения

Параметры исключений из проверки

Блок параметров	Описание
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Исключения по названию угрозы	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях, во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

Проверка съемных дисков

В Консоли администрирования вы можете настраивать параметры проверки съемных дисков в свойствах политики (**Локальные задачи** → **Проверка съемных дисков**).

Параметры компонента Проверка съемных дисков

Параметр	Описание
Включить проверку съемных дисков при подключении к устройству	Флажок включает или выключает проверку съемных дисков при подключении их к устройству пользователя. По умолчанию флажок снят.
Действие при подключении съемного диска	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять приложение при подключении съемных дисков к устройству пользователя: • **Не проверять** съемные диски при подключении (значение по умолчанию). • **Быстрая проверка** – проверять на съемных дисках (за исключением CD/DVD-приводов и дисков Blu-ray) только файлы определенных типов и не распаковывать составные объекты. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Проверка важных областей*. • **Подробная проверка** – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и дисков Blu-ray). Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Поиск вредоносного ПО*.
Действие при подключении CD/DVD-привода	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять приложение при подключении CD/DVD-приводов и дисков Blu-ray к устройству пользователя: • **Не проверять** CD/DVD-приводы и диски Blu-ray при подключении (значение по умолчанию). • **Быстрая проверка** – проверять на CD/DVD-приводах и дисках Blu-ray только файлы определенных типов. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Проверка важных областей*. • **Подробная проверка** – проверять все файлы на CD/DVD-приводах и дисках Blu-ray. Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Поиск вредоносного ПО*.
Блокировать доступ к съемному диску во время проверки	Флажок включает или выключает блокировку файлов на подключенном диске во время выполнения проверки. По умолчанию флажок снят.

Полезные статьи

Типы файлов для быстрой проверки

На съемных дисках проверяются файлы следующих форматов: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx.

Анализ поведения

В Консоли администрирования вы можете настраивать параметры анализа поведения приложений в свойствах политики (**Продвинутая защита** → **Анализ поведения**).

Параметры компонента Анализ поведения

Параметр	Описание
Включить Анализ поведения	Флажок включает или выключает компонент Анализ поведения. По умолчанию флажок установлен.
Действие при обнаружении вредоносной активности	Действие, которое Kaspersky Endpoint Security будет выполнять при обнаружении вредоносной активности в операционной системе: • **Блокировать** приложение, осуществляющее вредоносную активность (значение по умолчанию). Kaspersky Endpoint Security завершает процесс, осуществляющий вредоносную активность, и записывает в журнал событий информацию об обнаруженной вредоносной активности. • **Информировать** пользователя. Kaspersky Endpoint Security не завершает процесс, осуществляющий вредоносную активность, только записывает событие об обнаружении вредоносной активности в журнал событий.
Использовать исключения по процессам	Флажок включает или выключает использование исключений по процессам в работе компонента Анализ поведения. По умолчанию флажок снят. По кнопке **Настроить** открывается окно **Исключения по процессам**. В этом окне вы можете настроить исключение активности процессов из проверки.

Окно Исключения по процессам

Окно содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса из проверки.

Параметры области исключения по процессам

Параметр	Описание
Объединять значения при наследовании	Флажок включает или выключает объединение списка при наследовании в дочерних политиках. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

По умолчанию таблица областей исключения пуста. Элементы в таблице можно добавлять, изменять и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**.

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Исключения по процессам**.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки. Для указания пути вы можете использовать маски. Поле ввода не должно быть пустым.

Параметр	Описание
Применять к дочерним процессам	Исключение из проверки дочерних процессов исключаемого процесса, указанного параметром **Путь к исключаемому процессу**. По умолчанию флажок снят.
Использовать эту область	Флажок включает или выключает исключение этой области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область во время работы. Если флажок снят, приложение включает эту область во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Исключать процесс из проверки компонентом Анализ поведения	Флажок включает или выключает исключение процесса из проверки при работе компонента Анализ поведения. По умолчанию флажок снят.
Исключать процесс из телеметрии MDR и EDR Expert (on-premises)	Флажок включает или выключает исключение процесса из телеметрии, которую собирают компоненты MDR и EDR Expert (on-premises). По умолчанию флажок снят.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Защита от эксплойтов

В Консоли администрирования вы можете настраивать параметры защиты от эксплойтов в свойствах политики (**Продвинутая защита** → **Анализ поведения**).

Параметры компонента Защита от эксплойтов

Параметр	Описание
Включить Защиту от эксплойтов	Флажок включает или выключает компонент Защита от эксплойтов. По умолчанию флажок снят.
Защита от эксплойтов	По кнопке **Настроить** открывается окно Исключения Защиты от эксплойтов, в котором вы можете настроить исключения из проверки для компонента Защита от эксплойтов.
Действие при обнаружении эксплойта	Действие, которое приложение будет выполнять при обнаружении эксплойта: • **Блокировать** (значение по умолчанию). Приложение блокирует вредоносные действия эксплойта и записывает в журнал событий информацию об этом. • **Информировать**. Приложение не блокирует действия эксплойта, а только записывает в журнал событий информацию об обнаружении эксплойта.

Окно Исключения Защиты от эксплойтов

В этом окне вы можете настроить исключение объектов из проверки Защитой от эксплойтов. Приложение не будет проверять указанные объекты. По умолчанию список объектов пуст.

Параметры исключений Защиты от эксплойтов

Параметр	Описание
Объединять значения при наследовании	Флажок включает или выключает объединение списка при наследовании в дочерних политиках. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.
Статус	Статус показывает, используется ли это исключение в работе приложения.
Название угрозы	Название угрозы, исключаемой из проверки.
Путь к файлу или директории	Полный путь к файлу или директории, исключенным из проверки.
Хеш-сумма файла	Хеш-сумма файла, исключенного из проверки.
Комментарий	Комментарий, относящийся к исключению из проверки.

По умолчанию таблица исключения пуста. Элементы в таблице можно добавлять, изменять и удалять.

Окно Исключение Защиты от эксплойтов

В этом окне вы можете добавить или настроить исключение из проверки компонентом Защита от эксплойтов.

Параметры исключения Защиты от эксплойтов

Параметр	Описание
Использовать название угрозы	Флажок включает или выключает использование исключения из проверки объекта по названию обнаруженной в объекте угрозы. По умолчанию флажок установлен.
Название угрозы	Поле ввода названия обнаруженной в объекте угрозы. Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным. Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com . Поле доступно, если установлен флажок **Использовать название угрозы**.
Использовать хеш-сумму файла	Флажок включает или выключает использование исключения из проверки файла по его хеш-сумме. По умолчанию флажок установлен.
Тип хеш-суммы файла	В раскрывающемся списке вы можете выбрать тип хеш-суммы файла, по которой вы хотите исключить файл из проверки: • **MD5**. • **SHA256**. Раскрывающийся список доступен, если установлен флажок **Использовать хеш-сумму файла**.
Хеш-сумма файла	Поле ввода хеш-суммы файла, по которой вы хотите исключить файл из проверки. Поле доступно, если установлен флажок **Использовать хеш-сумму файла**.
Использовать путь к файлу или директории	Флажок включает или выключает использование исключения из проверки файла, в котором обнаружена угроза, по пути к нему. По умолчанию флажок установлен.
Путь к файлу или директории	Поле ввода пути к файлу или директории, которые вы хотите исключить из проверки. Для указания пути вы можете использовать символы * и ?. Поле доступно, если установлен флажок **Использовать путь к файлу или директории**.

Параметр	Описание
Комментарий	Поле ввода комментария (необязательное).
Использовать это исключение	Флажок включает или выключает использование этого исключения во время работы приложения. По умолчанию флажок установлен.

Защита от шифрования

В Консоли администрирования вы можете настраивать параметры защиты от шифрования в свойствах политики (**Продвинутая защита** → **Защита от шифрования**).

Параметры компонента Защита от шифрования

Параметр	Описание
Включить Защиту от шифрования	Флажок включает или выключает защиту файлов в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования. По умолчанию флажок снят.
Области защиты	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить области проверки и параметры защиты.
Исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области исключения**. В этом окне вы можете задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы.

Параметры области проверки

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно **добавлять**, **изменять**, **удалять**, перемещать **вверх** и **вниз**.

При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.

Kaspersky Endpoint Security будет проверять объекты в указанных областях в том порядке, в каком эти области перечислены в таблице областей проверки. Если вы хотите задать параметры безопасности для дочерней директории, отличные от параметров безопасности родительской директории, вам нужно разместить дочернюю директорию в таблице выше, чем родительскую.

Кнопка доступна, если в таблице выбрана область.

При нажатии на кнопку **Удалить** выбранная область исключается из проверки.

Кнопка доступна, если в таблице выбрана хотя бы одна область проверки.

Изменение параметров выбранного элемента выполняется в отдельном окне.

При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно Новая область проверки

В этом окне можно добавить или настроить область защиты компонента Защита от шифрования.

Параметры области защиты

Параметр	Описание
Название области	Поле ввода названия области защиты. Это название будет отображаться в таблице окна Области проверки. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область защиты во время работы компонента. Если флажок снят, приложение не обрабатывает эту область защиты во время работы компонента. В дальнейшем вы можете включить эту область в параметры работы компонента, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** – локальные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все общие** (значение по умолчанию) – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область защиты. Для указания пути вы можете использовать маски. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы компонента Защита от шифрования. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Окно Параметры защиты

Параметры защиты

Параметр	Описание
Действие при обнаружении шифрования	Действие, которое Kaspersky Endpoint Security будет выполнять при обнаружении вредоносного шифрования: • **Информировать** пользователя. Kaspersky Endpoint Security не блокирует устройство, осуществляющее шифрование, только записывает событие об обнаружении вредоносного шифрования в журнал событий. • **Блокировать** устройство, осуществляющее шифрование (значение по умолчанию).
Блокировать недоверенное устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки недоверенного устройства в минутах. По истечении указанного времени приложение Kaspersky Endpoint Security удаляет недоверенные устройства из списка заблокированных. Доступ устройства к сетевым файловым ресурсам восстанавливается автоматически после его удаления из списка недоверенных устройств. Изменение параметра не влияет на длительность блокировки ранее заблокированных скомпрометированных устройств. Длительность блокировки не является динамическим значением и рассчитывается в момент блокировки. Доступные значения: целые числа от 1 до 2147483647. Значение по умолчанию: 30.

Окно Области исключения

Окно содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

По умолчанию таблица областей исключения пуста. Элементы в таблице можно добавлять, изменять и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**.

Окно Новая область исключения

- В этом окне вы можете добавить или настроить область исключения из проверки.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы приложения. Если флажок установлен, приложение исключает эту область из проверки во время работы. Если флажок снят, приложение включает эту область в проверку во время работы. В дальнейшем вы можете исключить эту область, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область исключения. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, исключаемые из проверки: • **Локальная** – локальные директории. • **Смонтированная** – смонтированные директории. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски и теги. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в область исключения. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле ввода пути. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Как использовать теги

Вы можете использовать специальные теги для указания контейнера или образа:

- [container-id:<id>]/<path to local directory>
- [container-name:<name>]/<path to local directory>
- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

Где:

<id> – идентификатор контейнера.

<name> – имя контейнера.

<path to local directory> – путь к локальной директории.

Также вы можете использовать уникальные комбинации из тегов [container-id:<id>], [container-name:<name>], [image-id:<id>] и [image-name:<name>]/path to local directory>.

Возможна любая комбинация из уникальных тегов в количестве от 1 до 4 в рамках одной области. Порядок указания не важен.

Например:

- [container-name:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

В названиях и идентификаторах можно использовать маски (символы ? и *).

Окно Исключения по маске

Вы можете настроить исключение объектов из проверки по маске имени. Приложение не будет проверять файлы, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Вы можете включить объединение списка исключений при наследовании в дочерних политиках. Для объединения элементов списка требуется установить флажок **Объединять значения при наследовании**. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.

Kaspersky Security Network

В Консоли администрирования вы можете настраивать использование Kaspersky Security Network в работе приложения Kaspersky Endpoint Security в свойствах политики (**Продвинутая защита** → **Kaspersky Security Network**).

Текст Положения о Kaspersky Security Network вы можете прочитать в окне **Положение о Kaspersky Security Network**, которое можно открыть по ссылке **Положение о Kaspersky Security Network**.

Информация о доступности KSN отображается в Kaspersky Security Center с помощью статуса клиентского устройства (*OK, Критический, Предупреждение*) в списке управляемых устройств на вкладке **Устройства**.

Параметры использования Kaspersky Security Network

Параметр	Описание
Положение о Kaspersky Security Network	По ссылке открывается окно **Положение о Kaspersky Security Network**. В этом окне вы можете просмотреть текст Положения о Kaspersky Security Network.
Kaspersky Security Network (KSN)	В блоке отображается информация о режиме использования KSN или о том, что KSN не используется в работе Kaspersky Endpoint Security. По кнопке **Изменить** открывается окно, в котором вы можете настроить использование Kaspersky Security Network.
Включить облачный режим	*Облачный режим* – режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию антивирусных баз, что позволяет снизить нагрузку на оперативную память компьютера примерно в два раза. Флажок доступен, если включено использование KSN. Флажок установлен, если при создании политики вы приняли условия Положения о Kaspersky Security Network и используете расширенный режим KSN. Режим включается или выключается после следующего обновления баз приложения. Параметр применяется, только если приложение используется в стандартном режиме.
Использовать Сервер администрирования как прокси-сервер KSN	Если флажок установлен, приложение Kaspersky Endpoint Security взаимодействует с серверами KSN с помощью службы прокси-сервера KSN на Сервере администрирования. По умолчанию флажок установлен. Параметр применяется, только если приложение используется в стандартном режиме. В режиме Легкого агента приложение может взаимодействовать с инфраструктурой KSN только с помощью прокси-сервера KSN.

Параметр	Описание
Использовать серверы KSN, если прокси-сервер KSN недоступен	Если флажок установлен, приложение Kaspersky Endpoint Security взаимодействует с серверами KSN напрямую, когда служба прокси-сервера KSN недоступна. По умолчанию флажок установлен. Флажок доступен, если установлен флажок **Использовать Сервер администрирования как прокси-сервер KSN**. Параметр применяется, только если приложение используется в стандартном режиме.

Параметры Kaspersky Security Network

В этом окне вы можете настроить параметры использования Kaspersky Security Network.

Параметры Kaspersky Security Network

Параметр	Описание
Подробнее	По ссылке открывается веб-сайт "Лаборатории Касперского".
Не использовать Kaspersky Security Network	Выбирая этот вариант, вы отказываетесь от использования Kaspersky Security Network.
Стандартный режим KSN	Выбирая этот вариант, вы принимаете условия использования Kaspersky Security Network. Вы можете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения.
Расширенный режим KSN	Выбирая этот вариант, вы принимаете условия использования Kaspersky Security Network. Вы можете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Кроме того, для улучшения работы Kaspersky Security Network в "Лабораторию Касперского" будет отправляться анонимная статистика и данные о типах и источниках различных угроз.
Положение о Kaspersky Security Network	По ссылке открывается окно Положение о Kaspersky Security Network, в котором вы можете прочитать текст Положения о Kaspersky Security Network.

Положение о Kaspersky Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Security Network и принять его условия.

Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите использовать Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Security Network. Вариант доступен, если в окне Параметры Kaspersky Security Network вы выбрали вариант **Стандартный режим KSN** или **Расширенный режим KSN**.
Я не принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите использовать Kaspersky Security Network. Вариант доступен, если в окне Параметры Kaspersky Security Network вы выбрали вариант **Стандартный режим KSN** или **Расширенный режим KSN**.

Положение о Kaspersky Private Security Network

В этом окне вы можете прочитать текст Положения о Kaspersky Private Security Network и принять его условия.

Параметры Kaspersky Security Network

Параметр	Описание
Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что хотите использовать Kaspersky Security Network и полностью прочитали, поняли и принимаете условия Положения о Kaspersky Private Security Network.
Я не принимаю условия Положения о Kaspersky Security Network	Выбирая этот вариант, вы подтверждаете, что вы не хотите использовать Kaspersky Security Network.

Защита от атак BadUSB

В Консоли администрирования вы можете настраивать параметры защиты от веб-угроз в свойствах политики (**Базовая защита** → **Защита от атак BadUSB**).

Параметры компонента Защита от атак BadUSB

Параметр	Описание
Включить защиту от атак BadUSB	Флажок включает или выключает компонент Защита от атак BadUSB. По умолчанию компонент выключен.
Максимальное количество попыток авторизации USB-устройства	Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Endpoint Security покажет время блокировки USB-устройства. По истечении указанного времени вам будут снова доступны 5 попыток ввода кода авторизации.
Блокировка устройства при достижении максимального количества попыток авторизации (мин.)	Время блокировки USB-устройства после заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).
Запретить использование экранной клавиатуры для авторизации USB-устройств	Если переключатель включен, приложение запрещает использование экранной клавиатуры для авторизации USB-устройства, с которого невозможно ввести код авторизации.
Запретить использование штрихкода для авторизации USB-устройств	Если переключатель включен, приложение запрещает использование штрихкода для авторизации USB-устройства, с которого невозможно ввести код авторизации.

Защита сетевых соединений и средств коммуникации

Защита от почтовых угроз

В Консоли администрирования вы можете настраивать параметры защиты от веб-угроз в свойствах политики (**Базовая защита** → **Защита от почтовых угроз**).

Параметры компонента Защита от почтовых угроз

Параметр	Описание
Защита от почтовых угроз	Флажок включает или выключает компонент Защита от почтовых угроз. По умолчанию компонент включен.
Настроить (Параметры защиты)	По нажатию на кнопку открывается окно **Параметры Защиты от почтовых угроз**, в котором вы можете настроить область защиты от почтовых угроз и параметры проверки составных файлов.
Настроить (Фильтр вложений)	По нажатию на кнопку открывается окно **Фильтр вложений**, в котором вы можете настроить фильтрацию почтовых вложений.

Параметр	Описание
Использовать эвристический анализатор **Уровень эвристического анализа**	Флажок включает или выключает использование эвристического анализатора. 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. По умолчанию использование эвристического анализатора включено с выбранным средним уровнем эвристического анализа.
Действия при обнаружении угрозы	Действие, которое выполняет Защита от почтовых угроз при обнаружении угрозы в почтовых сообщениях: • **Лечить; удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.Действие выбрано по умолчанию. • **Лечить; блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением • **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. Параметр не применим к исходящим сообщениям. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения.

Окно Параметры защиты от почтовых угроз

В этом окне вы можете настроить область защиты от почтовых угроз и параметры проверки составных файлов.

Параметры защиты от почтовых угроз

Параметр	Описание
Область защиты	*Область защиты* – это объекты, которые проверяет компонент во время своей работы: входящие и исходящие сообщения или только входящие сообщения. По умолчанию выбран вариант **Входящие и исходящие сообщения**.
Проверять вложенные архивы	Включает и выключает проверку вложенных архивов. Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива). По умолчанию флажок установлен.
Проверять вложенные файлы офисных приложений	Включает или выключает проверку вложенных файлов офисных форматов. Приложение проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка. По умолчанию флажок установлен.
Не проверять архивы размером более (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. По умолчанию флажок снят.
Ограничивать время проверки архивов до (сек.)	Если флажок установлен, то время проверки архивов, вложенных в сообщения электронной почты, ограничено указанным периодом. По умолчанию флажок снят.

Окно Фильтр вложений

В этом окне вы можете настроить фильтрацию почтовых вложений.

Параметры фильтрации вложений

Параметр	Описание
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. Выбрано по умолчанию.
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.
Объединять значения при наследовании	Флажок включает или выключает объединение списка при наследовании в дочерних политиках. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.
Таблица типов вложений	В таблице отображены типы вложений, которые нужно переименовывать или удалять из сообщений электронной почты. Вы можете добавлять, изменять и удалять типы вложений с помощью одноименных кнопок.

Защита от веб-угроз

В Консоли администрирования вы можете настраивать параметры защиты от веб-угроз в свойствах политики (**Базовая защита** → **Защита от веб-угроз**).

Параметры компонента Защита от веб-угроз

Параметр	Описание
Включить Защиту от веб-угроз	Флажок включает или выключает компонент Защита от веб-угроз. По умолчанию флажок снят.
Доверенные веб-адреса	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные веб-адреса**, в котором вы можете указать список доверенных веб-адресов. Приложение не проверяет содержание веб-сайтов, веб-адреса которых указаны в этом списке.
Действие при обнаружении угрозы	Действие, которое приложение будет выполнять над веб-ресурсом, на котором обнаружен опасный объект: • **Блокировать** доступ ко всем опасным объектам, обнаруженным в веб-трафике, показывать уведомление о заблокированных попытках доступа и записывать в журнал информацию об опасных объектах (значение по умолчанию). • **Информировать** пользователя при обнаружении опасного объекта в веб-трафике. Защита от веб-угроз позволяет выполнить загрузку объекта на устройство. При этом приложение записывает в журнал и добавляет в список активных угроз информацию об опасном объекте.
Параметры проверки	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Параметры проверки**, в котором вы можете настроить параметры проверки входящего трафика.

Окно Доверенные веб-адреса

В этом окне вы можете добавить веб-адреса и веб-страницы, содержимое которых вы считаете доверенным.

В список доверенных веб-адресов вы можете добавлять только веб-адреса HTTP / HTTPS. Для указания веб-адресов вы можете использовать маски. Использование масок для указания IP-адресов не поддерживается. По умолчанию список пустой. Вы можете добавлять, изменять и удалять веб-адреса в списке.

Полезные статьи

Как задавать маски

При создании маски адреса вы можете использовать символ звездочка (*) вместо одного или нескольких символов. Так, если вы укажете маску адреса *abc*, она будет применена ко всем веб-ресурсам, содержащим последовательность abc (например, www.virus.com/download_virus/page_0-9abcdef.html). Чтобы включить звездочку в маску адреса в качестве символа, а не в качестве маски, введите символ * дважды (например, маска www.virus.com/**/page_0-9abcdef.html означает www.virus.com/*/page_0-9abcdef.html).

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки входящего трафика во время работы компонента Защита от веб-угроз.

Параметры Защиты от веб-угроз

Параметр	Описание
Обнаруживать вредоносные объекты	Флажок включает или выключает проверку ссылок по базе вредоносных веб-адресов. По умолчанию флажок установлен.
Обнаруживать фишинговые ссылки	Флажок включает или выключает проверку ссылок по базе фишинговых веб-адресов. По умолчанию флажок установлен.
Использовать эвристический анализ для обнаружения фишинговых ссылок	Флажок включает или выключает использование эвристического анализа для обнаружения фишинговых ссылок. Флажок доступен и установлен по умолчанию, если установлен флажок **Обнаруживать фишинговые ссылки**.
Обнаруживать рекламные приложения	Флажок включает или выключает проверку ссылок по базе рекламных веб-адресов. По умолчанию флажок снят.
Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным	Флажок включает или выключает проверку ссылок по базе легальных приложений, которые могут использоваться злоумышленниками для нанесения вреда устройствам или данным. По умолчанию флажок снят.

Защита от сетевых угроз

Консоли администрирования вы можете настраивать параметры защиты от сетевых угроз в свойствах политики (**Базовая защита** → **Защита от сетевых угроз**).

Параметры компонента Защита от сетевых угроз

Параметр	Описание
Включить Защиту от сетевых угроз	Флажок включает или выключает компонент Защита от сетевых угроз. По умолчанию флажок снят.
Действие при обнаружении угрозы	Действия, выполняемые при обнаружении сетевой активности, характерной для сетевых атак: • **Информировать** пользователя. Приложение разрешает сетевую активность и записывает в журнал информацию об обнаруженной сетевой активности. • **Блокировать** сетевую активность со стороны атакующего устройства и записывать в журнал информацию об обнаруженной сетевой активности (значение по умолчанию).
Блокировать атакующие устройства	Флажок включает или выключает блокировку сетевой активности при обнаружении попытки сетевой атаки. По умолчанию флажок установлен.

Параметр	Описание
Блокировать атакующее устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки атакующего устройства в минутах. По истечении указанного времени приложение Kaspersky Endpoint Security разрешает сетевую активность со стороны этого устройства. Доступные значения: целые числа от 1 до 32768. Значение по умолчанию: 60.
Исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения**, в котором вы можете указать список IP-адресов, сетевые атаки с которых не будут заблокированы.

Окно Исключения

В этом окне вы можете добавить IP-адреса, сетевые атаки с которых не будут заблокированы.

По умолчанию список пустой.

Вы можете добавлять, изменять и удалять IP-адреса в списке. Вы можете указывать IP-адреса в форматах IPv4 и IPv6.

Управление сетевым экраном

В Консоли администрирования вы можете настраивать параметры управления сетевым экраном в свойствах политики (**Базовая защита** → **Управление сетевым экраном**).

Параметры компонента Управление сетевым экраном

Параметр	Описание
Включить Управление сетевым экраном	Флажок включает или выключает компонент Управление сетевым экраном. По умолчанию флажок снят.
Сетевые пакетные правила	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Сетевые пакетные правила**. В этом окне вы можете настроить сетевые пакетные правила, которые будет применять компонент Управление сетевым экраном при обнаружении попытки установления сетевого соединения.
Доступные сети	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доступные сети**. В этом окне вы можете настроить список сетей, которые будет контролировать компонент Управление сетевым экраном.
Входящие соединения	В раскрывающемся списке вы можете выбрать действие для входящих сетевых соединений: • **Разрешать** сетевые соединения (значение по умолчанию). • **Блокировать** сетевые соединения.
Входящие пакеты	В раскрывающемся списке вы можете выбрать действие для входящих пакетов: • **Разрешать** входящие пакеты (значение по умолчанию). • **Блокировать** входящие пакеты.
Всегда добавлять разрешающие правила для портов Агента администрирования	Флажок включает или выключает автоматическое добавление разрешающих правил для портов Агента администрирования. По умолчанию флажок установлен.

Окно Сетевые пакетные правила

Таблица **Сетевые пакетные правила** содержит сетевые пакетные правила, используемые компонентом Управление сетевым экраном для контроля сетевой активности. Для сетевых пакетных правил вы можете настроить параметры, описанные в таблице ниже.

Параметры сетевых пакетных правил

Параметр	Описание
Название	Название сетевого пакетного правила.
Действие	Действие, выполняемое компонентом Управление сетевым экраном при обнаружении сетевой активности.
Локальный адрес	Сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты.
Удаленный адрес	Сетевые адреса удаленных устройств, которые могут передавать и/или получать сетевые пакеты.
Запись в отчет	В столбце указано, будет ли приложение записывать в отчет действия по сетевому пакетному правилу. Если в столбце указано **Да**, приложение записывает в журнал действия по сетевому пакетному правилу. Если в столбце указано **Нет**, приложение не записывает в журнале действия по сетевому пакетному правилу.

По умолчанию таблица сетевых пакетных правил пуста.

Сетевые пакетные правила в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно Добавление сетевого пакетного правила

В этом окне вы можете настроить параметры добавляемого сетевого пакетного правила.

Параметры сетевого пакетного правила

Параметр	Описание
Протокол	Вы можете выбрать тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность: • **Любой** (значение по умолчанию) • **GRE** • **ICMP** • **ICMPv6** • **IGMP** • **TCP** • **UDP**
Направление	Вы можете указать направление отслеживаемой сетевой активности: • **Входящие пакеты**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует только входящие пакеты. • **Входящие**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует только входящие соединения. • **Входящие/Исходящие** (значение по умолчанию). Если выбран этот вариант, компонент Управление сетевым экраном контролирует как входящие, так и исходящие соединения. • **Входящие/Исходящие пакеты**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует как входящие, так и исходящие пакеты. • **Исходящие пакеты**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует только исходящие пакеты. • **Исходящие**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует только исходящие соединения.
ICMP-тип	Вы можете указать тип ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного типа, отправляемые узлом или шлюзом. Если выбран вариант **Определенный**, отображается поле для ввода типа ICMP. Окно отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **ICMP** или **ICMPv6**.
ICMP-код	Вы можете указать код ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного в поле **ICMP-тип** типа и с указанным в поле **ICMP-код** кодом, отправляемые узлом или шлюзом. Если выбран вариант **Определенный**, отображается поле для ввода кода ICMP. Окно отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **ICMP** или **ICMPv6**.
Удаленные порты	Вы можете указать номер порта или диапазон номеров портов удаленных устройств, между которыми требуется контролировать соединение. Если выбран вариант **Определенный**, отображается поле для ввода номеров портов. Окно отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **TCP** или **UDP**.

Параметр	Описание
Локальные порты	Вы можете указать номер порта или диапазон номеров портов локальных устройств, между которыми требуется контролировать соединение. Если выбран вариант **Определенный**, отображается поле для ввода номеров портов. Окно отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **TCP** или **UDP**.
Удаленные адреса	Вы можете указать сетевые адреса удаленных устройств, которые могут передавать и получать сетевые пакеты: • **Любой адрес** (значение по умолчанию). Если выбран этот вариант, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с любым IP-адресом. • **Указанный адрес или диапазон адресов**. Если выбран этот вариант, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с IP-адресами, указанными в таблице ниже. По кнопке **Добавить** над таблицей открывается окно **Добавление IP-адресов**, в котором вы можете указать IP-адрес устройства, адрес сети или диапазон IP-адресов. • **По типу сети**. Если выбран этот вариант, сетевое правило контролирует сетевые пакеты, отправляемые и получаемые удаленными устройствами с IP-адресами, которые относятся к выбранному ниже типу сетей: **Публичные сети**, **Локальные сети** или **Доверенные сети**.
Локальные адреса	Вы можете указать сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты: • **Любой адрес** (значение по умолчанию). Если выбран этот вариант, сетевое правило контролирует отправку и получение сетевых пакетов устройствами с установленным приложением Kaspersky Endpoint Security и любым IP-адресом. • **Указанный адрес или диапазон адресов**. Если выбран этот вариант, сетевое правило контролирует указанные в таблице ниже сетевые адреса устройств с установленным приложением Kaspersky Endpoint Security, которые могут передавать и получать сетевые пакеты. По кнопке **Добавить** над таблицей открывается окно **Добавление IP-адресов**, в котором вы можете указать IP-адрес устройства, адрес сети или диапазон IP-адресов.
Действие	Вы можете выбрать действие, которое будет выполнять компонент Управление сетевым экраном при обнаружении сетевой активности: • **Блокировать** сетевую активность. • **Разрешать** сетевую активность (значение по умолчанию).
Запись в отчет	Вы можете указать, будут ли действия по сетевому правилу записываться в отчет.
Название правила	Поле ввода названия сетевого пакетного правила.

Окно Добавление IP-адресов

В этом окне вы можете указать IP-адрес устройства, адрес сети или диапазон IP-адресов.

Вы можете указать несколько адресов, в этом случае указывайте каждый адрес в новой строке для удобства их копирования.

Окно Доступные сети

Таблица **Доступные сети** содержит сети, контролируемые компонентом Управление сетевым экраном. По умолчанию таблица доступных сетей пустая.

Параметры доступных сетей

Параметр	Описание
IP-адрес	IP-адрес сети.
Тип сети	Тип сети (**Публичная сеть**, **Локальная сеть** или **Доверенная сеть**).

Вы можете добавлять, изменять и удалять доступные сети.

Окно Сетевое соединение

В этом окне вы можете настроить сетевое соединение, которое будет контролировать компонент Управление сетевым экраном.

Сетевое соединение

Параметр	Описание
IP-адрес	Поле ввода IP-адреса сети.
Тип сети	Вы можете выбрать тип сети: • **Публичная сеть**. • **Локальная сеть**. • **Доверенная сеть**.

Контроль безопасности

Контроль устройств

В Консоли администрирования вы можете настраивать параметры контроля устройств в свойствах политики (**Контроль безопасности** → **Контроль устройств**).

Параметры компонента Контроль устройств

Параметр	Описание
Включить Контроль устройств	Флажок включает или выключает компонент Контроль устройств. По умолчанию флажок установлен.
Доверенные устройства	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Доверенные устройства**. В этом окне вы можете добавить устройство в список доверенных.
Режим работы Контроля устройств	Режим работы приложения при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств: • **Информировать**. При выборе этого варианта приложение Kaspersky Endpoint Security тестирует выбранный режим доступа и формирует событие об обнаружении попытки доступа к устройству. • **Блокировать** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security применяет режим доступа, заданный для устройства или шины.
Параметры Контроля устройств	Блок параметров содержит кнопки, по нажатию на которые открываются окна, в которых вы можете настроить режим доступа к устройствам в зависимости от их типа и режим доступа для шин подключения.
Разрешить запрашивать временный доступ	Если флажок установлен, то пользователь может запрашивать временный доступ к заблокированному устройству в графическом интерфейсе или командной строке приложения.
Шаблоны сообщений	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Шаблоны сообщений**.

Окно Доверенные устройства

Таблица содержит список доверенных устройств. По умолчанию таблица пустая.

Параметры доверенного устройства

Параметр	Описание
Идентификатор устройства	Идентификатор доверенного устройства.
Имя устройства	Название доверенного устройства.
Тип устройства	Тип доверенного устройства (например, Жесткий диск или Устройство чтения смарт-карт).
Имя клиентского устройства	Имя клиентского устройства, к которому подключено доверенное устройство.
Пользователь или группа	Имя пользователя или название группы пользователей, для которых устройство является доверенным.
Комментарий	Комментарий, относящийся к доверенному устройству.

Вы можете добавлять устройства в список доверенных устройств по кнопке **Добавить** следующими способами:

- Указать идентификатор или маску идентификатора устройства (**Добавить** → **Добавить устройство по идентификатору или маске**).
- Выбрать нужное устройство в списке устройств, обнаруженных на управляемых устройствах (**Добавить** → **Выбрать устройство в списке устройств, найденных на клиентских устройствах**).
- Выбрать нужное устройство в списке устройств, обнаруженных в событиях Контроля устройств в Kaspersky Security Center (**Добавить** → **Добавить устройство на основе событий**).

Доверенные устройства в таблице можно изменять и удалять.

Вы также можете экспортировать список добавленных устройств в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все** и импортировать список устройств из файла формата JSON по кнопке **Дополнительно** → **Импортировать**.

При импорте предусмотрено три режима:

- **Объединить с существующими** – объединить списки доверенных устройств при импорте. Если в файле для устройства с таким идентификатором уже есть запись, то параметры существующей записи изменяются. Для устройств, которых ранее не было в списке, записи добавляются.
- **Добавить к существующим** – дополнить список доверенных устройств при импорте. В список устройств добавляются только записи для устройств, которых ранее не было.
- **Заменить существующие** – заменить список доверенных устройств. Существующий список доверенных устройств заменяется списком из файла.

Окно Доверенное устройство (Идентификатор устройства)

В этом окне вы можете добавить устройство в список доверенных устройств по его идентификатору.

Добавление устройства по идентификатору

Параметр	Описание
Идентификатор устройства	Поле для ввода идентификатора или маски идентификатора устройства, которое вы хотите добавить в список доверенных устройств. Для указания идентификатора вы можете использовать маски * (любая последовательность символов) или ? (один любой символ). Например, вы можете указать маску USBSTOR* для разрешения доступа ко всем USB-накопителям.
Поиск на устройствах	По нажатию на кнопку отображаются устройства, найденные по указанному идентификатору или маске на подключенных клиентских устройствах. Кнопка доступна, если поле **Идентификатор устройства** не пустое.

Параметр	Описание
Найденные устройства	Таблица содержит следующие столбцы: • **Тип устройства** – тип найденного устройства (например, Жесткий диск или Устройство чтения смарт-карт). • **Идентификатор устройства** – идентификатор найденного устройства. • **Имя устройства** – имя найденного устройства. • **Имя клиентского устройства** – имя клиентского устройства, к которому подключено найденное устройство.
Комментарий	Поле ввода комментария к устройству, которое вы хотите добавить в список доверенных устройств (необязательное).
Разрешать доступ пользователям и/или группам пользователей	Поле, в котором отображается имя пользователя и/или название группы пользователей, для которых устройство является доверенным. По умолчанию указано значение **\Everyone** (все пользователи).
Настроить	По нажатию на кнопку открывается окно **Доступ к доверенному устройству**.

Окно Устройства на клиентских устройствах

В этом окне вы можете добавить устройство в список доверенных, выбрав его в списке устройств, обнаруженных на управляемых клиентских устройствах.

Информация о существующих устройствах доступна, если создана активная политика и выполнена синхронизация с Агентом администрирования (выполняется с частотой, указанной в политике Агента администрирования, по умолчанию – каждые 15 минут).

При создании новой неактивной политики список будет пустым.

Добавление устройств из списка устройств, обнаруженных на управляемых клиентских устройствах

Параметр	Описание
Имя клиентского устройства	Поле ввода имени или маски имени управляемого устройства, для которого вы хотите найти подключенные устройства. По умолчанию указана маска * – все управляемые устройства.
Тип устройства	В раскрывающемся списке вы можете выбрать тип подключенного устройства для поиска (например, Жесткие диски или Устройства чтения смарт-карт). По умолчанию выбран элемент **Все устройства**.
Идентификатор устройства	Поле для ввода идентификатора или маски идентификатора устройства, которое вы хотите найти. По умолчанию указана маска * – все устройства.
Поиск на устройствах	По нажатию на кнопку приложение выполняет поиск устройств с указанными параметрами. Результаты поиска отображаются в таблице ниже.
Список обнаруженных устройств	Таблица содержит следующие столбцы: • **Имя клиентского устройства** – имя клиентского устройства, к которому подключено найденное устройство. • **Тип устройства** – тип найденного устройства (например, Жесткий диск или Устройство чтения смарт-карт). • **Имя устройства** – имя найденного устройства. • **Идентификатор устройства** – идентификатор найденного устройства.

Окно Список устройств на основе событий Контроля устройств

В этом окне вы можете сформировать список устройств, которые обнаружены в событиях Контроля устройств в Kaspersky Security Center. Устройства из этого списка вы можете затем добавить в список доверенных устройств.

Вы можете выбрать одно или несколько устройств для добавления в список доверенных устройств.

Информация об устройствах доступна, если включен Контроль устройств, существует активная политика и выполнена синхронизация с Агентом администрирования (выполняется с частотой, указанной в политике Агента администрирования, по умолчанию – каждые 15 минут).

При создании новой неактивной политики список будет пустым.

Добавление устройств из списка устройств, обнаруженных в событиях Kaspersky Security Center

Параметр	Описание
Типы событий	Вы можете выбрать с помощью флажков типы событий Контроля устройств, отправленные в Kaspersky Security Center. В список попадают устройства, обнаруженные в событиях указанного типа. По умолчанию все флажки установлены.
Группа администрирования	Поле для ввода названия группы администрирования, содержащей клиентские устройства, к которым подключены обнаруженные устройства. В список попадают только устройства, подключенные к клиентским устройствам из указанной группы администрирования. Вы можете указать часть названия группы. По умолчанию в список попадают устройства, подключенные к клиентским устройствам из любой группы администрирования.
Период формирования событий	В раскрывающемся списке вы можете выбрать период времени, в течение которого произошли события. В список попадают устройства, которые обнаружены в событиях, отправленных в Kaspersky Security Center в указанный период. По умолчанию в список попадают устройства, обнаруженные в событиях за последний месяц.
Поиск устройств	По нажатию на кнопку приложение выполняет поиск устройств с указанными параметрами. Результаты поиска отображаются в таблице ниже.
Найденные устройства	Таблица содержит следующие столбцы: • **Тип устройства** – тип найденного устройства (например, Жесткий диск или Устройство чтения смарт-карт). • **Идентификатор устройства** – идентификатор найденного устройства. • **Имя устройства** – имя найденного устройства. • **Имя клиентского устройства** – имя клиентского устройства, к которому подключено найденное устройство. • **Дата подключения** – дата подключения найденного устройства. • **Группа администрирования** – название группы администрирования, содержащей клиентское устройство, к которому подключено найденное устройство.
Комментарий	Поле ввода комментария к устройству, которое вы хотите добавить в список доверенных устройств (необязательное).
Разрешать доступ пользователям и/или группам пользователей	Поле, в котором отображается имя пользователя и/или название группы пользователей, для которых устройство является доверенным. По умолчанию указано значение **\Everyone** (все пользователи).
Настроить	По нажатию на кнопку открывается окно Доступ к доверенному устройству.

Окно Доступ к доверенному устройству

В этом окне вы можете настроить доступ пользователей или групп пользователей к выбранному доверенному устройству.

Доступ к доверенному устройству

Параметр	Описание
Пользователи и/или группы пользователей	Список пользователей и групп, для которых добавляемое устройство будет доверенным. По умолчанию таблица содержит элемент **\Everyone** (все пользователи). Вы можете добавлять, изменять и удалять пользователей и группы пользователей.

Окно Пользователь или группа

В этом окне вы можете указать пользователя или группу пользователей, для которых устройство будет доверенными.

Параметры доверенного устройства

Параметр	Описание
Тип	**Пользователь** или **Группа**, для которых устройство будет доверенным.
Имя пользователя или группы	Имя локального или доменного пользователя (без указания полного имени с доменом, если система допускает ввод имен пользователей в таком формате, или в формате <имя домена>\<имя пользователя> или <имя пользователя>@<имя домена>) или название группы пользователей, для которых устройство будут доверенным.

Окно Тип устройства

В этом окне вы можете настроить режим доступа для различных типов устройств.

Режим доступа для типов устройств

Параметр	Описание
Тип устройства	Тип устройства (например, Жесткие диски, Принтеры).
Режим доступа	Режим доступа к устройству. При нажатии на правую кнопку мыши открывается контекстное меню, в котором вы можете выбрать один из следующих пунктов: • **Разрешать** – разрешать доступ к устройствам выбранного типа. • **Блокировать** – запрещать доступ к устройствам выбранного типа. • **Зависит от шины** (значение по умолчанию) – разрешать или запрещать доступ к устройствам в зависимости от режима доступа для шины подключения. • **По правилам** – разрешать или запрещать доступ к устройствам в зависимости от правила доступа и расписания. Этот пункт меню доступен только для устройств хранения данных (Жесткие диски, Съемные диски, Дискеты, CD/DVD-приводы). • **Только чтение** – разрешать доступ к устройствам выбранного типа только на чтение. Этот пункт меню доступен только для устройств хранения данных (Жесткие диски, Съемные диски, Дискеты, CD/DVD-приводы).

Вы можете настроить правила доступа и расписания доступа в окне **Настройка правила доступа к устройствам**, которое открывается двойным щелчком мыши по названию типа устройства.

Окно Настройка правила доступа к устройствам

В этом окне вы можете настроить правила доступа и расписания для выбранного типа устройств.

Окно открывается по двойному щелчку на названии типа устройства в окне **Тип устройства**.

Правила доступа и расписания для устройств

Параметр	Описание
Пользователи и/или группы пользователей	Список пользователей и групп, для которых можно настроить расписание доступа. По умолчанию таблица содержит элемент **\Everyone** (все пользователи). Вы можете добавлять, изменять и удалять пользователей и группы пользователей.
Правила доступа к устройствам	Таблица содержит расписания доступа для пользователей и групп и состоит из следующих столбцов: • **Расписание доступа** – названия существующих расписаний доступа. Флажок рядом с расписанием показывает, используется ли это расписание в работе компонента. • **Доступ** – тип доступа для расписания: **Разрешать** (предоставить доступ к устройствам выбранного типа) или **Блокировать** (запретить доступ к устройствам выбранного типа). Расписания можно настраивать только для жестких дисков, съемных дисков, дискет и CD/DVD-приводов. По умолчанию таблица содержит расписание доступа **По умолчанию**, которое обеспечивает полный доступ к устройствам для всех пользователей (выбран элемент **\Everyone** в списке **Пользователи и/или группы пользователей**) в любое время, если для этого типа устройства разрешен доступ по шине подключения. Вы можете добавлять, изменять и удалять расписания доступа для выбранных пользователей. Расписание **По умолчанию** невозможно изменить или удалить.

Окно Пользователь или группа

В этом окне вы можете указать пользователя или группу пользователей, на которых распространяется правило доступа к устройствам.

Настройка правила доступа к устройствам

Параметр	Описание
Тип	**Пользователь** или **Группа**, на которых распространяется правило.
Имя пользователя или группы	Имя локального пользователя или название группы пользователей, на которых распространяется правило.

Окно Расписание доступа

В этом окне вы можете настроить расписание доступа к устройствам.

Расписание доступа к устройствам

Параметр	Описание
Название	Поле для ввода названия расписания доступа.
Интервалы времени	Таблица, в которой вы можете выбрать интервалы времени для расписания (дни и часы). Интервалы, выделенные зеленым, включены в расписание. Чтобы исключить интервал из расписания, выберите соответствующие ячейки. Исключенные из расписания интервалы выделены серым цветом. По умолчанию в расписание включены все интервалы (24/7).

Окно Шины подключения

В этом окне вы можете настроить режим доступа для шин подключения.

Режим доступа для шин подключения

Параметр	Описание
Шина подключения	Шина подключения, по которой устройства подключаются к клиентскому устройству: • **FireWire** • **USB**
Режим доступа	Режим доступа для шины подключения. При нажатии на правую кнопку мыши открывается контекстное меню, в котором вы можете выбрать один из следующих пунктов: • **Разрешать** (значение по умолчанию) – предоставлять доступ к устройствам, подключенным по этой шине подключения. • **Блокировать** – запрещать доступ к устройствам, подключенным по этой шине подключения.

Веб-Контроль

В Консоли администрирования вы можете настраивать параметры Веб-Контроля в свойствах политики (**Контроль безопасности** → **Веб-Контроль**).

Параметры компонента Веб-Контроль

Параметр	Описание
Включить Веб-Контроль	Флажок включает компонент Веб-Контроль. По умолчанию флажок снят.

Параметры Веб-Контроля	Таблица содержит список правил доступа к веб-ресурсам. В процессе работы Веб-Контроль применяет правила в том порядке, в котором они указаны в таблице.
	Таблица содержит следующие столбцы:
	• **Статус**. Статус работы правила доступа к веб-ресурсам:
	  • *Включено* – правило включено, Веб-Контроль применяет это правило во время работы.
	  • *Выключено* – правило выключено и не используется во время работы Веб-Контроля.
	  Вы можете установить или снять флажок в таблице, а также установить или снять флажок **Использовать это правило** в окне Правило Веб-Контроля.
	• **Действие**. Действие, которое приложение будет выполнять при обнаружении попытки доступа к веб-ресурсам, удовлетворяющим правилу.
	• **Название**. Название правила доступа к веб-ресурсам.
	Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.
	Вы также можете импортировать список правил из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных правил в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**. При импорте вам будет предложено заменить список правил или добавить правила к уже существующему списку.

Правило по умолчанию	В раскрывающемся списке вы можете выбрать правило по умолчанию, согласно которому приложение будет регулировать доступ к веб-ресурсам, которые не попадают под действие других правил: • **Разрешать** (значение по умолчанию) – разрешать доступ к веб-ресурсам. • **Блокировать** – блокировать доступ к веб-ресурсам.
Шаблоны сообщений	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Шаблоны сообщений.

Окно Правило Веб-Контроля

В этом окне вы можете настроить параметры правила доступа к веб-ресурсам.

Добавление правила Веб-Контроля

Параметр	Описание
Название правила	Поле ввода названия правила доступа к веб-ресурсам. Название правила должно быть уникальным.
Использовать это правило	Флажок включает или выключает использование этого правила во время работы приложения. Если флажок установлен, правило включено, Веб-Контроль применяет это правило во время работы. Если флажок снят, правило выключено и не используется во время работы Веб-Контроля. В дальнейшем вы можете включить использование этого правила Веб-Контролем, установив флажок. По умолчанию флажок установлен.
Фильтровать содержимое	В раскрывающемся списке вы можете выбрать фильтр содержимого веб-ресурса: • **Не фильтровать** (значение по умолчанию). При выборе этого элемента списка фильтр содержимого веб-ресурсов не используется. • **По категориям содержания**. При выборе этого элемента списка становится доступна кнопка **Выбрать**, по нажатию на которую открывается окно Выбор категорий содержания. • **По категориям типов данных**. При выборе этого элемента списка становится доступна кнопка **Выбрать**, по нажатию на которую открывается окно Выбор категорий типов данных. • **По категориям содержания и типов данных**. При выборе этого элемента списка становятся доступны кнопки **Выбрать**, по нажатии на которые открываются окна, в которых вы можете выбрать нужные категории.
Фильтровать адрес	В раскрывающемся списке вы можете выбрать фильтр адреса веб-ресурса: • **Любой адрес** (значение по умолчанию). При выборе этого элемента списка фильтр адресов веб-ресурсов не используется, правило Веб-Контроля применяется ко всем адресам веб-ресурсов. • **Указанные адреса**. При выборе этого элемента списка становится доступна кнопка **Выбрать адреса**, по нажатию на которую открывается окно Выбор адресов, в котором вы можете выбрать нужные адреса веб-ресурсов.

Параметр	Описание
Применять к пользователям	В раскрывающемся списке вы можете выбрать пользователей, на которых распространяется правило доступа к веб-ресурсам: • **Ко всем пользователям** (значение по умолчанию). При выборе этого элемента списка фильтр пользователей не используется, правило Веб-Контроля применяется ко всем пользователям. • **К выбранным пользователям**. При выборе этого элемента списка становится доступна кнопка **Выбрать пользователей**, по нажатию на которую открывается окно **Выбор пользователей**.
Расписание работы правила	В раскрывающемся списке вы можете настроить расписание работы правила доступа к веб-ресурсу: • **Всегда** (значение по умолчанию). При выборе этого элемента списка настраиваемое правило доступа к веб-ресурсу применяется без ограничений по времени, то есть в любое время. • **<Название расписания>**. При выборе этого элемента списка становятся доступны кнопки **Удалить** и **Изменить**, по нажатию на которые вы можете удалить или настроить это расписание. • **Добавить новое расписание**. При выборе этого элемента списка открывается окно **Расписание доступа**, в котором вы можете настроить новое расписание работы правила доступа к веб-ресурсу.
Действие правила	В раскрывающемся списке вы можете выбрать действие, которое Веб-Контроль будет выполнять при обнаружении попытки доступа к веб-ресурсу, удовлетворяющему правилу: • **Разрешать** (значение по умолчанию) – разрешать доступ к веб-ресурсу. • **Блокировать** – блокировать доступ к веб-ресурсу и выводить сообщение о запрете доступа. • **Информировать** – выводить предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

Окно Выбор категорий содержания

В этом окне вы можете выбрать категории содержания, доступ к которым вы хотите контролировать.

Для этого установите флажки рядом с нужными категориями.

По умолчанию все флажки сняты.

> При установке флажков около всех вложенных категорий содержания флажок рядом с основной категорией содержания, содержащей вложенные, автоматически не устанавливается.

Окно Выбор категорий типов данных

В этом окне вы можете выбрать категории типов, доступ к которым вы хотите контролировать.

Для этого установите флажки рядом с нужными категориями.

По умолчанию все флажки сняты.

Окно Выбор адресов

В этом окне вы можете указать адреса веб-ресурсов, доступ пользователей к которым вы хотите контролировать. Вы можете указать несколько адресов, в этом случае указывайте каждый адрес в новой строке для удобства их копирования. Для указания адресов вы можете использовать маски.

Если вы хотите указать группу адресов, откройте окно **Выбор групп адресов**, нажав на кнопку **Добавить группу адресов**.

Окно Выбор групп адресов

Таблица содержит группы адресов веб-ресурсов, доступ пользователей к которым контролирует компонент Веб-Контроль.

Если вы хотите добавить группу адресов в список групп в окне **Выбор адресов**, установите флажок около названия группы в таблице и нажмите на кнопку **Добавить**, расположенную под таблицей.

Элементы в таблице можно добавлять, изменять и удалять.

Если вы хотите добавить новую группу адресов в список групп в этом окне, откройте окно **Добавление группы адресов**, нажав на кнопку **Добавить**, расположенную над таблицей.

По умолчанию таблица пустая.

Окно Добавление группы адресов

В этом окне вы можете указать группы адресов веб-ресурсов, доступ пользователей к которым вы хотите контролировать. Вы можете указать несколько адресов в группе адресов, в этом случае указывайте каждый адрес в новой строке для удобства их копирования. Для указания адресов вы можете использовать маски.

Окно Выбор пользователей

Таблица содержит имена и группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом.

Элементы в таблице можно добавлять, изменять и удалять

Если вы хотите добавить новую пользователя и/или группу пользователей в список пользователей в этом окне, нажав на кнопку **Добавить**, расположенную над таблицей, откройте окно **Пользователь или группа**.

По умолчанию таблица пустая.

Окно Пользователь или группа

В этом окне вы можете указать пользователя или группу пользователей, на которых распространяется правило доступа к веб-ресурсам.

Настройка правила доступа к веб-ресурсам

Параметр	Описание
Тип	**Пользователь** или **Группа**, на которых распространяется правило.
Имя пользователя или группы	Имя пользователя или название группы пользователей, на которых распространяется правило.

Окно Расписание доступа

В этом окне вы можете настроить расписание доступа к веб-ресурсам.

Расписание доступа к веб-ресурсам

Параметр	Описание
Название	Поле для ввода названия расписания доступа.
Интервалы времени	Таблица, в которой вы можете выбрать интервалы времени для расписания (дни и часы). Интервалы, выделенные зеленым, включены в расписание. Чтобы исключить интервал из расписания, выберите соответствующие ячейки. Исключенные из расписания интервалы выделены серым цветом. По умолчанию в расписание включены все интервалы (24/7).

Контроль приложений

В Консоли администрирования вы можете настраивать параметры контроля приложений в свойствах политики (**Контроль безопасности** → **Контроль приложений**).

Параметры компонента Контроль приложений

Параметр	Описание
Включить Контроль приложений	Флажок включает компонент Контроль приложений. По умолчанию флажок снят.
Действие при попытке запуска приложения	Действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам: • **Применять правила** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security применяет правила контроля приложений и выполняет заданное в правилах действие. • **Тестировать правила**. При выборе этого варианта приложение Kaspersky Endpoint Security тестирует правила и формирует событие о попытке запуска приложения, удовлетворяющего правилам.
Режим Контроля приложений	Режим работы компонента Контроль приложений: • **Список разрешенных**. При выборе этого варианта приложение Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. • **Список запрещенных** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.
Правила Контроля приложений	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Правила Контроля приложений.
Применение правил	В раскрывающемся списке вы можете выбрать способ добавления правил: • **Заменить правилами из политики локальные правила**. При выборе этого элемента списка приложение применяет только правила, заданные в политике. • **Добавить правила из политики к локальным правилам** (значение по умолчанию). При выборе этого элемента списка приложение применяет правила, заданные в политике, совместно с локальными правилами, настроенными на защищаемом устройстве.

Окно Правила Контроля приложений

Таблица **Правила Контроля приложений** содержит правила, используемые компонентом Контроль приложений. По умолчанию таблица правил контроля приложений пустая.

Параметры правил контроля приложений

Параметр	Описание
Название категории	Название категории приложений, которая используется в работе правила.
Статус	Статус работы правила контроля приложений: • *Включено* – правило включено, Контроль приложений применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля приложений. • *Тест* – Контроль приложений разрешает запуск приложений, которые удовлетворяют условиям правила, но регистрирует информацию о запуске этих приложений в отчете. Вы можете изменить статус правила в окне **Добавление правила**.

Вы можете добавлять, изменять и удалять правила контроля приложений.

Окно Добавление правила

В этом окне вы можете настроить параметры правила контроля приложений.

Добавление правила контроля приложений

Параметр	Описание
Описание	Описание правила Контроля приложений.
Статус правила	В раскрывающемся списке вы можете выбрать статус работы правила контроля приложений: • *Включено* – правило включено, Контроль приложений применяет это правило во время работы. • *Выключено* – правило выключено и не используется во время работы Контроля приложений. • *Тест* – Контроль приложений разрешает запуск приложений, которые удовлетворяют условиям правила, но записывает информацию о запуске этих приложений в отчет.
Категория	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Категории приложений**.
Пользователи и их права	Таблица содержит список пользователей или групп пользователей, на которых распространяется правило контроля приложений, и назначенные им типы доступа, и состоит из следующих столбцов: • **Имя пользователя или группы** – имена пользователей или названия групп пользователей, на которых распространяется правило контроля приложений. • **Доступ** – тип доступа: **Разрешать** запуск приложений или **Блокировать** запуск приложений. Вы можете добавлять, изменять и удалять пользователей или группы пользователей.

Окно Категории приложений

В этом окне вы можете добавить новую категорию или настроить параметры категории для правила контроля приложений.

Использование KL-категорий приложения Kaspersky Security Center не поддерживается приложением Kaspersky Endpoint Security.

Категории Контроля приложений

Параметр	Описание
Название категории	Список добавленных категорий Контроля приложений.
Добавить	При нажатии на кнопку запускается мастер создания категории. Следуйте указаниям мастера. Подробнее о создании категории см. в справке Kaspersky Security Center.
Изменить	При нажатии на кнопку открывается окно свойств категории, в котором вы можете изменить параметры категории. Категорию **Золотой образ (локальная)** изменить нельзя.

Окно Пользователь или группа

В этом окне вы можете указать локального или доменного пользователя или группу пользователей, для которых вы хотите настроить правило.

Добавление правила Контроля приложений

Параметр	Описание
Тип	**Пользователь** или **Группа**, на которых распространяется правило.
Имя пользователя или группы	Имя пользователя или название группы пользователей, на которых распространяется правило контроля приложений.
Доступ	Тип доступа: **Разрешать** запуск приложений или **Блокировать** запуск приложений.

Инвентаризация

В Консоли администрирования Kaspersky Security Center вы можете выполнять инвентаризацию приложений защищаемого устройства с помощью задачи *Инвентаризация*.

Вы можете создавать и запускать пользовательские задачи инвентаризации. Вы можете настраивать параметры проверки, изменяя параметры задач.

В базе данных приложения 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 устройства с установленным приложением Kaspersky Endpoint Security файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.

Параметры задачи Инвентаризация

Параметр	Описание
Действие с категорией Золотой образ по завершении задачи	В раскрывающемся списке вы можете выбрать действие, которое приложение Kaspersky Endpoint Security выполняет с категорией приложений "Золотой образ" (Golden Image) по завершении задачи Инвентаризация: • **Оставить без изменений** – не изменять категорию приложений "Золотой образ" (Golden Image) после выполнения инвентаризации. Это значение выбрано по умолчанию. • **Обновить или создать (если не создана)** – добавлять приложения, обнаруженные на устройстве задачей Инвентаризация, в категорию приложений "Золотой образ" (Golden Image). Если категория отсутствует, она будет создана. Если категория существует, список приложений в ней будет обновлен. • **Удалить** – очистить категорию приложений "Золотой образ" (Golden Image). Приложение очищает категорию сразу после запуска задачи без инвентаризации файлов на устройстве. Вы можете использовать категорию "Золотой образ" (Golden Image) в правилах Контроля приложений.
Проверять все исполняемые файлы	Флажок включает или выключает проверку исполняемых файлов. По умолчанию флажок установлен.
Проверять двоичные файлы	Флажок включает или выключает проверку двоичных файлов (с расширениями .elf, .java и .pyc). По умолчанию флажок установлен.
Проверять скрипты	Флажок включает или выключает проверку скриптов. По умолчанию флажок установлен.
Области инвентаризации	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки**.

В разделе **Исключения** для задачи Инвентаризация вы можете также настроить области исключения из проверки.

Окно Области проверки

Таблица содержит области проверки. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область проверки – /usr/bin.

Параметры области проверки задачи Инвентаризация

Параметр	Описание
Название области	Название области проверки.
Путь	Путь к проверяемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно Новая область проверки

В этом окне вы можете добавить или настроить область проверки для задачи Инвентаризация.

Параметры области инвентаризации

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время выполнения задачи. Если флажок установлен, приложение обрабатывает эту область проверки во время выполнения задачи. Если флажок снят, приложение не обрабатывает эту область проверки во время выполнения задачи. В дальнейшем вы можете включить эту область в параметры задачи, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать маски. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время выполнения задачи. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Раздел Исключения

Параметры исключений из проверки

Блок параметров	Описание
Области исключения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Области исключения. В этом окне вы можете задать список областей исключений из мониторинга.

Окно Области исключения

Окно содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям.

Параметры области исключения

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, используется ли это исключение в работе приложения.

По умолчанию таблица областей исключения пуста. Элементы в таблице можно добавлять, изменять и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**.

Окно Новая область исключения

В этом окне вы можете добавить или настроить область исключения из проверки для задачи Инвентаризация.

Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна Области исключения. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области во время выполнения задачи. Если флажок установлен, приложение исключает эту область во время выполнения задачи. Если флажок снят, приложение включает эту область во время выполнения задачи. В дальнейшем вы можете исключить эту область из проверки, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения из инвентаризации. Для указания пути вы можете использовать маски. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Контроль целостности системы

В Консоли администрирования вы можете настраивать параметры контроля целостности системы в свойствах политики (**Контроль безопасности** → **Контроль целостности системы**).

Параметры компонента Контроль целостности системы

Параметр	Описание
Включить Контроль целостности системы	Флажок включает или выключает Контроль целостности системы. По умолчанию флажок снят.
Области мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Области проверки.
Исключения из мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Области исключения.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Исключения по маске.

Окно Области проверки

Таблица содержит области мониторинга для компонента Контроль целостности системы. Приложение контролирует файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kesl/).

Параметры области мониторинга

Параметр	Описание
Объединять значения при наследовании	Флажок включает или выключает объединение списка при наследовании в дочерних политиках. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.
Название области	Название области мониторинга.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в каком эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно Новая область проверки

В этом окне вы можете добавить или настроить области мониторинга для компонента Контроль целостности системы.

Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение контролирует эту область мониторинга во время работы приложения. Если флажок снят, приложение не контролирует эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Поле не должно быть пустым. По умолчанию указан путь /opt/kaspersky/kesl.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Окно Области исключения

Окно содержит области исключения из мониторинга для компонента Контроль целостности системы. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям.

Параметры области исключения из мониторинга

Параметр	Описание
Объединять значения при наследовании	Флажок включает или выключает объединение списка при наследовании в дочерних политиках. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из мониторинга.
Статус	Статус показывает, исключает ли приложение эту область из мониторинга при работе компонента.

По умолчанию таблица областей исключения пуста. Элементы в таблице можно добавлять, изменять и удалять.

Вы также можете импортировать список областей исключения из файла по кнопке **Импортировать** и экспортировать список областей исключения в файл в формате JSON по кнопке **Экспортировать**. При импорте вам будет предложено заменить список областей исключения или добавить области исключения к уже существующему списку.

Окно Новая область исключения

В этом окне вы можете добавить или настроить область исключения из мониторинга для компонента Контроль целостности системы.

Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы приложения. Если флажок установлен, приложение исключает эту область из мониторинга во время работы компонента. Если флажок снят, приложение контролирует эту область во время работы компонента. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Поле не должно быть пустым. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение исключает из мониторинга. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из мониторинга. Примеры: Маска `*.txt` – все текстовые файлы. Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Приложение не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из мониторинга.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Вы также можете импортировать список исключений из файла по кнопке **Импортировать** и экспортировать список исключений в файл в формате JSON по кнопке **Экспортировать**. При импорте вам будет предложено заменить список исключений или добавить исключения к уже существующему списку.

Вы можете включить объединение списка исключений при наследовании в дочерних политиках. Для объединения элементов списка требуется установить флажок **Объединять значения при наследовании**. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.

Проверка целостности системы

В Консоли администрирования вы можете выполнять проверку целостности системы с помощью задачи *Проверка целостности системы*.

Вы можете создавать и запускать пользовательские задачи проверки целостности системы. Вы можете настраивать параметры проверки, изменяя параметры задач.

В разделе **Параметры** в свойствах задачи Проверка целостности системы вы можете настроить параметры, приведенные в таблице ниже.

Параметры задачи Проверка целостности системы

Параметр	Описание
Обновлять снимок состояния системы при каждом запуске задачи	Флажок включает или выключает обновление снимка состояния системы при каждом запуске задачи Проверка целостности системы. По умолчанию флажок снят.
Использовать хеш SHA256 для проверки	Флажок включает или выключает использование хеша файла в качестве критерия для сравнения текущего состояния файла с исходным состоянием. Если флажок снят, приложение сравнивает только размер файла (если размер файла не изменился, время изменения не считается критическим параметром). По умолчанию флажок снят.
Проверять директории в областях мониторинга	Флажок включает или выключает проверку директорий в указанных областях мониторинга во время выполнения проверки целостности системы. По умолчанию флажок снят.
Отслеживать время последнего доступа к файлу	Флажок включает или выключает отслеживание времени доступа к файлу во время выполнения проверки целостности системы. По умолчанию флажок снят.
Области мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Области проверки.

В разделе **Области исключения** в свойствах задачи Проверка целостности системы вы можете настроить области исключения из мониторинга и исключения по маске.

Окно Области проверки

Таблица содержит области мониторинга для задачи Проверка целостности системы. Приложение контролирует файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kesl/).

Параметры области мониторинга

Параметр	Описание
Название области	Название области мониторинга.
Путь	Путь к защищаемой директории.
Статус	Статус показывает, проверяет ли приложение эту область при работе.

Элементы в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в каком эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно Новая область проверки

В этом окне вы можете добавить или настроить области мониторинга для задачи Проверка целостности системы.

Параметры области мониторинга

Параметр	Описание
Название области проверки	Поле ввода названия области мониторинга. Это название будет отображаться в таблице окна Области проверки. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение контролирует эту область мониторинга во время работы приложения. Если флажок снят, приложение не контролирует эту область мониторинга во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите включить в область мониторинга. Для указания пути вы можете использовать маски. Поле не должно быть пустым. По умолчанию указан путь /opt/kaspersky/kesl.
Маски	Список содержит маски имен объектов, которые приложение проверяет во время работы. По умолчанию список содержит маску * (все объекты). Вы можете добавлять, изменять и удалять маски.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Раздел Исключения

Параметры исключений из проверки

Блок параметров	Описание
Исключения из мониторинга	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Области исключения. В этом окне вы можете задать список областей исключений из мониторинга.
Исключения по маске	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Исключения по маске. В этом окне вы можете настроить исключение объектов из мониторинга по маске имени.

Окно Области исключения

Таблица содержит области исключения из проверки для задачи Проверка целостности системы. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.

Параметры области исключения из проверки задачи Проверка целостности системы

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Путь к директории, исключенной из проверки.
Статус	Статус показывает, исключает ли приложение эту область из проверки при работе задачи.

Элементы в таблице можно добавлять, изменять и удалять.

Окно Новая область исключения

В этом окне вы можете добавить или настроить область исключения из мониторинга для задачи Проверка целостности системы.

Параметры области исключения из мониторинга

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Области исключения**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает исключение области из мониторинга во время работы приложения. Если флажок установлен, приложение исключает эту область из мониторинга во время работы задачи. Если флажок снят, приложение контролирует эту область во время работы задачи. В дальнейшем вы можете исключить эту область из мониторинга, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Поле ввода пути к локальной директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать маски. Поле не должно быть пустым. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.
Маски	Список содержит маски имен объектов, которые приложение исключает из мониторинга. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски. При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки. Примеры: Маска `*.txt` – все текстовые файлы. Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Окно Исключения по маске

Вы можете настроить исключение объектов из мониторинга по маске имени. Приложение не будет выполнять проверку файлов, имена которых содержат указанную маску. По умолчанию список масок пуст.

Вы можете добавлять, изменять и удалять маски.

При нажатии на кнопку **Добавить** открывается окно **Маска объекта**. В этом окне в поле **Задайте маску объекта** вы можете задать шаблон для имен файлов, которые Kaspersky Endpoint Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Локальные задачи

Управление задачами

В Консоли администрирования вы можете настраивать разрешение на просмотр и управление задачами в свойствах политики (**Локальные задачи** → **Управление задачами**).

Параметры управления задачами

Параметр	Описание
Разрешить использование локальных задач	Флажок разрешает или запрещает пользователям просмотр локальных задач, созданных в приложении Kaspersky Endpoint Security, и управление этими задачами на управляемых клиентских устройствах. Если флажок установлен, пользователи могут настраивать и запускать задачи в графическом интерфейсе приложения и в командной строке. Если флажок снят, использование локальных задач прекращается. Локальные задачи не запускаются по расписанию. Задачи недоступны для запуска и настройки в графическом интерфейсе приложения и в командной строке. По умолчанию флажок снят.
Разрешить просмотр и управление задачами, созданными через KSC	Флажок разрешает или запрещает пользователям просмотр задач, созданных через Kaspersky Security Center, и управление этими задачами на клиентских устройствах. Если флажок установлен, задачи, созданные через Kaspersky Security Center, отображаются в графическом интерфейсе приложения. Пользователи могут запускать и останавливать эти задачи в графическом интерфейсе приложения и в командной строке. Если флажок снят, в графическом интерфейсе приложения и в командной строке недоступен просмотр и управление задачами, созданными через Kaspersky Security Center. По умолчанию флажок снят.

Защита от сложных угроз и целевых атак

Интеграция с Kaspersky Managed Detection and Response

В Консоли администрирования вы можете включать и выключать компонент MDR и загружать файл MDR BLOB в свойствах политики (**Detection and Response** → **Managed Detection and Response**).

Параметры интеграции с MDR

Параметр	Описание
Включить Managed Detection and Response	Флажок включает или выключает компонент MDR, необходимый для интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response. По умолчанию компонент выключен. Если вы включаете компонент MDR, а Kaspersky Security Network выключен или используется в стандартном режиме, вам будет предложено принять условия использования Kaspersky Security Network для включения Kaspersky Security Network в расширенном режиме. Если изменение параметров KSN запрещено родительской политикой, отображается сообщение об ошибке, компонент MDR не включается.
Загрузить	По нажатию на кнопку открывается стандартное окно Microsoft Windows, в котором вы можете выбрать файл MDR BLOB для загрузки. Действие обязательно при наличии тенантов и/или если вы активировали компонент MDR с помощью файла MDR BLOB.

Файл BLOB находится в ZIP-архиве конфигурационного файла MDR, который входит в поставку решения Kaspersky Managed Detection and Response.

Загружая файл BLOB, вы соглашаетесь автоматически передавать данные с устройства с установленным приложением Kaspersky Endpoint Security в "Лабораторию Касперского" для обработки. Не загружайте файл, если вы не согласны на обработку передаваемых данных. Подробное описание передаваемых данных см. в справке Kaspersky Managed Detection and Response.

Интеграции с Kaspersky Endpoint Detection and Response (on-premises)

В Консоли администрирования вы можете включать и выключать компонент EDR Expert (on-premises) и настраивать параметры интеграции приложения Kaspersky Endpoint Security с компонентом Kaspersky Endpoint Detection and Response (KATA) в свойствах политики (**Detection and Response** → **EDR Expert (on-premises)**).

Если в Web Console для компонента EDR Expert (on-premises) выбран вариант **Endpoint Detection and Response Expert (версия 8.0 и выше)**, то есть режим интеграции EDR Expert (on-premises), в Консоли администрирования отображается предупреждение, параметры интеграции с Kaspersky Endpoint Detection and Response (KATA) недоступны. Вы можете изменить режим интеграции в Web Console.

Параметры интеграции с Kaspersky Endpoint Detection and Response (on-premises)

Параметр	Описание
Включить Endpoint Detection and Response Expert (on-premises)	Флажок включает или выключает компонент EDR Expert (on-premises), обеспечивающий интеграцию с Kaspersky Endpoint Detection and Response (KATA). По умолчанию компонент выключен.
Включить запрет запуска объектов	Флажок включает или выключает применение правил запрета запуска объектов компонента EDR Expert (on-premises).
Серверы KATA	По кнопке **Настроить** открывается окно, в котором вы можете настроить подключение к серверам KATA, а также просмотреть список серверов, к которым настроено подключение.
Параметры подключения к серверам	По кнопке **Настроить** открывается окно, в котором вы можете настроить общие параметры подключения к серверам KATA, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверам KATA.
Параметры передачи данных	По кнопке **Настроить** открывается окно, в котором вы можете настроить параметры передачи данных на серверы KATA.

Настройка подключения к серверам KATA

В таблице отображается список параметров подключения к серверам KATA. Для каждого сервера, к которому настроено подключение, в таблице указывается IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера и порт.

С помощью кнопок и меню над таблицей вы можете выполнить следующие действия:

- Добавить параметры подключения к серверу KATA.
- Изменить или удалить ранее настроенные параметры подключения.
- Экспортировать или импортировать список настроенных параметров подключения.

Параметры подключения к серверу

Параметр	Описание
Адрес	Адрес сервера KATA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Чтобы связь с сервером не прерывалась в случае сбоя работы приложения при включенной сетевой изоляции устройства, рекомендуется указывать IP-адрес сервера. Значение по умолчанию: `127.0.0.1`.
Порт	Порт для подключения к серверу KATA. Значение по умолчанию: `443`.

Настройка общих параметров подключения к серверам KATA

В этом окне вы можете настроить общие параметры подключения к серверам KATA.

Параметры подключения к серверам KATA

Параметр	Описание
Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)	Периодичность отправки запросов на синхронизацию на сервер KATA в минутах. Значение по умолчанию: `5`.
Максимальное время ожидания соединения с сервером (сек.)	Максимальное время ожидания соединения с сервером KATA в секундах. Значение по умолчанию: `10`.
Максимальное время ожидания ответа от сервера (сек.)	Максимальное время ожидания ответа от сервера KATA в секундах. Значение по умолчанию: `10`.

Параметр	Описание
Разрешить отправку телеметрии	Флажок включает или выключает отправку данных о событиях на устройствах (телеметрии) на сервер KATA. По умолчанию отправка телеметрии включена.

Сертификат сервера	Блок параметров содержит кнопки для добавления и удаления сертификата сервера:
	• **Добавить** – открывает окно добавления сертификата сервера. Кнопка отображается, если сертификат сервера еще не добавлен.
	В окне добавления сертификата вы можете добавить сертификат сервера KATA одним из следующих способов:
	  • Указать в поле **Добавить из файла** путь к файлу сертификата, содержащему сертификат формата DER или PEM. По кнопке **Обзор** открывается стандартное окно для выбора файла.
	  • Скопировать в поле **Ввести данные сертификата** содержимое файла сертификата.
	Если сертификат сервера добавлен, выполняется проверка сертификата сервера на стороне Kaspersky Endpoint Security, это позволяет повысить уровень безопасности соединения.
	• **Удалить** – удаляет ранее добавленный сертификат сервера. Кнопка отображается, только если сертификат сервера добавлен.

Дополнительная защита подключения	Блок параметров содержит элементы интерфейса для настройки дополнительной защиты подключения с помощью двусторонней аутентификации:
	• **Использовать двустороннюю аутентификацию** – включает или выключает использование двусторонней аутентификации для дополнительной защиты соединения с сервером KATA. Чтобы использовать двустороннюю аутентификацию, вам нужно добавить сертификат клиента.
	  Двусторонняя аутентификация должна быть включена на стороне сервера KATA.
	• **Добавить** – открывает окно добавления сертификата клиента для дополнительной защиты соединения с сервером KATA. Кнопка отображается, если установлен флажок **Использовать двустороннюю аутентификацию** и сертификат клиента еще не добавлен.
	Чтобы добавить сертификат клиента, в окне добавления сертификата укажите путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ. По кнопке **Обзор** открывается стандартное окно для выбора файла. Далее введите пароль сертификата клиента в поле **Пароль криптоконтейнера**.
	  Поле является обязательным. При попытке сохранить настройки без указания пароля отображается сообщение об ошибке.
	Если введен корректный пароль, кнопка **OK** активна. Вы можете сохранить настройки.
	• **Удалить** – удаляет ранее добавленный сертификат клиента. Кнопка отображается, только если сертификат клиента добавлен.

Настройка параметров передачи данных на серверы KATA

В этом окне вы можете настроить параметры передачи данных на серверы KATA.

Параметры передачи данных на серверы KATA

Параметр	Описание
Максимальная задержка отправки событий (сек.)	Максимальная задержка отправки событий на сервер KATA в секундах. Значение по умолчанию: `30`.
Включить регулирование количества событий	Включает или выключает регулирование количества событий, отправляемых на сервер KATA.
Максимальное количество событий в час	Максимальное количество событий в час. Значение по умолчанию: `3000`.
Процент превышения ограничения на количество событий	Процент превышения ограничения на количество событий. Передача событий ограничивается, если соотношение событий одного типа (например, событий изменений в реестре) к общему количеству событий превышает установленное ограничение в процентах. Значение по умолчанию: `15`.

Интеграция с Kaspersky Network Detection and Response (KATA)

В Консоли администрирования вы можете включать и выключать компонент NDR (KATA) и настраивать параметры интеграции приложения Kaspersky Endpoint Security с компонентом Kaspersky Network Detection and Response (KATA) в свойствах политики (**Detection and Response** → **Network Detection and Response (KATA)**).

Параметры интеграции с Kaspersky Network Detection and Response (KATA)

Параметр	Описание
Включить Network Detection and Response (KATA)	Флажок включает или выключает компонент NDR (KATA). По умолчанию компонент выключен.
Серверы NDR	По кнопке **Настроить** открывается окно, в котором вы можете настроить подключение к серверам NDR, а также просмотреть список серверов, к которым настроено подключение.
Параметры подключения к серверам	По кнопке **Настроить** открывается окно, в котором вы можете настроить общие параметры подключения к серверам NDR, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверам NDR.
Параметры передачи данных	По кнопке **Настроить** открывается окно, в котором вы можете настроить параметры передачи данных на серверы NDR.

Настройка подключения к серверам NDR

В таблице отображается список параметров подключения к серверам NDR. Для каждого сервера, к которому настроено подключение, в таблице указывается IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера и порт.

С помощью кнопок и меню над таблицей вы можете выполнить следующие действия:

- Добавить параметры подключения к серверу NDR.
- Изменить или удалить ранее настроенные параметры подключения.
- Экспортировать или импортировать список настроенных параметров подключения.

Параметры подключения к серверу

Параметр	Описание
Адрес	Адрес сервера NDR. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Значение по умолчанию: `127.0.0.1`.
Порт	Порт для подключения к серверу NDR. Значение по умолчанию: `443`.

Настройка общих параметров подключения к серверам NDR

В этом окне вы можете настроить общие параметры подключения к серверам NDR.

Параметры подключения к серверам NDR

Параметр	Описание
Отправлять запрос на синхронизацию на сервер NDR каждые (мин.)	Периодичность отправки запросов на синхронизацию на сервер NDR в минутах. Значение по умолчанию: `5`.
Максимальное время ожидания соединения с сервером (сек.)	Максимальное время ожидания соединения с сервером NDR в секундах. Значение по умолчанию: `10`.
Максимальное время ожидания ответа от сервера (сек.)	Максимальное время ожидания ответа от сервера NDR в секундах. Значение по умолчанию: `10`.

Сертификат сервера	Блок параметров содержит кнопки для добавления и удаления сертификата сервера:
	• **Добавить** – открывает окно добавления сертификата сервера. Кнопка отображается, если сертификат сервера еще не добавлен.
	В окне добавления сертификата вы можете добавить сертификат сервера NDR одним из следующих способов:
	  • Указать в поле **Добавить из файла** путь к файлу сертификата, содержащему сертификат формата DER или PEM. По кнопке **Обзор** открывается стандартное окно для выбора файла.
	  • Скопировать в поле **Ввести данные сертификата** содержимое файла сертификата.
	Если сертификат сервера добавлен, выполняется проверка сертификата сервера на стороне Kaspersky Endpoint Security, это позволяет повысить уровень безопасности соединения.
	• **Удалить** – удаляет ранее добавленный сертификат сервера. Кнопка отображается, только если сертификат сервера добавлен.

Дополнительная защита подключения	Блок параметров содержит элементы интерфейса для настройки дополнительной защиты подключения с помощью двусторонней аутентификации:
	• **Использовать двустороннюю аутентификацию** – включает или выключает использование двусторонней аутентификации для дополнительной защиты соединения с сервером NDR. Чтобы использовать двустороннюю аутентификацию, вам нужно добавить сертификат клиента.
	  Двусторонняя аутентификация должна быть включена на стороне сервера NDR.
	• **Добавить** – открывает окно добавления сертификата клиента для дополнительной защиты соединения с сервером NDR. Кнопка отображается, если установлен флажок **Использовать двустороннюю аутентификацию** и сертификат клиента еще не добавлен.
	Чтобы добавить сертификат клиента, в окне добавления сертификата укажите путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ. По кнопке **Обзор** открывается стандартное окно для выбора файла. Далее введите пароль сертификата клиента в поле **Пароль криптоконтейнера**.
	  Поле является обязательным. При попытке сохранить настройки без указания пароля отображается сообщение об ошибке.
	Если введен корректный пароль, кнопка **OK** активна. Вы можете сохранить настройки.
	• **Удалить** – удаляет ранее добавленный сертификат клиента. Кнопка отображается, только если сертификат клиента добавлен.

Настройка параметров передачи данных на серверы NDR

В этом окне вы можете настроить параметры передачи данных на серверы NDR.

Параметры передачи данных на серверы NDR

Параметр	Описание
Максимальная задержка отправки событий (сек.)	Максимальная задержка отправки событий на сервер NDR в секундах. Значение по умолчанию: `30`.
Максимальное количество событий в пакете	Максимальное количество событий в одном пакете. Значение по умолчанию: `1024`.

Параметр	Описание
Периодичность опроса серверов	Периодичность отправки запросов на синхронизацию на сервер NDR в секундах. Значение по умолчанию: `450`.
Включить регулирование количества событий	Включает или выключает регулирование количества событий, отправляемых на сервер NDR.
Максимальное количество событий в час	Максимальное количество событий в час. Значение по умолчанию: `3000`.
Процент превышения ограничения на количество событий	Процент превышения ограничения на количество событий. Передача событий ограничивается, если соотношение событий одного типа (например, событий изменений в реестре) к общему количеству событий превышает установленное ограничение в процентах. Значение по умолчанию: `15`.

Интеграция с KUMA

В Консоли администрирования вы можете включать и выключать интеграцию приложения Kaspersky Endpoint Security с Kaspersky Unified Monitoring and Analysis Platform и настраивать параметры интеграции в свойствах политики (**Интеграция с KUMA** → **Интеграция с KUMA**).

Параметры интеграции с Kaspersky Unified Monitoring and Analysis Platform

Параметр	Описание
Включить интеграцию с KUMA	Включает или выключает интеграцию приложения Kaspersky Endpoint Security с решением Kaspersky Unified Monitoring and Analysis Platform. По умолчанию интеграция с KUMA выключена.
Использовать защищенное соединение	Флажок включает или выключает использование проверки сертификата сервера для дополнительной защиты подключения к серверу KUMA. Для проверки сертификата сервера вам нужно установить этот флажок и добавить сертификат сервера в окне **Серверы KUMA**. По умолчанию флажок снят.
Серверы KUMA	По кнопке **Настроить** открывается окно **Серверы KUMA**. В этом окне вы можете настраивать подключение к серверам KUMA, а также просматривать список серверов, к которым настроено подключение.
Параметры подключения к серверам KUMA	По кнопке **Настроить** открывается окно **Параметры подключения к серверам**, в котором вы можете настроить общие параметры подключения к серверам KUMA, добавить сертификат сервера и настроить двустороннюю аутентификацию при подключении к серверам KUMA.
Максимальная задержка отправки событий (сек.)	Максимальная задержка отправки событий на сервер KUMA в секундах. Значение по умолчанию: `30`.

Окно Серверы KUMA

В этом окне в таблице отображается список параметров подключения к серверам KUMA. Для каждого сервера, к которому настроено подключение, в таблице указывается:

- IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Если в окне настройки интеграции с KUMA вы установили флажок **Использовать защищенное соединение**, требуется указать полное доменное имя (FQDN) сервера из сертификата, полученного при приобретении лицензии на использование KUMA.
- Порт для подключения к серверу KUMA.
- Протокол, используемый для подключения к серверу KUMA.

С помощью кнопок и меню над таблицей вы можете выполнить следующие действия:

- Добавить параметры подключения к серверу KUMA.
- Изменить или удалить ранее настроенные параметры подключения.
- Экспортировать или импортировать список настроенных параметров подключения.

Окно Сервер KUMA

В этом окне вы можете указать параметры подключения к серверу KUMA.

Параметры подключения к серверу KUMA

Параметр	Описание
Адрес	Адрес сервера KUMA. Вы можете указать IP-адрес (IPv4 или IPv6) или полное доменное имя (FQDN) сервера. Если в окне настройки интеграции с KUMA вы установили флажок **Использовать защищенное соединение**, требуется указать полное доменное имя (FQDN) сервера из сертификата, полученного при приобретении лицензии на использование KUMA.
Порт	Порт для подключения к серверу KUMA. Значение по умолчанию: `443`.
Протокол	Протокол для подключения к серверу KUMA: TCP, UDP или HTTP/HTTPS со сжатием. При выборе протокола UDP использование сертификатов для обеспечения безопасности соединения не поддерживается, а также отсутствуют события о соединении с сервером KUMA. Значение по умолчанию: TCP.

Окно Параметры подключения к серверам KUMA

В этом окне вы можете настроить общие параметры подключения к серверам KUMA.

Параметры подключения к серверам KUMA

Параметр	Описание
Максимальное время ожидания соединения с сервером (сек.)	Максимальное время ожидания соединения с сервером KUMA в секундах. Значение по умолчанию: `5`.
Сертификат сервера	Блок параметров содержит кнопки для добавления и удаления сертификата сервера.
Добавить (сертификат сервера)	Открывает окно добавления сертификата сервера. Кнопка отображается, если сертификат сервера еще не добавлен.
Удалить (сертификат сервера)	Удаляет сертификат сервера. Кнопка отображается, если сертификат сервера добавлен.
Дополнительная защита подключения	Блок параметров содержит элементы интерфейса для настройки дополнительной защиты подключения с помощью двусторонней аутентификации.
Использовать двустороннюю аутентификацию	Флажок включает или выключает использование двусторонней аутентификации для дополнительной защиты соединения с сервером KUMA. Чтобы использовать двустороннюю аутентификацию, вам нужно добавить сертификат клиента. Двусторонняя аутентификация должна быть включена на стороне сервера KUMA.

Параметр	Описание
Добавить (сертификат клиента)	Открывает окно добавления сертификата клиента для защиты соединения с сервером KUMA. Кнопка отображается, если сертификат клиента еще не добавлен. Если вы хотите настроить дополнительную защиту соединения, вам нужно включить проверку сертификатов клиентов на стороне сервера KUMA и установить флажок **Использовать двустороннюю аутентификацию** в этом окне.
Удалить (сертификат клиента)	Удаляет сертификат клиента. Кнопка отображается, если сертификат клиента добавлен.

Окно добавления сертификата сервера

В этом окне вы можете добавить сертификат сервера KUMA одним из следующих способов:

- Указать путь к файлу сертификата в поле **Добавить из файла**. По кнопке **Обзор** открывается стандартное окно для выбора файла. Укажите путь к файлу, содержащему сертификат формата DER или PEM.
- Скопировать содержимое файла сертификата в поле **Ввести данные сертификата**.

Если сертификат сервера добавлен, выполняется проверка сертификата сервера на стороне Kaspersky Endpoint Security, это позволяет повысить уровень безопасности соединения.

Окно добавления сертификата клиента

В этом окне вы можете добавить сертификат клиента для дополнительной защиты соединения с сервером KUMA.

Если вы хотите настроить дополнительную защиту соединения, вам нужно включить проверку сертификатов клиентов на стороне сервера KUMA и установить флажок **Использовать двустороннюю аутентификацию** в окне Параметры подключения к серверам KUMA.

Чтобы добавить сертификат клиента, укажите путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ. По кнопке **Обзор** открывается стандартное окно для выбора файла. Далее введите пароль сертификата клиента в поле **Пароль криптоконтейнера**.

Поле является обязательным. При попытке сохранить настройки без указания пароля отображается сообщение об ошибке.

Если введен корректный пароль, кнопка **OK** активна. Вы можете сохранить настройки.

Карантин

В Консоли администрирования вы можете настраивать параметры карантина в свойствах политики (**Общие параметры** → **Параметры хранилищ**) и в свойствах управляемого устройства (**Управляемые устройства** → вкладка **Устройства** → окно свойств устройства → раздел **Приложения** → окно свойств приложения → **Параметры хранилищ**).

Параметры карантина

Параметр	Описание
Ограничить размер карантина до (МБ)	Флажок включает или выключает ограничение максимального размера карантина заданным значением (в мегабайтах). Если флажок снят, размер карантина не ограничен. Доступные значения: 1–999999. Значение по умолчанию: 200, если приложение используется в стандартном режиме или в режиме EDR-Агента, и 100, если приложение используется в режиме Легкого агента.
Уведомлять при заполнении карантина на (%)	Флажок включает или выключает ограничение на процент заполнения карантина, при котором формируется событие о заполнении карантина. Если флажок снят, событие о заполнении карантина не формируется. Доступные значения: 1–100. Значение по умолчанию: 90.

Запрет запуска объектов

Вы можете включать и выключать запрет запуска объектов в Консоли администрирования только если включена интеграция с Kaspersky Endpoint Detection and Response Expert (on-premises) или с Kaspersky Endpoint Detection and Response (KATA).

Вы можете включать и выключать запрет запуска объектов в свойствах политики (**Параметры приложения** → **Detection and Response** → **EDR Expert (on-premises)**).

Флажок **Включить запрет запуска объектов** в блоке параметров **Запрет запуска объектов** включает или выключает применение правил запрета запуска объектов компонента EDR Expert (on-premises).

Общие параметры

В Консоли администрирования вы можете настраивать общие параметры приложения, которые определяют работу приложения в целом и работу отдельных функций, в свойствах политики (**Общие параметры**).

Прокси-сервер

В Консоли администрирования вы можете настраивать использование прокси-сервера в свойствах политики (**Общие параметры** → **Параметры прокси-сервера**).

Параметры прокси-сервера

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, прокси-сервер не используется в работе приложения.
Использовать указанные параметры прокси-сервера	Если выбран этот вариант, приложение использует указанные параметры прокси-сервера для подключения к серверам активации "Лаборатории Касперского", к источникам обновлений баз и модулей приложения, к Kaspersky Security Network и при проверке сертификатов сайтов компонентом Защита от веб-угроз.
Адрес и порт	Поля для ввода IP-адреса или доменного имени прокси-сервера и порта прокси-сервера. Порт по умолчанию: 3128. Поля доступны, если выбран вариант **Использовать указанные параметры прокси-сервера**.

Параметр	Описание
Использовать аутентификацию на прокси-сервере	Флажок включает или выключает аутентификацию с помощью имени пользователя и пароля при доступе к прокси-серверу. Флажок доступен, если выбран вариант **Использовать указанные параметры прокси-сервера**. По умолчанию флажок снят. Для подключения через прокси-сервер по протоколу HTTP рекомендуется использовать отдельную учетную запись, которая не используется для аутентификации в других системах. HTTP-прокси-сервер использует незащищенное соединение, и учетная запись может быть скомпрометирована.
Имя пользователя	Поле ввода имени пользователя для его аутентификации на прокси-сервере. Поле ввода доступно, если установлен флажок **Использовать аутентификацию на прокси-сервере**.
Пароль	Поле для ввода пароля пользователя для авторизации на прокси-сервере. Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев. При нажатии на кнопку **Показать** пароль пользователя отображается в поле **Пароль** в открытом виде. По умолчанию пароль пользователя скрыт и отображается в виде точек. Поле ввода и кнопка доступны, если установлен флажок **Использовать аутентификацию на прокси-сервере**.
Использовать Kaspersky Security Center в качестве прокси-сервера для активации приложения	Включает или выключает использование Сервера администрирования Kaspersky Security Center в качестве прокси-сервера для доступа к серверам активации "Лаборатории Касперского". Это нужно при активации приложения в изолированном сегменте сети без доступа в интернет с помощью кода активации. Если флажок установлен, приложение получает доступ к серверам активации через Сервер администрирования с доступом в интернет. По умолчанию флажок снят. Параметр применяется, только если приложение используется в стандартном режиме. Если приложение используется в режиме Легкого агента, информацию о лицензии предоставляет Сервер защиты.
Исключения для прокси-сервера	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Исключения для прокси-сервера.

Окно Исключения для прокси-сервера

В этом окне вы можете настроить использование прокси-сервера при интеграции с компонентами решения Kaspersky Anti Targeted Attack Platform, а также список адресов, для подключения к которым не будет использоваться прокси-сервер.

Исключения для прокси-сервера

Параметр	Описание
Не использовать прокси-сервер в работе компонентов	Установите флажки рядом с теми компонентами приложения, в работе которых не нужно использовать прокси-сервер: • **Endpoint Detection and Response Expert (on-premises)** – не использовать прокси-сервер при подключении к серверам, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises) или с Kaspersky Endpoint Detection and Response (KATA). • **Sandbox** – не использовать прокси-сервер при подключении к серверам, обеспечивающим интеграцию с Sandbox. • **Network Detection and Response (KATA)** – не использовать прокси-сервер при подключении к серверам, обеспечивающим интеграцию с Kaspersky Network Detection and Response (KATA).

Параметр	Описание
Не использовать прокси-сервер для адресов	Таблица содержит список адресов, для подключения к которым не будет использоваться прокси-сервер: • **IP-адрес/DNS-имя** – IP-адрес или DNS-имя, для подключения к которому не будет использоваться прокси-сервер. Для указания адреса вы можете использовать маски (символы `*` и `?`). • **Комментарий** – поле ввода комментария (необязательное). Вы можете добавлять, изменять и удалять адреса в таблице.

Потребление ресурсов процессора для задач проверки

В Консоли администрирования вы можете включать и выключать ограничение на использование ресурсов процессора и настраивать ограничение на использование памяти для задач проверки в свойствах политики (**Общие параметры** → **Параметры приложения**, блок **Производительность**).

По нажатию на кнопку **Настроить** в блоке **Производительность** открывается окно **Параметры производительности задач проверки**, в котором в блоке **Потребление ресурсов процессора и памяти** вы можете настроить ограничения (см. таблицу ниже).

Параметры использования ресурсов процессора и памяти

Параметр	Описание
Ограничить потребление ресурсов процессора для задач проверки (%)	Флажок включает или выключает ограничение на использование ресурсов процессора для задач *Поиск вредоносного ПО*, *Проверка важных областей*, *Инвентаризация* и *Проверка контейнеров*. Если флажок установлен, максимальная нагрузка на все ядра процессора при работе этих задач не превышает значения, указанного в поле справа (в процентах). Значение в поле должно быть целым числом и находиться в пределах от 10 до 100. По умолчанию флажок снят.
Ограничение на использование памяти для задач проверки (МБ)	Поле ввода ограничения на использование памяти для задач проверки (в мегабайтах). Значение по умолчанию: 8192.

Запуск задач при работе от аккумулятора

В Консоли администрирования вы можете настраивать отмену запуска запланированных задач в свойствах политики (**Общие параметры** → **Параметры приложения**, блок **Производительность**).

Параметры запуска задач при работе от аккумулятора

Параметр	Описание
Пропускать запланированные задачи при работе от аккумулятора	Флажок включает или выключает отмену запуска задач, для которых настроено расписание. По умолчанию флажок установлен. Если флажок снят, на устройстве запускаются все запланированные по расписанию задачи, независимо от источника питания, к которому подключено устройство (сеть или аккумулятор).

Запуск приложения

В Консоли администрирования вы можете настраивать параметры запуска приложения в свойствах политики (**Общие параметры** → **Параметры приложения**, блок **Параметры запуска приложения**).

В блоке **Параметры запуска приложения** по нажатию на кнопку **Настроить** открывается окно **Параметры запуска приложения**, в котором вы можете настроить параметры запуска приложения (см. таблицу ниже).

Параметры запуска приложения

Параметр	Описание
Максимальное количество неудачных последовательных попыток запуска приложения	Поле ввода максимального количества неудачных последовательных попыток запуска приложения. Значение по умолчанию: 5.
Максимальное время ожидания запуска приложения (мин.)	Поле ввода максимального времени ожидания запуска приложения (в минутах), после которого процесс kesl будет перезапущен. Значение по умолчанию: 3.

Автоматический перезапуск при получении критических обновлений

В Консоли администрирования вы можете настраивать автоматический перезапуск приложения при получении критически важных обновлений в свойствах политики (**Общие параметры** → **Параметры приложения**).

В блоке **Дополнительные параметры приложения** по нажатию на кнопку **Настроить** открывается окно **Дополнительные параметры**, в котором вы можете настроить перезапуск приложения при получении критических обновлений (см. таблицу ниже).

Параметры применения критических обновлений

Параметр	Описание
Автоматически перезапускать приложение при получении критических обновлений	Флажок включает или выключает автоматический перезапуск приложения при получении критически важных обновлений по истечении первых суток после установки приложения. По умолчанию флажок снят. Если флажок установлен, то при получении критически важных обновлений по истечении первых суток после установки приложение будет перезапущено.

Защита паролем

В Консоли администрирования вы можете настраивать параметры защиты паролем в свойствах политики (**Общие параметры** → **Интерфейс**, блок **Защита паролем**).

В блоке **Защита паролем** по нажатию на кнопку **Настроить** открывается окно **Настройка защиты паролем**, в котором вы можете настроить параметры защиты паролем (см. таблицу ниже).

Параметры запуска приложения

Параметр	Описание
Включить защиту паролем	Флажок включает или выключает защиту паролем параметров приложения от изменения. По умолчанию флажок снят.
Разрешения	Таблица содержит пользователей и групп, для которых можно настроить разрешения на изменение параметров приложения. Таблица состоит из следующих столбцов: • **Пользователь / Группа** – имя локального или доменного пользователя или название группы пользователей, для которых настраиваются разрешения. • **Тип** – **Пользователь** или **Группа**, для которых настраиваются разрешения. • **Разрешения** – список операций, которые разрешено выполнять пользователю или группе пользователей. Вы можете добавлять, изменять и удалять пользователей и группы пользователей. При нажатии на кнопку **Добавить** открывается окно **Разрешения пользователя / группы**, в котором вы можете добавить пользователя или группу и указать для них разрешения на изменение параметров приложения.

Параметры трассировки и записи дампов

В Консоли администрирования вы можете настраивать параметры трассировки и записи дампов в свойствах политики (**Общие параметры** → **Параметры приложения**, блок **Параметры трассировки и записи дампов**).

В блоке **Параметры трассировки и записи дампов** по нажатию на кнопку **Настроить** открывается окно **Параметры трассировки и записи дампов**, в котором вы можете настроить параметры трассировки и записи дампов (см. таблицу ниже).

Параметры трассировки и записи дампов

Параметр	Описание
Путь к директории с файлами трассировки	Поле ввода пути к директории, в которой хранятся файлы трассировки. Значение по умолчанию: /var/log/kaspersky/kesl. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, под которой работает Kaspersky Endpoint Security. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права.
Максимальный размер файла трассировки (МБ)	Поле ввода максимального размера файла трассировки приложения (в мегабайтах). Значение по умолчанию: 500.
Максимальное количество файлов трассировки	Поле ввода максимального количества файлов трассировки приложения. Значение по умолчанию: 10.
Создавать файл дампа при сбое в работе приложения	Флажок включает или выключает создание файла дампа при сбое в работе приложения. По умолчанию флажок снят.
Путь к директории с файлами дампа	Поле ввода пути к директории, в которой хранятся файлы дампа. Размер поля ввода ограничен 128 символами. Значение по умолчанию: /var/opt/kaspersky/kesl/common/dumps.

Использование резидентной памяти приложением

В Консоли администрирования вы можете настраивать ограничение на использование резидентной памяти приложением в свойствах политики (**Общие параметры** → **Параметры приложения**).

В блоке **Дополнительные параметры приложения** по нажатию на кнопку **Настроить** открывается окно **Дополнительные параметры**, в котором вы можете настроить ограничение на использование резидентной памяти (см. таблицу ниже).

Чтобы измененные настройки вступили в силу, после применения политики на управляемом устройстве перезапустите приложение Kaspersky Endpoint Security.

Параметры использования резидентной памяти приложением

Параметр	Описание
Использование памяти приложением	В раскрывающемся списке вы можете выбрать способ ограничения на использование резидентной памяти: • **Не ограничено**. При выборе этого элемента списка использование резидентной памяти не ограничивается. • **Ограничивается автоматически (рекомендуется)**. При выборе этого элемента списка использование резидентной памяти ограничивается автоматически (значение по умолчанию). • **Ограничено значением в процентах от общего объема**. При выборе этого элемента списка становится доступно поле **Ограничение на использование памяти (%)**, в котором вы можете указать нужное значение в процентах. • **Ограничено значением в мегабайтах**. При выборе этого элемента списка становится доступно поле **Ограничение на использование памяти (МБ)**, в котором вы можете указать нужное значение в мегабайтах. • **Ограничено наименьшим из указанных значений (%, МБ)**. При выборе этого элемента списка становятся доступны поля **Ограничение на использование памяти (%)** и **Ограничение на использование памяти (МБ)**, в которых вы можете указать нужные значения. • **Ограничено наибольшим из указанных значений (%, МБ)**. При выборе этого элемента списка становятся доступны поля **Ограничение на использование памяти (%)** и **Ограничение на использование памяти (МБ)**, в которых вы можете указать нужные значения.
Ограничение на использование памяти (%)	Поле ввода ограничения на использование памяти (в процентах). Значение по умолчанию: 50.
Ограничение на использование памяти (МБ)	Поле ввода ограничения на использование памяти (в мегабайтах). Значение по умолчанию: 2000.

Проверка зашифрованных соединений

В Консоли администрирования вы можете настраивать параметры проверки сетевого трафика в свойствах политики (**Общие параметры** → **Параметры сети**).

Параметры проверки зашифрованных соединений

Параметр	Описание
Включить проверку зашифрованных соединений	Флажок включает или выключает проверку зашифрованных соединений. По умолчанию флажок установлен.

Параметры зашифрованных соединений	Блок содержит параметры проверки зашифрованных соединений:
	• **Переход на домен с недоверенным сертификатом** – действие, которое приложение будет выполнять при переходе на домен с недоверенным сертификатом:
	  • **Разрешать** (значение по умолчанию) – разрешать подключение к домену с недоверенным сертификатом.
	  • **Блокировать** – блокировать подключение к домену с недоверенным сертификатом.
	• **Переход на домен с ошибкой проверки сетевого трафика** – действие, которое приложение будет выполнять при переходе на домен с ошибкой проверки сетевого трафика:
	  • **Добавлять домен в исключения** (значение по умолчанию) – добавить домен, вызвавший ошибку, в список доменов с ошибками при проверке и не проверять зашифрованный сетевой трафик при посещении этого домена.
	  • **Блокировать** – блокировать подключение к домену с ошибкой проверки.
	• **Политика проверки сертификатов** – способ проверки сертификатов приложением:
	  • **Локальная проверка** – приложение не использует интернет для проверки сертификата.
	  • **Полная проверка** (значение по умолчанию) – приложение использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата.

Доверенные домены	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Доверенные домены, в котором вы можете настроить список имен доверенных доменов.
Доверенные корневые сертификаты	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно Доверенные корневые сертификаты. В этом окне вы можете настроить список корневых сертификатов, которые приложение Kaspersky Endpoint Security будет считать доверенными при проверке зашифрованных соединений.

Параметр	Описание
Исключения из перехвата трафика	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения из перехвата трафика**. В этом окне вы можете настроить параметры соединений, трафик которых приложение исключает из перехвата.
Параметры сетевых портов	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Контролируемые порты**.
Дополнительные параметры	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Режим перехвата трафика**. В этом окне вы можете настроить режим перехвата трафика, который приложение использует в своей работе: • **Использовать технологию eBPF**. Если выбран этот вариант, приложение использует для перехвата трафика технологию eBPF. • **Использовать утилиту iptables** (значение по умолчанию). Если выбран этот вариант, приложение использует для перехвата трафика утилиту iptables. Для изменения режима перехвата трафика требуется перезапустить приложение. Во время перезапуска происходит разрыв установленных сетевых соединений.

Окно Доверенные домены

Список содержит доменные имена и маски доменных имен, которые будут исключены из проверки. Приложение не проверяет соединения, установленные при посещении указанных доменов.

Пример: `*example.com`. Например, `*example.com/*` – это неправильное значение, так как требуется указывать адрес домена, а не веб-страницы.

По умолчанию список пуст. Вы можете добавлять, изменять и удалять домены в списке доверенных доменов.

Окно Доверенные корневые сертификаты

Вы можете настроить список корневых сертификатов, которые приложение Kaspersky Endpoint Security будет считать доверенными. Список корневых доверенных сертификатов используется при проверке зашифрованных соединений.

Для каждого сертификата отображаются следующие сведения:

- субъект сертификата;
- серийный номер сертификата;
- издатель сертификата;
- дата начала срока действия сертификата;
- дата окончания срока действия сертификата;
- отпечаток сертификата SHA256.

По умолчанию список сертификатов пуст.

Вы можете добавлять и удалять сертификаты.

По нажатию на кнопку **Добавить** открывается окно, в котором вы можете добавить сертификат в список доверенных сертификатов одним из следующих способов:

- Указать путь к файлу сертификата. По кнопке **Обзор** открывается стандартное окно для выбора файла. Укажите путь к файлу формата DER или PEM, содержащему сертификат.
- Скопировать содержимое файла сертификата в поле **Ввести данные сертификата**.

Окно Исключения из перехвата трафика

Таблица содержит параметры соединений, которые приложение исключает из перехвата трафика:

- **Удаленный IP-адрес** – IP-адрес, трафик на который или трафик с которого исключается из перехвата (в зависимости от направления трафика).
- **Порт назначения** – порт на защищенном устройстве (в исключении из перехвата входящего трафика) или порт на удаленном устройстве (в исключении из перехвата исходящего трафика).
- **Направление трафика** – направление трафика в соединении: входящий или исходящий.

Вы можете добавлять, изменять и удалять исключения.

Окно Исключение из перехвата трафика

В этом окне вы можете добавить исключение из перехвата трафика. Для этого вам нужно указать следующие параметры соединения:

- **Удаленный IP-адрес** – адрес удаленного устройства в формате IPv4 или IPv6. В зависимости от направления трафика будет исключаться трафик с указанного IP-адреса (исключение для входящего трафика) или трафик на указанный IP-адрес (исключение для исходящего трафика).
- **Порт назначения** – в зависимости от направления трафика:
  - Порт на защищенном устройстве (исключение для входящего трафика). Из перехвата будет исключаться трафик на этот порт с удаленных устройств.
  - Порт на удаленном устройстве (исключение для исходящего трафика). Из перехвата будет исключаться трафик на этот порт с защищенного устройства.
- **Направление трафика** – направление трафика в исключаемом соединении. Вы можете настроить исключение для входящего трафика или для исходящего трафика.

Вы можете указать в исключении только IP-адрес удаленного устройства или только порт назначения.

> Если в исключении для входящего трафика вы указываете только IP-адрес удаленного устройства (без указания порта на защищенном устройстве), весь трафик с удаленного устройства исключается из перехвата. Настраивать такое исключение рекомендуется только для трафика с устройств, которым вы доверяете.

Окно Контролируемые порты

Параметры сетевых портов

Параметр	Описание
Контролировать все сетевые порты	Если выбран этот вариант, приложение проверяет все сетевые порты.
Контролировать только выбранные сетевые порты	Если выбран этот вариант, приложение проверяет только сетевые порты, указанные в таблице. Этот вариант выбран по умолчанию.
Параметры сетевых портов	Таблица содержит сетевые порты, которые будет проверять приложение, если выбран вариант **Контролировать только выбранные сетевые порты**. Таблица содержит два столбца: • **Порт** – контролируемый порт. • **Описание** – описание контролируемого порта. По умолчанию в таблице отображается список сетевых портов, которые обычно используются для передачи почтового и сетевого трафика. Список сетевых портов входит в пакет приложения. Элементы в таблице можно добавлять, изменять и удалять.

Глобальные исключения

В Консоли администрирования вы можете настраивать глобальные исключения в свойствах политики (**Общие параметры** → **Глобальные исключения**).

Блок параметров **Исключенные точки монтирования** содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключенные точки монтирования**.

Список в окне содержит пути к исключенным точкам монтирования. По умолчанию список пуст.

Элементы в списке можно добавлять, изменять и удалять.

Окно Путь к точке монтирования

Параметры точки монтирования

Параметр	Описание
Файловая система, протокол доступа и путь	Блок параметров позволяет задать расположение точки монтирования. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные точки монтирования. • **Смонтированная** – удаленные директории, смонтированные на устройстве по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – все ресурсы файловой системы устройства, указанной в поле ниже.

Параметр	Описание
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к точке монтирования, которую вы хотите добавить в исключения из перехвата файловых операций. Для указания пути вы можете использовать маски. Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды `mount`.
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из перехвата файловых операций. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Смонтированная** и в раскрывающемся списке справа выбран элемент **Пользовательская**.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Исключение памяти процессов из проверки

В Консоли администрирования вы можете настраивать исключения памяти процессов из проверки в свойствах политики (**Общие параметры** → **Исключение памяти процессов**).

По кнопке **Настроить** в блоке **Исключение памяти процессов из проверки** открывается окно, в котором вы можете сформировать список исключений.

Список в окне **Исключение памяти процессов из проверки** содержит пути к процессам, которые приложение исключает из проверки памяти процессов. Для указания пути вы можете использовать маски. По умолчанию список пуст.

Вы можете включить объединение списка исключений при наследовании в дочерних политиках. Для объединения элементов списка требуется установить флажок **Объединять значения при наследовании** в окне **Исключение памяти процессов из проверки**. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.

Полезные статьи

Как задавать маски

Вы можете использовать символ `*` (звездочка) для формирования маски имени файла или директории.

Вы можете указать один символ `*` вместо любого набора символов (включая пустой набор), предшествующего символу `/` в имени файла или директории. Например, `/dir/*/file` или `/dir/*/*/file`.

Вы можете указать два последовательно идущих символа `*` вместо любого набора символов (включая пустой набор) в имени файла или директории, включающего символ `/`. Например, `/dir/**/file*/` или `/dir/file**/`.

Маску `**` можно использовать в имени директории только один раз. Например, `/dir/**/**/file` – это неправильная маска.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Резервное хранилище

В Консоли администрирования вы можете настраивать параметры резервного хранилища в свойствах политики (**Общие параметры** → **Параметры хранилищ**) и в свойствах управляемого устройства (**Управляемые устройства** → вкладка **Устройства** → окно свойств устройства → раздел **Приложения** → окно свойств приложения → **Параметры хранилищ**).

Параметры резервного хранилища

Параметр	Описание
Хранить объекты не более (дней)	Флажок включает или выключает ограничение срока хранения объектов в резервном хранилище заданным интервалом времени. Доступные значения: 0–10000. Если задано значение 0, период хранения объектов в резервном хранилище не ограничен. Значение по умолчанию: 30.
Ограничить размер резервного хранилища до (МБ)	Флажок включает или выключает ограничение максимального размера резервного хранилища заданным значением (в мегабайтах). Доступные значения: 1–4000. Если флажок снят, размер резервного хранилища не ограничен. По умолчанию флажок снят.

Обнаружение приложений, которые злоумышленники могут использовать для нанесения вреда

В Консоли администрирования вы можете включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным, в свойствах политики (**Общие параметры** → **Параметры приложения**, блок **Параметры проверки**).

Параметры обнаружения приложений, которые злоумышленники могут использовать для нанесения вреда

Параметр	Описание
Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным	Флажок включает или выключает обнаружение легальных приложений, через которые злоумышленники могут навредить устройству или данным пользователя. По умолчанию флажок снят.

Перехват файловых операций

В Консоли администрирования вы можете настраивать режим перехвата файлов в свойствах политики (**Общие параметры** → **Параметры приложения**, блок **Режим перехвата файловых операций**).

Параметры перехвата файловых операций

Параметр	Описание
Блокировать доступ к файлам во время проверки	Флажок включает или выключает блокировку доступа к файлам во время проверки компонентами Защита от файловых угроз и Контроль устройств, действия Запрет запуска объектов и задачи Проверка съемных дисков. По умолчанию флажок установлен. Если флажок снят, во время проверки обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме.

Отправка информации в хранилище Kaspersky Security Center

В Kaspersky Security Center вы можете включать и выключать отправку в хранилище Kaspersky Security Center информации о файлах в резервном хранилище, файлах на карантине, необработанных файлах и о подключенных устройствах.

Общий список файлов, помещенных на карантин приложениями "Лаборатории Касперского" на клиентских устройствах, формируется в Kaspersky Security Center и доступен в Консоли администрирования (**Дополнительно** → **Хранилища** → **Карантин**).

Общий список файлов, помещенных в резервное хранилище приложениями "Лаборатории Касперского" на клиентских устройствах, формируется в Kaspersky Security Center и доступен в Консоли администрирования (**Дополнительно** → **Хранилища** → **Резервное хранилище**).

Информация о необработанных файлах отображается в списке активных угроз в Консоли администрирования (**Дополнительно** → **Хранилища** → **Активные угрозы**).

Информация об устройствах, установленных на клиентском устройстве или подключенных к нему, отображается в списке оборудования в Консоли администрирования (**Дополнительно** → **Хранилища** → **Оборудование**). Информация передается, если включен компонент Контроль устройств.

Информация о приложениях, обнаруженных на клиентском устройстве, также отображается в списке приложений в Консоли администрирования (**Дополнительно** → **Управление приложениями** → **Реестр приложений**). Информация передается, если включен компонент Контроль приложений.

Включение и выключение отправки информации в Консоли администрирования

В Консоли администрирования вы можете включать и выключать отправку информации на Сервер администрирования в свойствах политики (**Общие параметры** → **Параметры хранилищ**, блок **Передача данных на Сервер администрирования**) и в свойствах управляемого устройства (**Управляемые устройства** → вкладка **Устройства** → окно свойств устройства → раздел **Приложения** → окно свойств приложения → **Параметры хранилищ**, блок **Передача данных на Сервер администрирования**).

По нажатию на кнопку **Настроить** в блоке **Передача данных на Сервер администрирования** открывается окно **Параметры передачи данных**, в котором вы можете вы можете включать и выключать отправку информации на Сервер администрирования.

Параметры передачи данных на Сервер администрирования

Параметр	Описание
О файлах карантина	Флажок включает или выключает передачу на Сервер администрирования информации о файлах, помещенных на карантин. По умолчанию флажок установлен.
О файлах резервного хранилища	Флажок включает или выключает передачу на Сервер администрирования информации о файлах в резервном хранилище. По умолчанию флажок установлен.
О необработанных файлах	Флажок включает или выключает отправку уведомлений о файлах, не обработанных во время проверки, на Сервер администрирования. По умолчанию флажок установлен.
Об установленных устройствах	Флажок включает или выключает передачу на Сервер администрирования информации об устройствах, установленных на клиентском устройстве или подключенных к нему. По умолчанию флажок установлен.
О приложениях, обнаруженных на устройстве	Флажок включает или выключает передачу на Сервер администрирования списка приложений, обнаруженных на клиентском устройстве в результате работы задачи инвентаризации. По умолчанию флажок установлен.

Перехват системных событий

В Консоли администрирования вы можете настраивать параметры перехвата системных событий в свойствах политики (**Общие параметры** → **Параметры взаимодействия с ОС**, блок **Параметры перехвата системных событий**).

Параметры применяются только на устройствах, где операционная система поддерживает технологию fanotify.

Параметры перехвата системных событий

Параметр	Описание
Механизм перехвата	Механизм перехвата системных событий, который приложение использует в своей работе: • **Технология fanotify** (значение по умолчанию). Если выбран этот вариант, приложение использует технологию fanotify для перехвата системных событий. • **Обновляемый модуль ядра**. Если выбран этот вариант, приложение использует обновляемый модуль ядра для перехвата системных событий.

Параметр	Описание
Если обновляемый модуль ядра не запускается	Действие, которое приложение выполняет в случае ошибки запуска обновляемого модуля ядра: • **Использовать технологию fanotify** (значение по умолчанию). Если выбран этот вариант, приложение переходит к использованию технологии fanotify для перехвата системных событий. • **Выключить перехват системных событий**. Если приложение не использует перехват системных событий, проверка файлов в режиме реального времени не выполняется, уровень защиты устройства снижается. Параметр доступен, если выбран механизм перехвата **Обновляемый модуль ядра**.

Дополнительные параметры телеметрии

В Консоли администрирования вы можете настраивать дополнительные параметры сбора телеметрии в свойствах политики (**Общие параметры** → **Параметры взаимодействия с ОС**, блок **Дополнительные параметры телеметрии**).

Дополнительные параметры сбора телеметрии

Параметр	Описание
Источник телеметрии	Источник, который использует приложение Kaspersky Endpoint Security для сбора телеметрии: • **Использовать только eBPF** – использовать для сбора телеметрии только технологию eBPF. • **Использовать eBPF и auditd** (значение по умолчанию) – использовать для сбора телеметрии технологию eBPF и службу auditd.
Использование auditd	Режим использования службы auditd: • **В монопольном режиме** (значение по умолчанию) – приложение Kaspersky Endpoint Security использует службу auditd в монопольном режиме. • **В режиме многоадресной рассылки** – служба auditd используется в режиме многоадресной рассылки. Параметр применяется, только если для параметра **Источник телеметрии** выбран вариант **Использовать eBPF и auditd**.

Режим Легкого агента

В Консоли администрирования вы можете настраивать параметры подключения Легкого агента к SVM в свойствах политики (**Режим Легкого агента**).

Подключение к Серверу интеграции

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Подключение к Серверу интеграции требуется, если вы хотите, чтобы Легкие агенты получали информацию об SVM через Сервер интеграции, или если вы хотите защищать соединение между Сервером защиты и Легким агентом.

В этом окне отображаются текущие параметры подключения Легких агентов к Серверу интеграции: адрес и порт для подключения. По нажатию на кнопку **Изменить** открывается окно **Подключение к Серверу интеграции**, в котором вы можете настроить подключение к Серверу интеграции.

Окно Подключение к Серверу интеграции

В этом окне вы можете указать или изменить параметры подключения Легких агентов к Серверу интеграции.

Параметры подключения к Серверу интеграции

Параметр	Описание
Адрес	IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции. Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, входит в домен, в поле по умолчанию указано доменное имя этого устройства. Если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или Сервер интеграции установлен на другом устройстве, поле требуется заполнить вручную. Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.
Порт	Порт для подключения к Серверу интеграции. По умолчанию указан порт 7271.

Если в вашей инфраструктуре развернут отказоустойчивый кластер Серверов интеграции на базе Linux, в качестве адреса и порта для подключения к Серверу интеграции вам нужно указать адрес и порт балансировщика нагрузки. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Окно Проверка сертификата Сервера интеграции

Это окно отображается, если SSL-сертификат, полученный от Сервера интеграции, содержит ошибку или не является доверенным.

С помощью ссылки в окне вы можете посмотреть информацию о полученном сертификате.

При возникновении проблем с SSL-сертификатом рекомендуется убедиться в безопасности используемого канала передачи данных.

Чтобы продолжить подключение к Серверу интеграции, нажмите на кнопку **Игнорировать**. Полученный сертификат будет установлен в качестве доверенного на устройстве, где установлена Консоль администрирования Kaspersky Security Center.

Окно Аутентификация на Сервере интеграции

Это окно отображается, если устройство, на котором установлена Консоль администрирования Kaspersky Security Center, не входит в домен или ваша учетная запись не входит в локальную или доменную группу KLAdmins или в группу локальных администраторов.

Укажите пароль администратора Сервера интеграции (пароль учетной записи `admin`) и нажмите на кнопку **OK**.

> Рекомендуется убедиться, что сложность пароля и механизмы защиты от перебора гарантируют невозможность подбора пароля за 6 месяцев.

После подключения к Серверу интеграции с правами администратора в политику автоматически передается пароль учетной записи `agent`, которая используется для подключения Легких агентов к Серверу интеграции.

Параметры обнаружения SVM

> Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента.

В этом окне вы можете выбрать способ, который используют Легкие агенты для обнаружения доступных для подключения SVM.

Параметры обнаружения SVM

Параметр	Описание
Использовать Сервер интеграции	Если выбран этот вариант, Легкий агент подключается к Серверу интеграции для получения списка доступных для подключения SVM и информации о них. Если вы хотите использовать Сервер интеграции, вам нужно настроить параметры подключения Легких агентов к Серверу интеграции.
Использовать список адресов SVM, заданный вручную	Если выбран этот вариант, вы можете указать список SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением этой политики. Легкие агенты будут подключаться только к SVM, указанным в списке.
Список SVM	Список IP-адресов в формате IPv4 или полных доменных имен (FQDN) SVM, к которым могут подключаться Легкие агенты, находящиеся под управлением политики. По нажатию на кнопку **Добавить** открывается окно, в котором вы можете указать IP-адрес в формате IPv4 или полное доменное имя (FQDN) SVM. Вы можете ввести несколько IP-адресов или полных доменных имен SVM с новой строки. Требуется указывать только полные доменные имена (FQDN), которым сопоставляется единственный IP-адрес. Использование полного доменного имени, которому соответствует несколько IP-адресов, может привести к ошибкам в работе приложения. Вы можете удалять выбранные в списке адреса по нажатию на кнопку **Удалить**. Список адресов SVM отображается, если выбран вариант **Использовать список адресов SVM, заданный вручную**.

> Если вы выбрали вариант **Использовать список адресов SVM, заданный вручную** и для Легкого агента применяется расширенный алгоритм выбора SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. В разделе **Алгоритм выбора SVM** требуется установить для параметра **Расположение SVM** значение **Игнорировать**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

Тег для подключения к SVM

В этом окне вы можете включить использование тегов Легким агентом и назначить тег, который Легкий агент будет использовать для подключения.

Убедитесь, что использование тегов для подключения также настроено в параметрах Сервера защиты: см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент. Легкие агенты, которым назначен тег, могут подключаться только к SVM, для которых разрешено подключение Легких агентов с этим тегом.

Параметры использования тегов для подключения

Параметр	Описание
Использовать тег для подключения	Флажок включает или выключает использование Легким агентом тегов для подключения к SVM.
Тег	Тег, который назначается Легким агентам. В качестве тега вы можете ввести текстовую строку длиной не более 255 символов. Вы можете использовать любые символы, кроме символа `;`. Поле доступно, если установлен флажок **Использовать тег для подключения**.

Алгоритм выбора SVM

В этом окне вы можете указать, какой алгоритм выбора SVM должны использовать Легкие агенты, и настроить параметры применения расширенного алгоритма выбора SVM.

Алгоритм выбора SVM

Параметр	Описание
Использовать стандартный алгоритм выбора SVM	Если выбран этот вариант, после установки и запуска на виртуальной машине Легкий агент выбирает для подключения SVM, которая является локальной для Легкого агента. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент. Если нет доступных для подключения локальных SVM, Легкий агент выбирает SVM, к которой подключено наименьшее количество Легких агентов, независимо от расположения SVM в виртуальной инфраструктуре. Этот вариант выбран по умолчанию.
Использовать расширенный алгоритм выбора SVM	Если выбран этот вариант, вы можете указать с помощью ползунка **Расположение SVM**, как расположение SVM в виртуальной инфраструктуре будет учитываться при определении локальности SVM относительно Легкого агента. Легкий агент сможет подключаться только к тем SVM, которые являются локальными. Также вы можете указать, что расположение SVM в виртуальной инфраструктуре не должно учитываться при выборе SVM для подключения. При выборе SVM Легкие агенты учитывают количество Легких агентов, подключенных к этой SVM, чтобы обеспечить равномерное распределение Легких агентов между доступными для подключения SVM.

Параметр	Описание

Расположение SVM	Позволяет указать тип расположения SVM в виртуальной инфраструктуре, который учитывается при выборе SVM для подключения:
	• **Гипервизор**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):
	  • SVM развернута на том же гипервизоре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Numa vServer или Базис Dynamix Standard).
	  • SVM находится в той же Группе серверов, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack или Private Cloud от VK).
	  • SVM находится на том же вычислительном узле, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).
	  Если на том же гипервизоре или в той же Группе серверов, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.
	• **Кластер**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):
	  • SVM развернута в том же кластере гипервизоров, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Numa vServer или Базис Dynamix Standard).
	  • SVM развернута в рамках того же проекта OpenStack, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack или Private Cloud от VK).
	  • SVM находится в той же зоне, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).
	  Если в том же кластере гипервизоров или в рамках того же проекта OpenStack, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.
	• **Дата-центр**. Легкий агент выбирает для подключения SVM, соответствующую критерию (в зависимости от вида виртуальной инфраструктуры):
	  • SVM развернута в том же дата-центре, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре на платформе Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Базис, HUAWEI FusionSphere, Nutanix Acropolis, Альт Сервер Виртуализации, Astra Linux, Numa vServer или Базис Dynamix Standard).
	  • SVM расположена в той же Зоне доступности, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре под управлением платформы OpenStack или Private Cloud от VK).
	  • SVM находится в том же ЦОД, что и виртуальная машина с установленным Легким агентом (в виртуальной инфраструктуре Базис Dynamix Enterprise).
	  Если в том же дата-центре или в той же Зоне доступности, где расположена виртуальная машина с Легким агентом, нет доступных для подключения SVM, Легкий агент не подключается к SVM.
	• **Игнорировать**. Легкий агент не учитывает при выборе SVM ее расположение.
	По умолчанию выбрано значение **Гипервизор**.
	Параметр доступен, если выбран вариант **Использовать расширенный алгоритм выбора SVM**.

Если для Легкого агента применяется расширенный алгоритм выбора SVM и в качестве способа обнаружения SVM выбран список адресов SVM, а на SVM включен режим защиты больших инфраструктур (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент), то подключение Легкого агента к этой SVM возможно, только если расположение SVM не учитывается. Требуется установить для параметра **Расположение SVM** значение **Игнорировать**. Если установлено любое другое значение, Легкий агент не сможет подключиться к SVM.

Защита соединения

В этом окне вы можете включить шифрование канала передачи данных между Легким агентом и Сервером защиты.

Убедитесь, что шифрование канала передачи данных между Легким агентом и Сервером защиты включено в параметрах Сервера защиты на SVM. См. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Параметры защиты соединения

Параметр	Описание
Шифровать канал передачи данных между Легким агентом и Сервером защиты	Защитить соединение между Легкими агентами и Сервером защиты с помощью шифрования. Если флажок установлен, между Легким агентом, находящимся под управлением политики, и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается защищенное соединение. Легкий агент, для которого включена защита соединения, может подключиться только к SVM, на которой также включена защита соединения или разрешено незащищенное соединение с Сервером защиты. Если флажок снят, между Легким агентом и Сервером защиты на SVM, к которой подключается Легкий агент, устанавливается незащищенное соединение. По умолчанию флажок снят.

Известные проблемы и ограничения

Ограничения работы приложения

Не поддерживается работа приложения Kaspersky Endpoint Security в следующих случаях:

- На операционных системах ОСнова в режиме замкнутой программной среды и в режиме hardened kernel.
- На операционных системах, построенных на основе Red Hat Enterprise Linux, в подсистеме IMA.
- На операционных системах, построенных на основе Red Hat Enterprise Linux, в режиме FIPS.
- На операционных системах Ubuntu и операционных системах, построенных на основе SUSE Linux Enterprise Server, в системе мандатного управления доступом AppArmor.
- В системы безопасности Grsecurity (на всех операционных системах).
- При использовании механизма seccomp (на всех операционных системах).
- При использовании технологий WSL1 и WSL2 (на всех операционных системах).
- При использовании параметров монтирования файловых систем (например, noexec, nosuid и других).
- При установке приложения Kaspersky Endpoint Security внутри контейнера.

Решения Detection and Response могут работать некорректно на виртуальных машинах, созданных из образа с установленным Kaspersky Endpoint Security для Linux. При интеграции с решениями Detection and Response используется уникальный идентификатор компьютера (Sensor ID). Приложение создает этот идентификатор при первой установке и сохраняет его даже после удаления. При клонировании образа виртуальная машина наследует Sensor ID, из-за чего решения Detection and Response могут определять несколько виртуальных машин как одно устройство.

Ограничения работы приложения на некоторых типах архитектуры

Приложение имеет ограничения при работе на следующих типах архитектуры процессора:

Эльбрус

- Режим Легкого агента: не поддерживается.
- Режим EDR-агента: не поддерживается.
- Защита от атак BadUSB: не работает.
- Защита от эксплойтов: не работает.
- Защита от веб-угроз: недоступно использование эвристического анализа при проверке веб-страниц на наличие фишинговых ссылок.

- Интеграция с Kaspersky Endpoint Detection and Response Optimum: не работает.
- Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud): не работает.
- Интеграция с Kaspersky Endpoint Detection and Response (KATA): не работает.
- Интеграция с Kaspersky Managed Detection and Response: не работает.
- Sandbox: не работает.
- Интеграция с KUMA: не работает.
- Проверка контейнеров: не работает.
- Обновляемый модуль ядра: не поддерживается.
- Графический пользовательский интерфейс управления: пользователям недоступна отправка файлов на проверку в Sandbox, так как не поддерживается компонент Sandbox.

Ограничения работы приложения на некоторых операционных системах

Приложение имеет ограничения при работе на следующих операционных системах:

Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5)

- Защита от атак BadUSB: не работает, так как отсутствует служба systemd-logind в операционной системе.
- Ограничение на использование ресурсов процессора для задач Поиск вредоносного ПО, Проверка важных областей, Инвентаризация и Проверка контейнеров не работает на ядрах "4.2.0-23-generic".

CentOS 5.2 и 5.4

- Анализ поведения: корректная работа компонента не гарантируется, так как отсутствуют синхронные перехваты старта процессов.
- Защита от почтовых угроз: не работает.
- Защита от веб-угроз: не работает, так как нет поддержки механизма TProxy.
- Защита от сетевых угроз: не работает, так как нет поддержки механизма TProxy.
- Защита от шифрования: не работает, так как нет поддержки механизма TProxy.
- Защита от атак BadUSB: не работает, так как отсутствует служба systemd-logind в операционной системе.
- Проверка контейнеров: не работает, так как нет поддержки контейнеров в операционной системе.
- Контроль устройств: режим ReadOnly для устройств работает только в том случае, если устройство было подключено после активации режима в приложении. Для устройств, подключенных до активации этого режима, режим доступа остается без изменений.

- Контроль приложений: не работает, так как отсутствует поддержка технологии fanotify, необходимой для синхронного перехвата старта процессов.
- Управление сетевым экраном: не работает, так как отсутствует поддержка добавления цепочек в iptables.
- Веб-Контроль: не работает, так как нет поддержки механизма TProxy.
- Обновляемый модуль ядра: не поддерживается.
- Сетевая изоляция: не работает, так как нет поддержки механизма TProxy.
- Запрет запуска объектов: не работает, так как отсутствуют синхронные перехваты старта процессов.
- Интеграция с Kaspersky Endpoint Detection and Response Optimum: не работает.
- Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud): не работает.
- Интеграция с Kaspersky Endpoint Detection and Response (KATA): недоступен источник телеметрии eBPF.
- Интеграция с Kaspersky Managed Detection and Response: недоступен источник телеметрии auditd.
- Графический пользовательский интерфейс управления: не работает, так как в операционной системе отсутствует библиотека libxcb.
- Агент администрирования Kaspersky Security Center: требуется дополнительная настройка устройства, см. справку Kaspersky Security Center.
- Установка/удаление: приложение несовместимо с SELinux этих версий операционной системы. Возможное решение: перевести SELinux в неблокирующий режим (режим permissive); отключить SELinux или настроить SELinux вручную.
- Поиск вредоносного ПО: на операционных системах, где версия glibc ниже 2.11, не выполняется лечение и удаление файлов, расположенных в директориях с длиной пути более 4096 символов.
- Ограничение на использование ресурсов процессора для задач Поиск вредоносного ПО, Проверка важных областей, Инвентаризация и Проверка контейнеров не работает.
- Не поддерживается работа приложения в режиме Легкого агента, поэтому при установке приложения параметры KSVLA_MODE, SERVER_MODE, VDI_MODE неприменимы.
- Не поддерживается работа приложения в режиме EDR-агента.
- Не поддерживается работа приложения в Kaspersky Security Center Cloud Console.
- Не поддерживается работа приложения с файловыми системами, основанными на технологии FUSE.
- Не собирается статистика наиболее часто проверяемых файлов.
- В некоторых случаях телеметрия, передаваемая при интеграции с Kaspersky Endpoint Detection and Response (KATA), может содержать неполную информацию о событиях из журналов системных событий.

CentOS 6.4 и 6.6

- Анализ поведения: корректная работа компонента не гарантируется, так как отсутствуют синхронные перехваты старта процессов.
- Защита от веб-угроз: не работает перехват IPv6-трафика.
- Защита от сетевых угроз: не работает перехват IPv6-трафика.
- Защита от шифрования: не работает перехват IPv6-трафика.
- Защита от атак BadUSB: не работает, так как отсутствует служба systemd-logind в операционной системе.
- Проверка контейнеров: не работает, так как нет поддержки контейнеров в операционной системе.
- Контроль приложений: не работает, так как отсутствует поддержка технологии fanotify, необходимой для синхронного перехвата старта процессов.
- Управление сетевым экраном: не работают IPv6-правила сетевого экрана.
- Веб-Контроль: не работает перехват IPv6-трафика.
- Обновляемый модуль ядра: не поддерживается.
- Запрет запуска объектов не работает, так как отсутствуют синхронные перехваты старта процессов.
- Kaspersky Endpoint Detection and Response Optimum: цепочка развития угрозы не отображает сетевую активность, так как нет поддержки механизма TProxy; доступны только события телеметрии об операциях с файлами; запрет запуска объектов не работает, так как отсутствуют синхронные перехваты старта процессов.
- Интеграция с Kaspersky Endpoint Detection and Response Expert (cloud): не работает.
- Интеграция с Kaspersky Endpoint Detection and Response (KATA): недоступен источник телеметрии eBPF.
- Интеграция с Kaspersky Managed Detection and Response: недоступен источник телеметрии auditd.
- Агент администрирования Kaspersky Security Center: требуется дополнительная настройка устройства, см. справку Kaspersky Security Center.
- Установка/удаление: приложение несовместимо с SELinux этих версий операционной системы. Возможное решение: перевести SELinux в неблокирующий режим (режим permissive); отключить SELinux или настроить SELinux вручную.
- Поиск вредоносного ПО: на операционных системах, где версия glibc ниже 2.11, не выполняется лечение и удаление файлов, расположенных в директориях с длиной пути более 4096 символов.
- Не поддерживается работа приложения в режимах Легкого агента и EDR-агента.
- Не поддерживается работа приложения в Kaspersky Security Center Cloud Console.
- Не собирается статистика наиболее часто проверяемых файлов.
- В некоторых случаях телеметрия, передаваемая при интеграции с Kaspersky Endpoint Detection and Response (KATA), может содержать неполную информацию о событиях из журналов системных событий.

Ограничения работы приложения, связанные со значениями параметра трассировки ptrace

На работу приложения Kaspersky Endpoint Security могут влиять следующие значения параметра операционной системы `kernel.yama.ptrace_scope`:

- 1 (ограниченный ptrace). Процесс может подключаться только к процессам, которые он запустил. Для подключения к другим процессам требуется специальное разрешение. Функциональность приложения ограничена следующим образом:
  - Компонент Анализ поведения не может получать параметры окружения процессов.
  - На операционных системах с версией ядра выше 5.7 компонент Контроль приложений не может читать аргументы командной строки и переменные окружения процессов, так как запрещено чтение /proc/<pid>/syscall, /proc/<pid>/mem. На операционных системах с версией ядра 5.0 компонент Контроль приложений не может нормально работать.
  - Не работает проверка памяти процессов и памяти ядра в задачах проверки, так как запрещено чтение /proc/<pid>/mem.
  - Не гарантируется YARA-проверка памяти процессов, так как запрещено чтение /proc/<pid>/mem.
- 2 (административный ptrace). Только процессы с правами CAP_SYS_PTRACE (обычно root) могут использовать ptrace или получить доступ к процессу в /proc (/proc/<pid>/mem). Есть ограничение в диагностике проблем - не работает создание аварийных файлов дампов пользовательских процессов (таких как kesl-control и kesl-gui), запись дампов самого процесса kesl работает.
- 3 (запрет ptrace): Трассировка ptrace полностью запрещена на уровне операционной системы. Функциональность приложения ограничена следующим образом:
  - Не работает создание аварийных файлов дампов процесса kesl и пользовательских процессов (таких как kesl-control и kesl-gui).
  - Компонент Анализ поведения не может получать параметры окружения процессов.
  - Не поддерживается работа компонента Контроль приложений.
  - Из-за запрета чтения директории /proc/<pid>/mem:
    - Не работает проверка памяти процессов и памяти ядра в задачах проверки.
    - Не работают задачи получения дампа памяти (Get memory dump) и задачи получения дампа памяти процесса (Get process memory dump) при интеграции с решениями Detection and Response.
    - Не гарантируется работа YARA-проверки памяти процессов в режиме мандатного разграничения доступа при интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises).

Ограничения работы обновляемого модуля ядра

Обновляемый модуль ядра не поддерживает следующие виды и версии ядер:

Ubuntu

- `*-kvm`
- `*-gkeop 5.15.0-100[1234] (bionic/jammy)`
- `focal 5.10.0-1002-oem`
- `noble 6.8.0-1014-ibm`
- `*-realtime`
- `*-uc-*`
- `kinetic 5.18.0-100(1|2)-(ibm|gcp|oracle)`

Astra

- `6.1.90-1-generic-*, 6.6.28-1-generic-*`
- `*-hardened`

Debian

- `*-rt`
- `5.14.0-1-(cloud-amd64|amd64)-5.14.6-2`
- `6.1.0-36-(cloud-amd64|amd64)-6.1.139-1`
- `6.5.0-5-*amd64-6.5.13-1`
- `6.6.*`

РЕД ОС 7.3

- `kernel-ml-5.14.9-1.el7`

РЕД ОС 8.0

- `6.6.26-1.red80`
- `6.6.34-1.red80`
- `6.6.51-1.red80`
- `6.6.76-1.red80`
- `6.6.6-1.red80`

Ограничения в использовании технологии eBPF

Для использования технологии eBPF для перехвата сетевого трафика требуется ядро Linux 4.18 и выше, собранное с параметрами:

- `CONFIG_DEBUG_INFO_BTF=y` или `m` (поддержка eBPF с BTF)
- `CONFIG_KPROBES= y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_FSNOTIFY=y`

Для использования технологии eBPF для отправки телеметрии при интеграции с решениями Detection and Response требуется ядро Linux 4.18 и выше, собранное с параметрами:

- `CONFIG_BPF=y`
- `CONFIG_BPF_SYSCALL=y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_KPROBES=y`
- `CONFIG_KPROBES_ON_FTRACE=y`
- `CONFIG_KRETPROBES=y`
- `CONFIG_HAVE_SYSCALL_TRACEPOINTS=y`
- `CONFIG_FTRACE=y`
- `CONFIG_FUNCTION_TRACER=y`
- `CONFIG_DYNAMIC_FTRACE=y`
- `CONFIG_DYNAMIC_FTRACE_WITH_REGS=y`
- `CONFIG_FTRACE_SYSCALLS=y`
- `CONFIG_KPROBE_EVENTS=y`
- `CONFIG_FSNOTIFY=y`

Особенности работы приложения

- Приложение не может одновременно использоваться в режиме Легкого агента и EDR-агента.
- На операционных системах с auditd версии 3.0.7 и ядром Linux версии 4.18 при использовании компонента Анализ поведения возможны зависания приложения и ssh-соединений.
- На операционных системах Kylin Desktop V10 SP1 2303 запущенный компонент Анализ поведения может приводить к зависанию операционной системы. Для решения проблемы рекомендуется обновить системное ядро.

Особенности работы приложения в режиме Легкого агента

Если Kaspersky Endpoint Security используется в режиме Легкого агента:

- Недоступно управление приложением с помощью Kaspersky Security Center Cloud Console и графического пользовательского интерфейса.
- Не поддерживается использование облачных баз.
- Kaspersky Endpoint Security взаимодействует с серверами KSN с помощью прокси-сервера KSN. Взаимодействие с KSN напрямую не поддерживается.
- Не поддерживается использование прокси-сервера приложения при подключении к Серверу интеграции, к SVM и к серверам KSN.

Особенности работы приложения в режиме EDR-агента

Если приложение Kaspersky Endpoint Security используется в режиме EDR-агента, набор доступных компонентов и задач приложения ограничен. После установки параметры приложения настроены следующим образом:

- Не поддерживается интеграция приложения с решением Kaspersky Endpoint Detection and Response Expert (cloud).
- Полностью доступны для управления следующие компоненты, обеспечивающие интеграцию с решениями Detection and Response:
  - EDR Expert (on-premises).
  - NDR (KATA).

  Компоненты выключены по умолчанию, вам нужно их включить для работы приложения в режиме EDR-агента. Вы можете настраивать параметры интеграции, в том числе функциональность запрета запуска объектов.

- Доступ к файлам на время проверки не блокируется: снят флажок **Блокировать доступ к файлам во время проверки** (`FileBlockDuringScan=No`). Этот параметр доступен для изменения, но не будет применен на защищаемом устройстве.

- Компоненты Защита от файловых угроз и Защита от шифрования доступны в режиме ограниченной функциональности: при обнаружении угрозы эти компоненты не пытаются лечить или удалять вредоносные объекты, запрещать доступ или блокировать активность приложений, а только отправляют информацию об обнаружении угрозы на серверы, обеспечивающие интеграцию с решениями Detection and Response.

  Вы можете включать и выключать Защиту от файловых угроз и Защиту от шифрования и настраивать параметры компонентов, кроме действий при обнаружении угрозы. Следующие параметры не будут применены на защищаемом устройстве:

  - Компонент Защита от файловых угроз: **Действие при обнаружении угрозы** – **Пропускать** (`ActionOnThreat=Skip`).

  - Компонент Защита от шифрования: **Действие при обнаружении шифрования** – **Информировать** (`ActionOnDetect=Notify`).

- Полностью доступен для управления компонент Анализ поведения.

- Все остальные компоненты защиты и контроля выключены и недоступны для управления.

При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises) или с Kaspersky Endpoint Detection and Response (KATA) в рамках действия по реагированию на угрозы приложение Kaspersky Endpoint Security может контролировать запуск исполняемых файлов и скриптов на устройстве. Функциональность Запрета запуска объектов доступна со следующими ограничениями:

- Если скрипт запущен из интерпретатора, приложение не контролирует запуск скрипта.

- Приложение не контролирует открытие файлов офисных приложений на устройстве.

Обращение в Службу технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о приложении, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Endpoint Security.

Kaspersky предоставляет поддержку каждой версии приложения Kaspersky Endpoint Security в течение жизненного цикла версии (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Kaspersky CompanyAccount позволяет организациям, использующим приложения "Лаборатории Касперского", взаимодействовать с техподдержкой "Лаборатории Касперского" через электронные запросы. На портале можно создавать новые обращения, следить за их выполнением и хранить историю обработки обращений.

Зарегистрируйте всех сотрудников вашей организации в одной учетной записи Kaspersky CompanyAccount. Это позволит централизованно управлять электронными запросами в Лабораторию Касперского и разграничивать права доступа пользователей Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;

- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки Kaspersky CompanyAccount.

Получение информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас прислать *файл трассировки* или *файл дампа*.

Кроме того, специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на устройстве, подробные отчеты работы компонентов приложения.

Во время работ по диагностике специалисты Службы технической поддержки могут попросить вас изменить параметры приложения:

- активировать функциональность получения расширенной диагностической информации;
- выполнить более тонкую настройку работы отдельных компонентов приложения, недоступную через стандартные средства пользовательского интерфейса;
- изменить параметры хранения полученной диагностической информации;
- настроить перехват и сохранение в файл сетевого трафика.

Вся необходимая для выполнения перечисленных действий информация (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав полученных в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Полученная расширенная диагностическая информация сохраняется на устройстве пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

Перечисленные выше действия требуется выполнять только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы приложения способами, не описанными в документации к приложению или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе приложения и операционной системы, снижению уровня защиты вашего устройства, а также к нарушению доступности и целостности обрабатываемой информации.

Как включить и настроить создание файла трассировки

Файл трассировки приложения Kaspersky Endpoint Security позволяет отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка.

По умолчанию файлы трассировки приложения не создаются. Вы можете включать и выключать создание файлов трассировки приложения и настраивать уровень детализации файлов трассировки в командной строке с помощью общих параметров приложения, а также с помощью графического пользовательского интерфейса.

Если вы управляете приложением Kaspersky Endpoint Security через Kaspersky Security Center, вы можете настраивать параметры трассировки приложения в параметрах политики Kaspersky Endpoint Security с помощью Web Console или Консоли администрирования.

Как настроить параметры трассировки в Web Console

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

2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Общие настройки** → **Служба технической поддержки**, блок **Настройки файла трассировки**.

5. Если вы хотите изменить директорию, в которой будут сохраняться файлы трассировки приложения по умолчанию, укажите директорию для хранения файлов трассировки в поле ввода **Путь к папке трассировки**. Значение по умолчанию: /var/log/kaspersky/kesl. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись только для учетной записи root (права `700` или `rwx--------`).

6. Если требуется, укажите максимальный размер файла трассировки приложения (в мегабайтах) в поле ввода **Максимальный размер файла трассировки (МБ)**. Значение по умолчанию: 500.

7. Если требуется, укажите максимальное количество файлов трассировки приложения в поле ввода **Максимальное количество файлов трассировки**. Значение по умолчанию: 10.

8. Сохраните внесенные изменения.

9. Перезапустите приложение для применения параметров трассировки.

Как настроить параметры трассировки в Консоли администрирования

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.

2. В рабочей области выберите вкладку **Политики**.

3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

   Вы также можете открыть окно свойств политики с помощью пункта **Свойства** контекстного меню политики или по ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.

4. Перейдите в раздел **Общие параметры** → **Параметры приложения**.

5. В блоке **Параметры трассировки и записи дампов** нажмите на кнопку **Настроить**.

6. Откроется окно **Параметры трассировки и записи дампов**.

7. Если вы хотите изменить директорию, в которой будут сохраняться файлы трассировки приложения по умолчанию, укажите директорию для хранения файлов трассировки в поле ввода **Путь к директории с файлами трассировки**. Значение по умолчанию: /var/log/kaspersky/kesl. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись только для учетной записи root (права `700` или `rwx--------`).

8. Если требуется, укажите максимальный размер файла трассировки приложения (в мегабайтах) в поле ввода **Максимальный размер файла трассировки (МБ)**. Значение по умолчанию: 500.

9. Если требуется, укажите максимальное количество файлов трассировки, которые будет создавать приложение, в поле ввода **Максимальное количество файлов трассировки**. Значение по умолчанию: 10.

10. Нажмите на кнопку **OK** в окне **Параметры трассировки и записи дампов**.

11. Нажмите на кнопку **Применить**.

12. Перезапустите приложение для применения параметров трассировки.

Как включить трассировку и настроить параметры трассировки в командной строке

В командной строке вы можете настраивать трассировку приложения с помощью параметров `TraceLevel`, `TraceFolder`, `TraceMaxFileCount` и `TraceMaxFileSize` в общих параметрах приложения. Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Чтобы создать файл трассировки и настроить параметры трассировки в командной строке:

1. Включите создание файла трассировки и выберите уровень детализации файла трассировки:

   ```
   kesl-control --set-app-settings TraceLevel=Detailed | MediumDetailed | NotDetailed
   ```

   Где:

   - `Detailed` – создавать детализированный файл трассировки.
   - `MediumDetailed` – создавать файл трассировки, содержащий информационные сообщения и сообщения об ошибках.
   - `NotDetailed` – создавать файл трассировки, содержащий сообщения об ошибках.

2. Если вы хотите изменить директорию, в которой будут сохраняться файлы трассировки приложения по умолчанию, укажите директорию для хранения файлов трассировки:

   ```
   kesl-control --set-app-settings TraceFolder=<path to trace files directory>
   ```

   Где `<path to trace files directory>` – путь к директории хранения файлов трассировки. Значение по умолчанию: /var/log/kaspersky/kesl. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись только для учетной записи root (права `700` или `rwx--------`).

3. Если требуется, укажите максимальное количество файлов трассировки приложения:

```
kesl-control --set-app-settings TraceMaxFileCount=<number of application trace files>
```

   Где `<number of application trace files>` – максимальное количество файлов трассировки приложения. Доступные значения от 1 до 10000. Значение по умолчанию: 10.

4. Если требуется, укажите максимальный размер файла трассировки приложения (в мегабайтах):

```
kesl-control --set-app-settings TraceMaxFileSize=<size of an application trace file>
```

   Где `<size of an application trace file>` – максимальный размер файла трассировки приложения (в мегабайтах). Доступные значения от 1 до 1000. Значение по умолчанию: 500.

После изменения значений параметров `TraceFolder`, `TraceMaxFileCount`, `TraceMaxFileSize` требуется перезапустить приложение.

```
Выключить создание файла трассировки, выполните команду:

kesl-control --set-app-settings TraceLevel=None
```

Как включить трассировку и настроить параметры трассировки в графическом интерфейсе

Для создания и настройки уровня детализации файла трассировки требуются права пользователя с ролью Администратор (admin).

1. Откройте главное окно графического интерфейса приложения.

2. В нижней части главного окна приложения нажмите на кнопку **Поддержка**.

   Откроется окно **Поддержка**.

3. По ссылке **Трассировка** откройте окно **Трассировка**.

4. В раскрывающемся списке **Уровень** выберите уровень детализации файла трассировки:

   - **Диагностический (300)** – только сообщения об ошибках.
   - **Информационный (700)** – информационные сообщения и сообщения об ошибках.
   - **Отладочный (800)** – детализированный файл трассировки.

   Рекомендуем уточнить требуемый уровень детализации у специалистов Службы технической поддержки "Лаборатории Касперского". По умолчанию выбрано **Диагностический (300)**.

5. Нажмите на кнопку **Включить**, чтобы запустить процесс трассировки.

6. Воспроизведите ситуацию, при которой у вас возникает проблема.

7. Нажмите на кнопку **Выключить**, чтобы остановить процесс трассировки.

Созданные файлы трассировки хранятся в директории /var/log/kaspersky/kesl/.

Также вы можете включить и настроить создание файлов трассировки Watchdog-сервера.

Как включить трассировку и настроить параметры трассировки Watchdog-сервера в командной строке

В командной строке вы можете настраивать трассировку Watchdog-сервера с помощью параметра `WdTraceLevel` в общих параметрах приложения. Вы можете изменять значения параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Создать файл трассировки Watchdog-сервера и настроить параметры трассировки в командной строке

```
kesl-control --set-app-settings WdTraceLevel=Detailed | MediumDetailed | NotDetailed | Product
```

Где:

- `Detailed` – создавать детализированный файл трассировки.
- `MediumDetailed` – создавать файл трассировки, содержащий информационные сообщения и сообщения об ошибках.
- `NotDetailed` – создавать файл трассировки, содержащий сообщения об ошибках.
- `Product` – установить значение, равное значению параметра `TraceLevel` в общих параметрах приложения. Если значение параметра `TraceLevel=None`, файл трассировки не создается.

Выключить создание файла трассировки Watchdog-сервера и настроить параметры трассировки в командной строке

```
kesl-control --set-app-settings WdTraceLevel=None
```

По умолчанию созданные файлы трассировки хранятся в директории /var/log/kaspersky/kesl/. Для доступа к этой директории требуются root-права. Вы можете указать другую директорию для хранения файлов трассировки. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись только для учетной записи root (права `700` или `rwx-------`).

Файлы трассировки графического интерфейса и утилиты командной строки kesl-control хранятся в директории /var/log/kaspersky/kesl-user. Для включения создания этих файлов трассировки требуется задать переменную окружения LFS_ENABLE_ALL_COMPONENTS_LOGGING.

Для хранения файлов трассировки приложения требуется дополнительное к указанному в минимальных аппаратных требованиях место на диске.

Файлы трассировки хранятся на устройстве в течение всего времени использования приложения и удаляются без возможности восстановления при удалении приложения. Автоматическая отправка файлов трассировки в "Лабораторию Касперского" не выполняется.

Файлы трассировки хранятся в доступном для чтения виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

Файлы трассировки MMC-плагина управления

Если для управления приложением Kaspersky Endpoint Security вы используете Консоль администрирования, информация о событиях, возникающих во время работы MMC-плагина управления, может записываться в файл трассировки MMC-плагина Kaspersky Endpoint Security на устройстве, где установлен Сервер администрирования. Имя файла содержит номер версии приложения, дату и время создания файла и идентификатор процесса (PID). В этот файл записывается информация о событиях, возникающих во время работы MMC-плагина, в частности, о работе политик и задач.

По умолчанию файлы трассировки MMC-плагина не создаются. Вы можете создать файл трассировки MMC-плагина с помощью ключей реестра. За подробной информацией о том, как создать файлы трассировки, вы можете обратиться к специалистам Службы технической поддержки.

Все созданные файлы трассировки MMC-плагина расположены в папке, указанной пользователем во время настройки ключей реестра.

Файлы трассировки веб-плагина управления

Если для управления приложением Kaspersky Endpoint Security вы используете Web Console, информация о событиях, возникающих во время работы веб-плагина управления, может записываться в файлы трассировки веб-плагина.

Файлы трассировки веб-плагина создаются автоматически, если в мастере установки Web Console включена запись в журнал активности Web Console (см. подробнее в справке Kaspersky Security Center).

Файлы трассировки веб-плагина сохраняются в папке установки Web Console во вложенной папке logs.

Содержимое файлов трассировки приложения

В файлах трассировки содержатся следующие общие данные:

- время возникновения события;
- номер потока исполнения;
- компонент приложения, инициировавший событие;
- уровень важности события (информационное событие, предупреждение, критическое событие, ошибка);
- описание события, связанного с выполнением команды компонентом приложения, и результат выполнения этой команды.

В файлах трассировки могут храниться следующие данные в дополнение к общим данным:

- статусы компонентов приложения и их рабочие данные;
- данные о действиях пользователей в приложении;
- данные об оборудовании, установленном на устройстве;
- данные обо всех объектах и событиях операционной системы, а также данные о действиях пользователей;
- данные, содержащиеся в объектах операционной системы (например, содержимое файлов, в которых могут находиться персональные данные пользователей);
- данные о сетевом трафике (например, содержимое полей ввода на веб-сайте, которые могут включать данные банковской карты или любые другие конфиденциальные данные);
- данные, полученные с серверов "Лаборатории Касперского" (например, версия баз приложения);

- данные, полученные с серверов KATA, серверов OSMP, серверов NDR и серверов, обеспечивающих взаимодействие с Sandbox;
- данные о потребленных ресурсах центрального процессора;
- данные о потребленных ресурсах оперативной памяти;
- данные об операциях чтения и записи файлов приложениями;
- данные о количестве кешированной информации, необходимой для работы приложения.

Содержимое файлов трассировки плагинов управления

В файлах трассировки плагинов управления содержатся следующие общие данные:

- время возникновения события;
- номер потока исполнения;
- компонент приложения, инициировавший событие;
- уровень важности события (информационное событие, предупреждение, критическое событие, ошибка);
- описание события, связанного с выполнением команды компонентом приложения, и результат выполнения этой команды.

Помимо общих данных файлы трассировки плагинов управления могут содержать следующую информацию:

- персональные данные, в том числе фамилию, имя и отчество, если эти данные являются частью пути к файлам;
- имя учетной записи для входа в операционную систему, если имя учетной записи является частью имени файла.

Как включить и настроить запись дампов

Файл дампа содержит всю информацию о рабочей памяти процессов приложения Kaspersky Endpoint Security на момент создания файла дампа.

Файлы дампов могут содержать персональные данные. Рекомендуется обеспечить защиту информации от несанкционированного доступа до ее передачи в "Лабораторию Касперского".

По умолчанию файлы дампов не создаются. Вы можете включать и выключать запись дампов при сбое в работе приложения.

Если вы управляете приложением Kaspersky Endpoint Security через Kaspersky Security Center, вы можете включать и выключать запись дампов и настраивать параметры записи дампов в параметрах политики Kaspersky Endpoint Security с помощью Web Console или Консоли администрирования.

Если вы управляете приложением через командную строку, вы можете включать и выключать запись дампов с помощью общих параметров приложения.

Максимальное количество файлов дампов ограничено.

> При некоторых параметрах операционной системы пользовательские файлы дампа могут не создаваться. Убедитесь, что значение параметра `sysctl kernel.yama.ptrace_scope=0`.

Как включить запись дампов и настроить параметры записи дампов в Web Console

Чтобы включить и настроить параметры записи дампов в Web Console:

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

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Общие настройки** → **Служба технической поддержки**, блок **Отладочная информация**.
5. Если вы хотите, чтобы при сбое в работе приложения создавался файл дампа, включите переключатель **Запись дампов ВКЛЮЧЕНА**.
6. Если вы хотите изменить директорию, в которой будут сохраняться файлы дампов процесса kesl по умолчанию, укажите директорию для хранения файлов дампов в поле ввода **Путь к файлу дампа**. Значение по умолчанию: /var/opt/kaspersky/kesl/common/dumps. Для доступа к директории хранения файлов дампов, заданной по умолчанию, требуются root-права. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись только для учетной записи root (права `700` или `rwx-------`).
7. Сохраните внесенные изменения.

Как включить запись дампов и настроить параметры записи дампов в Консоли администрирования

Чтобы включить и настроить параметры записи дампов в Консоли администрирования:

1. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входят нужные устройства.
2. В рабочей области выберите вкладку **Политики**.
3. В списке политик выберите нужную политику и откройте окно **Свойства: <Название политики>** двойным щелчком мыши.

   Вы также можете открыть окно свойств политики с помощью пункта **Свойства** контекстного меню политики или по ссылке **Настроить параметры политики**, расположенной справа от списка политик в блоке с параметрами политики.
4. Перейдите в раздел **Общие параметры** → **Параметры приложения**.
5. В блоке **Параметры трассировки и записи дампов** нажмите на кнопку **Настроить**.
6. Откроется окно **Параметры трассировки и записи дампов**.
7. Если вы хотите, чтобы при сбое в работе приложения создавался файл дампа, установите флажок **Создавать файл дампа при сбое в работе приложения**.

8. Если вы хотите изменить директорию, в которой будут сохраняться файлы дампов процесса kesl по умолчанию, укажите директорию для хранения файлов дампов в поле ввода **Путь к директории с файлами дампа**. Значение по умолчанию: /var/opt/kaspersky/kesl/common/dumps. Для доступа к директории хранения файлов дампов, заданной по умолчанию, требуются root-права (права `700` или `rwx-------`). Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись только для учетной записи root.

9. Нажмите на кнопку **OK** в окне **Параметры трассировки и записи дампов**.

10. Нажмите на кнопку **Применить**.

Как включить запись дампов и настроить параметры записи дампов в командной строке

В командной строке вы можете включать, выключать и настраивать параметры записи дампов с помощью параметров `CoreDumps` и `CoreDumpsPath` из общих параметров приложения.

Чтобы включить и настроить запись дампов:

1. Выполните команду, чтобы включить запись дампов:

```
kesl --set-app-settings CoreDumps=Yes
```

2. Если вы хотите изменить директорию, в которой сохраняются файлы дампа по умолчанию, укажите путь к директории для хранения файлов дампов в качестве значения параметра `CoreDumpsPath`.

```
kesl --set-app-settings CoreDumpsPath=<path to directory with dump files>
```

   Где: `<path to directory with dump files>` – путь к директории, в которой хранятся файлы дампов. Значение по умолчанию: /var/opt/kaspersky/kesl/common/dumps. Для доступа к директории хранения файлов дампов, заданной по умолчанию, требуются root-права (права `700` или `rwx-------`). Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись только для учетной записи root.

Чтобы выключить запись дампов, выполните следующую команду:

```
kesl --set-app-settings CoreDumps=No
```

Если вы включили запись дампов, по умолчанию файлы дампов хранятся в следующих директориях:

- /var/opt/kaspersky/kesl/common/dumps (файлы дампов процесса kesl);
- /var/opt/kaspersky/kesl/common/dumps-user (файлы дампов пользовательских процессов).

Для доступа к директории хранения файлов дампов, заданной по умолчанию, требуются root-права. Вы можете указать другую директорию для хранения файлов дампов процесса kesl. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись только для учетной записи root (права `700` или `rwx-------`).

Для хранения файлов дампов требуется дополнительное к указанному в минимальных аппаратных требованиях место на диске.

Файлы дампов хранятся на устройстве в течение всего времени использования приложения и удаляются без возможности восстановления при удалении приложения. Автоматическая отправка файлов дампов в "Лабораторию Касперского" не выполняется.

Удаленная диагностика устройства с помощью Kaspersky Security Center

В Kaspersky Security Center вы можете выполнять удаленную диагностику клиентских устройств. Процедура удаленной диагностики позволяет удаленно выполнять следующие операции:

- включать и выключать трассировку;
- изменять уровень трассировки;
- загружать файлы трассировки;
- загружать журнал удаленной установки приложения;
- загружать системные журналы событий (syslog);
- запускать, останавливать и перезапускать приложения.

Удаленная диагностика с помощью Web Console

Если вы управляете приложением Kaspersky Endpoint Security через Web Console, удаленная диагностика клиентского устройства выполняется в окне удаленной диагностики.

Чтобы открыть окно удаленной диагностики устройства:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.

   Откроется список управляемых устройств.

2. Выберите устройство, для которого вы хотите выполнить удаленную диагностику, и нажмите на ссылку <имя устройства>.

   Откроется окно свойств устройства.

3. На вкладке **Дополнительно** выберите раздел **Удаленная диагностика**.

В окне удаленной диагностики устройства вы можете посмотреть журнал удаленной установки приложения.

Чтобы просмотреть журнал удаленной установки приложения на устройстве:

1. Откройте окно удаленной диагностики устройства.

2. На вкладке **Журналы событий** в блоке **Файлы трассировки** нажмите на ссылку **Журналы удаленной установки**.

   Откроется окно **Журналы событий трассировки устройства**.

Подробнее об удаленной диагностике см. в справке Kaspersky Security Center.

Удаленная диагностика с помощью Консоли администрирования

Если вы управляете приложением Kaspersky Endpoint Security через Консоль администрирования, удаленная диагностика выполняется с помощью специальной утилиты удаленной диагностики Kaspersky Security Center, которая автоматически устанавливается на устройство совместно с Консолью администрирования.

Чтобы открыть главное окно утилиты удаленной диагностики устройства:

1. В дереве Консоли администрирования в папке **Управляемые устройства** выберите группу администрирования, в состав которой входит нужное вам устройство.

2. В рабочей области выберите вкладку **Устройства**.

3. В списке управляемых устройств выберите устройство, к которому вы хотите подключить утилиту удаленной диагностики, и в контекстном меню устройства выберите пункт **Внешние инструменты** → **Удаленная диагностика**.

   Откроется главное окно утилиты удаленной диагностики **Утилита удаленной диагностики Kaspersky Security Center**.

С помощью утилиты удаленной диагностики устройства вы можете посмотреть журнал удаленной установки приложения.

Чтобы просмотреть журнал удаленной установки приложения на устройстве:

1. Откройте главное окно утилиты удаленной диагностики устройства.

2. Если требуется, настройте параметры подключения утилиты к устройству. В главном окне утилиты удаленной диагностики нажмите на кнопку **Войти**.

3. В открывшемся окне в дереве объектов выберите папку **Журналы удаленной установки**.

Подробнее об утилите удаленной диагностики см. в справке Kaspersky Security Center.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст справки.

Приложение 1. Конфигурационные файлы и параметры приложения по умолчанию

Для управления работой приложения Kaspersky Endpoint Security используются следующие конфигурационные файлы:

- Конфигурационные файлы, которые содержат параметры первоначальной настройки приложения.
- Предустановленные конфигурационные файлы, которые создаются автоматически во время первоначальной настройки приложения и содержат значения параметров, заданные при первоначальной настройке. Эти параметры применяются во время работы приложения.
- Конфигурационные файлы, которые вы можете создавать с помощью команд управления приложением Kaspersky Endpoint Security. Эти конфигурационные файлы могут содержать параметры задач и другие параметры приложения. Вы можете изменять эти файлы и импортировать их в приложение, чтобы изменять соответствующие параметры.

Правила редактирования конфигурационных файлов задач приложения

При редактировании конфигурационного файла соблюдайте следующие правила:

- В конфигурационном файле укажите все обязательные параметры. Отдельные параметры задачи можно указать без файла, с помощью командной строки.
- Если параметр принадлежит к какой-либо секции, укажите его только в этой секции. В пределах одной секции вы можете указывать параметры в любом порядке.
- Заключайте имена секций в квадратные скобки [ ].
- Вводите значения параметров в формате `< имя параметра >=< значение параметра >` без пробелов между именем параметра и его значением.

  Пример:
  ```
  [ScanScope.item_0000]
  AreaDesc=Home
  AreaMask.item_0000=*doc
  Path=/home
  ```

  Символы "пробел" и "табуляция" игнорируются перед первой кавычкой и после последней кавычки строкового значения, а также в начале и в конце строкового значения, не заключенного в кавычки.
- Если вам нужно указать несколько значений параметра, повторите параметр столько раз, сколько значений вы хотите указать.

```
Пример:
AreaMask.item_0000=*xml
AreaMask.item_0001=*doc
```

- Соблюдайте регистр при вводе значений параметров следующих типов:
  - имена (маски) проверяемых объектов и объектов исключения;
  - названия (маски) угроз.

  При вводе остальных значений параметров соблюдать регистр не требуется.

- Указывайте значения параметров булевского типа следующим образом: `Yes` / `No`.

- Заключайте в кавычки строковые значения, содержащие символ "пробел" (например, имена файлов и директорий, пути к ним; выражения, содержащие дату и время в формате "ГГГГ-ММ-ДД ЧЧ:ММ:СС").

  Остальные значения вы можете вводить как в кавычках, так и без них.

  ```
  Пример:
  AreaDesc=" Проверка почтовых баз "
  ```

  Одиночная кавычка в начале или в конце строки считается ошибкой.

Конфигурационные файлы первоначальной настройки

Вы можете задавать параметры первоначальной настройки приложения с помощью конфигурационного файла:

- Если вы устанавливаете приложение с помощью Kaspersky Security Center, в составе архива для удаленной установки приложения вы получаете конфигурационный файл autoinstall.ini. Вы можете настроить параметры в этом файле перед созданием инсталляционного пакета. Kaspersky Security Center применит эти параметры во время установки приложения.

- Если вы устанавливаете приложение с помощью командной строки, вам нужно создать конфигурационный файл и указать путь к нему при запуске мастера первоначальной настройки приложения. Вы можете скопировать структуру для этого файла из конфигурационного файла autoinstall.ini.

В конфигурационном файле первоначальной настройки вы можете задавать параметры, приведенные в таблице ниже. Набор применимых параметров зависит от режима использования приложения. Значения по умолчанию указаны для файла autoinstall.ini.

Допустимые значения некоторых параметров отличаются при удаленной установке через Kaspersky Security Center и при установке через командную строку.

Для изменения параметра в конфигурационном файле укажите его значение в формате <имя параметра>=<значение>.

```
Пример

UPDATER_SOURCE=KLServers
```

Параметр	Описание	Значения

Секция **[CustomSettings]**	Тонкая настройка приложения при удаленной установке. Позволяет изменять некоторые параметры файла kesl.ini, а также уровень детализации файлов трассировки.
	
	Настройка приложения с помощью секции возможна только при первоначальной установке.
	
	Если секция `[CustomSettings]` дублирует параметры файла autoinstall.ini, то к приложению применятся значения файла autoinstall.ini.
		• Любой параметр конфигурационного файла kesl.ini в формате <секция параметров>.<имя параметра>=<значение>
		Пример
		`[CustomSettings]`
		`General.Locale=ru_RU.utf8`
		`Network.ProxyRouteTable=202`
		`Watchdog.MaxMemory=20MB`
		• `TraceLevel` – уровень детализации файлов трассировки приложения:
		  • `Detailed` – создавать детализированный файл трассировки приложения.
		  • `MediumDetailed` – создавать файл трассировки приложения, содержащий информационные сообщения и сообщения об ошибках.
		  • `NotDetailed` – создавать файл трассировки приложения, содержащий сообщения об ошибках.
		  • `None` (значение по умолчанию) – не создавать файл трассировки приложения.
		• `WdTraceLevel` – уровень детализации файлов трассировки Watchdog-сервера:
		  • `Detailed` – создавать детализированный файл трассировки Watchdog-сервера.
		  • `MediumDetailed` – создавать файл трассировки Watchdog-сервера, содержащий информационные сообщения и сообщения об ошибках.
		  • `NotDetailed` – создавать файл трассировки Watchdog-сервера, содержащий сообщения об ошибках.
		  • `None` – не создавать файл трассировки Watchdog-сервера.
		  • `Product` (значение по умолчанию) – установить значение, равное значению параметра `TraceLevel`.

EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения.	`Yes` (значение по умолчанию) – принять условия Лицензионного соглашения. `No` – не принимать условия Лицензионного соглашения. Установка приложения будет прервана.

Параметр	Описание	Значения
PRIVACY_POLICY_AGREED	Обязательный параметр. Согласие с условиями Политики конфиденциальности.	`Yes` (значение по умолчанию) – принять условия Политики конфиденциальности. `No` – не принимать условия Политики конфиденциальности. Установка приложения будет прервана.
USE_KSN	Обязательный параметр. Включение использования Kaspersky Security Network. Для включения использования KSN требуется принять условия Положения о Kaspersky Security Network. Если приложение Kaspersky Endpoint Security используется в стандартном режиме и вы включили использование KSN, автоматически включается облачный режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО.	`Yes` – принять условия Положения о Kaspersky Security Network и включить использование KSN. `No` (значение по умолчанию) – не принимать условия Положения о Kaspersky Security Network. Отказ от использования KSN не прерывает процесс установки приложения.
LOCALE	Языковой стандарт, используемый для локализации событий приложения, отправляемых в Kaspersky Security Center. Для отображения графического интерфейса и командной строки приложения используется локализация, указанная в переменной окружения `LANG`. Если приложение не поддерживает указанную локализацию, то используется английская локализация.	Языковой стандарт в формате, определенном в стандарте RFC 3066. Возможные значения: • `de_DE.UTF-8` – немецкий; • `en_US.UTF-8` – английский (США); • `es_MX.UTF-8` – испанский (Мексика); • `fr_FR.UTF-8` – французский; • `ja_JP.UTF-8` – японский; • `pt_BR.UTF-8` – португальский (Бразилия); • `ru_RU.UTF-8` – русский; • `zh_TW.UTF-8` – китайский традиционный; • `zh_CN.UTF-8` – китайский упрощенный. Если параметр `LOCALE` не указан, используется язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация не поддерживается, для локализации событий используется английский язык (en_US.UTF-8 в формате стандарта RFC 3066).

Параметр	Описание	Значения
INSTALL_LICENSE	В конфигурационном файле autoinstall.ini: код активации для добавления лицензионного ключа в приложение. В конфигурационном файле, который используется при установке через командную строку, вы также можете указать путь к файлу ключа для добавления лицензионного ключа в приложение. Параметр применяется, только если приложение используется в стандартном режиме.	`<activation code>` – если требуется активировать приложение с использованием кода активации во время установки через Kaspersky Security Center или через командную строку. `<full path to key file>` – если требуется активировать приложение с использованием файла ключа во время установки через командную строку. `None` – если активировать приложение во время установки не требуется, например, если приложение установлено в закрытом сегменте сети без доступа в интернет.
UPDATER_SOURCE	Источник обновлений баз и модулей приложения. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-агента.	`SCServer` – использовать в качестве источника обновлений Сервер администрирования Kaspersky Security Center. `KLServers` (значение по умолчанию) – использовать в качестве источника обновлений серверы "Лаборатории Касперского". `<update source address>` в виде локальной директории (например /home/bases/) или удаленного HTTP- или HTTPS-сервера (например http://example.com/bases/).
PROXY_SERVER	Адрес прокси-сервера, используемого для подключения к интернету. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-агента.	Адрес прокси-сервера в одном из следующих форматов: • `[<connection protocol>://] <address of the proxy server>:<port>`, если для подключения к прокси-серверу не требуется аутентификация; • `[<connection protocol>://] [<user name>: [<password>]@]<address of the proxy server>:<port>`, если для подключения к прокси-серверу требуется аутентификация. Если вы указываете IP-адрес в формате IPv6, то вводите адрес в квадратных скобках. Подключение к прокси-серверу по протоколу HTTPS не поддерживается.
UPDATE_EXECUTE	Запуск задачи обновления баз приложения во время первоначальной настройки. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-агента.	`Yes` (значение по умолчанию) – запускать задачу обновления. `No` – не запускать задачу обновления.

Параметр	Описание	Значения
KERNEL_SRCS_INSTALL	Автоматический запуск компиляции модуля ядра при запуске защиты от файловых угроз. Параметр применяется только на операционных системах, не поддерживающих технологию fanotify.	`Yes` (значение по умолчанию) – компилировать модуль ядра при запуске защиты от файловых угроз. `No` – не компилировать модуль ядра.
USE_GUI	Установка и использование графического интерфейса приложения. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-Агента.	`Yes` – установить и использовать графический интерфейс приложения (файлы для установки графического интерфейса должны быть добавлены в инсталляционный пакет). `No` (значение по умолчанию) – не использовать графический интерфейс.
GROUP_CLEAN	Обязательный параметр. Автоматическое удаление пользователей из привилегированных групп kesladmin и keslaudit перед установкой приложения.	`Yes` – удалять пользователей из привилегированных групп. Если указано значение `Yes` и группа nogroup отсутствует, то установка будет прервана и вам будет предложено удалить пользователей из привилегированных групп вручную. `No` (значение по умолчанию) – не удалять пользователей из привилегированных групп.
ADMIN_USER	Пользователь, которому назначается роль администратора (admin). Роль администратора позволяет управлять параметрами приложения и параметрами задач через графический интерфейс и командную строку приложения без использования команды `sudo`.	
CONFIGURE_SELINUX	Автоматическая настройка SELinux для работы с приложением Kaspersky Endpoint Security.	`Yes` (значение по умолчанию) – выполнить автоматическую настройку SELinux для работы с Kaspersky Endpoint Security. `No` – не выполнять автоматическую настройку SELinux.

Параметр	Описание	Значения
DISABLE_PROTECTION	Выключение функциональных компонентов приложения после его установки. Установка с выключенными компонентами может быть удобна, например, для воспроизведения проблемы в работе приложения с целью создания файла трассировки. Если после установки приложения с параметром `DISABLE_PROTECTION=Yes` вы включите нужные компоненты, то после перезапуска приложения включенные компоненты продолжат работу.	`Yes` – выключить компоненты защиты и задачи проверки при запуске приложения после установки. `No` – не выключать компоненты защиты и задачи проверки при запуске приложения после установки.
ENDPOINT_AGENT_MODE	Использование Kaspersky Endpoint Security в режиме EDR-агента. Параметр неприменим для устройств с процессором Эльбрус.	`Yes` – Kaspersky Endpoint Security используется в режиме EDR-агента для обеспечения совместной работы на защищаемых устройствах решений Detection and Response от "Лаборатории Касперского" и антивирусных решений от сторонних поставщиков. `No` (значение по умолчанию) – Kaspersky Endpoint Security используется в стандартном режиме или в режиме Легкого агента (см. параметр KSVLA_MODE).
EDR_EXPERT_CLOUD_MODE	Выбор режима компонента Endpoint Detection and Response Expert. Параметр применяется, только если приложение используется в стандартном режиме. Параметр неприменим для устройств с процессором Эльбрус.	`Yes` – приложение использует интеграцию с Kaspersky Endpoint Detection and Response Expert (cloud). `No` (значение по умолчанию) – приложение использует интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises).
KSVLA_MODE	Использование Kaspersky Endpoint Security в режиме Легкого агента. Параметр неприменим для устройств с процессором Эльбрус.	`Yes` – Kaspersky Endpoint Security используется в режиме Легкого агента (в составе решения Kaspersky Security для виртуальных сред Легкий агент). `No` (значение по умолчанию) – Kaspersky Endpoint Security используется в стандартном режиме или в режиме EDR-агента (см. параметр ENDPOINT_AGENT_MODE).

Параметр	Описание	Значения
SERVER_MODE	Роль защищаемой виртуальной машины (сервер или рабочая станция). Параметр применяется, только если приложение используется в режиме Легкого агента. Параметр неприменим для устройств с процессором Эльбрус.	`Yes` – защищаемая виртуальная машина используется как сервер. `No` – защищаемая виртуальная машина используется как рабочая станция.
VDI_MODE	Включение режима защиты инфраструктуры VDI для оптимизации работы приложения на временных виртуальных машинах. Параметр применяется, только если приложение используется в режиме Легкого агента. Параметр неприменим для устройств с процессором Эльбрус.	`Yes` – включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки Kaspersky Endpoint Security на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. `No` – не включать режим защиты инфраструктуры VDI.
INTERCEPTOR_MODE	Механизм перехвата системных событий, который приложение Kaspersky Endpoint Security использует в своей работе. Параметр применяется только на устройствах, где операционная система поддерживает технологию fanotify. Параметр неприменим для устройств с процессором Эльбрус.	`UseFanotify` (значение по умолчанию) – использовать технологию fanotify для перехвата системных событий. `UseUpdatableKernelModule` – использовать обновляемый модуль ядра для перехвата системных событий.

Параметр	Описание	Значения
INTERCEPTOR_FALLBACK_STRATEGY	Действие, которое приложение выполняет, если обновляемый модуль ядра не запускается. Параметр применяется только на устройствах, где операционная система поддерживает технологию fanotify. Параметр неприменим для устройств с процессором Эльбрус.	`FallbackToFanotify` (значение по умолчанию) – перейти к использованию технологии fanotify для перехвата системных событий. `FallbackToLimitedMode` – не использовать перехват системных событий. В результате проверка файлов в режиме реального времени не выполняется, уровень защиты устройства снижается.
INTERCEPTOR_APPLY_STRATEGY	Если приложение переходит к использованию обновляемого модуля ядра, для запуска модуля требуется перезапуск приложения. Параметр позволяет указать, будет ли перезапуск приложения выполняться автоматически или требуется перезапуск приложения вручную. Параметр применяется только при установке через Kaspersky Security Center. Параметр применяется только на устройствах, где операционная система поддерживает технологию fanotify. Параметр неприменим для устройств с процессором Эльбрус.	`RestartServiceAutomatically` (значение по умолчанию) – автоматически перезапускать приложение для запуска обновляемого модуля ядра. `RestartServiceManually` – запускать обновляемый модуль ядра после перезапуска приложения, выполненного пользователем вручную. Рекомендуется выполнять автоматический перезапуск приложения для перехода к использованию обновляемого модуля ядра. Запуск обновляемого модуля ядра после перезапуска приложения вручную может приводить к ошибкам в работе приложения.
ENABLE_TRACES_ON_FIRST_STARTUP	Создание файла трассировки приложения при первом запуске после установки. Для записи трассировки автоматически создается файл kesl_startup.log в директории /var/log/kaspersky/kesl/. К этому файлу не применяется ограничение на размер, заданное для обычных файлов трассировки приложения. Запись трассировки останавливается после запуска задачи Защита от файловых угроз или через пять минут после начала записи трассировки.	`Yes` – создавать файл трассировки при первом запуске приложения после установки. `No` (значение по умолчанию) – не создавать файл трассировки при первом запуске приложения.

Параметр	Описание	Значения
AK_FORCED_PACKAGE_MANAGER_OPERATIONS_AS_FALLBACK	Установка приложения в режиме игнорирования ошибок менеджера пакетов. Этот режим используется, если не удается установить приложение в штатном режиме. Параметр применяется только при установке через Kaspersky Security Center. Рекомендуется изменять значение этого параметра только под руководством специалистов Службы технической поддержки по полученным от них инструкциям.	`No` (значение по умолчанию) – устанавливать приложение в штатном режиме. `Yes` – устанавливать приложение, игнорируя системные ошибки.
AK_REMOVE_PARTIALLY_INSTALLED_PACKAGE	Автоматическое удаление инсталяционного пакета приложения, если он был установлен лишь частично. Отключите этот параметр, если не удается установить приложение в штатном режиме. Параметр применяется только при установке через Kaspersky Security Center. Рекомендуется изменять значение этого параметра только под руководством специалистов Службы технической поддержки по полученным от них инструкциям.	`Yes` (значение по умолчанию)– удалять частично установленный инсталляционный пакет приложения. `No` – устанавливать приложение, игнорируя частично установленный пакет.

Параметр	Описание	Значения
AK_PACKAGE_MANAGER_DEBUG_LOG_OUTPUT	Включение записи отладочных журналов для менеджеров пакетов. Этот параметр используется, если не удается установить приложение в штатном режиме. Параметр применяется только при установке через Kaspersky Security Center. Рекомендуется изменять значение этого параметра только под руководством специалистов Службы технической поддержки по полученным от них инструкциям.	`Yes` – включать запись отладочных журналов для менеджеров пакетов. `No` (значение по умолчанию) – не включать запись отладочных журналов для менеджеров пакетов.

Параметры первоначальной настройки в инсталляционном пакете

Вы можете задавать параметры первоначальной настройки приложения в инсталляционном пакете, который используется при установке приложения с помощью Kaspersky Security Center.

В Kaspersky Security Center Web Console вы можете указать параметры первоначальной настройки приложения Kaspersky Endpoint Security в свойствах инсталляционного пакета на вкладке **Параметры**. Созданные инсталляционные пакеты доступны в главном окне Web Console в одном из следующих разделов:

- **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
- **Операции** → **Хранилища** → **Инсталляционные пакеты**.

В Консоли администрирования Kaspersky Security Center вы можете указать параметры первоначальной настройки приложения Kaspersky Endpoint Security при создании инсталляционного пакета или в свойствах инсталляционного пакета в разделе **Параметры**. Созданные инсталляционные пакеты доступны в дереве Консоли администрирования в папке **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

Набор применимых параметров зависит от режима использования приложения.

Параметры первоначальной настройки в Web Console

Параметр	Описание
Режим использования приложения	• **Стандартный режим для защиты рабочих станций и серверов** (значение по умолчанию). Если выбран этот вариант, приложение используется как автономное приложение для защиты рабочих станций и серверов под управлением операционных систем Linux. • **Агент Endpoint Detection and Response**. Если выбран этот вариант, приложение используется для совместной работы решений Detection and Response от "Лаборатории Касперского" и антивирусных решений сторонних поставщиков на защищаемых устройствах. • **Легкий агент для защиты виртуальных сред**. Если выбран этот вариант, приложение используется в режиме Легкого агента (в составе решения Kaspersky Security для виртуальных сред Легкий агент). Режим EDR-агента и режим Легкого агента недоступны для устройств с процессором Эльбрус.
Включить Endpoint Detection and Response Expert (cloud)	Установите флажок, чтобы использовать интеграцию с Endpoint Detection and Response Expert (cloud). В стандартном режиме приложение поддерживает интеграцию с Endpoint Detection and Response Expert (cloud) и Endpoint Detection and Response Expert (on-premises). Если флажок снят, используется интеграция с Endpoint Detection and Response Expert (on-premises). Параметр применяется, только если приложение используется в стандартном режиме Параметр неприменим для устройств с процессором Эльбрус.
Включить режим защиты инфраструктуры VDI	Установите флажок, чтобы включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки приложения на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. По умолчанию флажок снят. Параметр применяется, только если приложение используется в режиме Легкого агента. Параметр неприменим для устройств с процессором Эльбрус.
Защищаемая виртуальная машина используется как сервер	Роль виртуальной машины, на которую будет установлено приложение: сервер или рабочая станция. По умолчанию флажок установлен (виртуальная машина используется в виртуальной инфраструктуре как сервер). Параметр применяется, только если приложение используется в режиме Легкого агента. Параметр неприменим для устройств с процессором Эльбрус.
Язык событий в KSC	Язык, который должен использоваться для локализации событий приложения, отправляемых в Kaspersky Security Center: • **Системный** (значение по умолчанию) – язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация не поддерживается, для локализации событий используется английский язык. • Один из национальных языков, поддерживаемых приложением Kaspersky Endpoint Security: английский (США), испанский (Мексика), китайский традиционный, китайский упрощенный, немецкий, португальский (Бразилия), русский, французский, японский. Для отображения графического интерфейса и командной строки приложения используется локализация, указанная в переменной окружения `LANG`. Если приложение не поддерживает указанную локализацию, то используется английская локализация.

Параметр	Описание
Активировать приложение	Установите флажок, если вы хотите активировать приложение во время установки. В открывшемся поле введите код активации. По умолчанию флажок снят. Параметр применяется, только если приложение используется в стандартном режиме.
Источники обновлений	Источник обновлений баз и модулей приложения: • **Серверы обновлений "Лаборатории Касперского"** (значение по умолчанию). • **Kaspersky Security Center**. • **Другие источники в локальной или глобальной сети**. Если вы выбрали этот вариант, в открывшемся поле введите адрес источника обновлений. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-агента.
Запустить задачу обновления баз после установки	Если флажок установлен, после установки приложения запускается задача обновления баз и модулей приложения. По умолчанию флажок установлен. Снимите этот флажок, если вы добавили в инсталляционный пакет предварительно скачанные базы приложения. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-агента.
Указать параметры прокси-сервера	Установите флажок, если вы используете прокси-сервер для доступа в интернет. В открывшемся поле введите адрес прокси-сервера в одном из следующих форматов: • `[<connection protocol>://]<address of the proxy server>:<port>`, если для подключения к прокси-серверу не требуется аутентификация; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, если для подключения к прокси-серверу требуется аутентификация. Если вы указываете IP-адрес в формате IPv6, то вводите адрес в квадратных скобках. Подключение к прокси-серверу по протоколу HTTPS не поддерживается. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-агента.
Установить исходный код ядра	Если флажок установлен, в операционных системах, не поддерживающих технологию fanotify, при запуске защиты от файловых угроз автоматически запускается компиляция модуля ядра. По умолчанию флажок установлен. Параметр применяется только на операционных системах, не поддерживающих технологию fanotify. Параметр неприменим для устройств с процессором Эльбрус.
Использовать графический пользовательский интерфейс	Установите флажок, если вы планируете установить и использовать графический интерфейс приложения. Файлы для установки графического интерфейса должны быть добавлены в инсталляционный пакет. По умолчанию флажок снят. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-агента.

Параметр	Описание
Указать пользователя с ролью администратора (admin)	Установите флажок, если вы хотите указать пользователя, которому назначается роль администратора (admin). Роль администратора позволяет управлять параметрами приложения и параметрами задач через графический интерфейс и командную строку приложения без использования команды `sudo`. В открывшемся поле введите имя пользователя.
Выполнить автоматическую настройку SELinux	Если флажок установлен, во время первоначальной настройки приложения выполняется автоматическая настройка SELinux для работы с Kaspersky Endpoint Security. По умолчанию флажок установлен.
Удалить пользователей из привилегированных групп	Установите флажок, чтобы перед установкой приложения автоматически удалить пользователей из привилегированных групп kesladmin и keslaudit. По умолчанию флажок снят. Если флажок установлен и группа nogroup отсутствует, то установка будет прервана и вам будет предложено удалить пользователей из привилегированных групп вручную.
Выключить компоненты защиты и задачи проверки при первом запуске приложения после установки	Установите флажок, если вы хотите после установки запустить приложение с выключенными компонентами защиты и задачами проверки. Установка с выключенными компонентами защиты может быть удобна, например, для воспроизведения проблемы в работе приложения с целью создания файла трассировки. Если вы включите нужные компоненты и задачи, то после перезапуска приложения включенные компоненты и задачи продолжат работу.
Включить трассировку приложения при первом запуске после установки	Установите флажок, если вы хотите включить создание файла трассировки при первом запуске приложения после установки. Для записи трассировки автоматически создается файл kesl_startup.log в директории /var/log/kaspersky/kesl/. К этому файлу не применяется ограничение на размер, заданное для обычных файлов трассировки приложения. Запись трассировки останавливается после запуска задачи Защита от файловых угроз или через пять минут после начала записи трассировки.
Механизм перехвата	Механизм перехвата системных событий, который приложение использует в своей работе: • **Технология fanotify** (значение по умолчанию). Если выбран этот вариант, приложение использует технологию fanotify для перехвата системных событий. • **Обновляемый модуль ядра**. Если выбран этот вариант, в ходе установки приложения устанавливается обновляемый модуль ядра. Приложение использует этот модуль для перехвата системных событий. Параметр применяется только на устройствах, где операционная система поддерживает технологию fanotify. Параметр неприменим для устройств с процессором Эльбрус.
Если обновляемый модуль ядра не запускается	Действие, которое приложение будет выполнять в случае ошибки запуска обновляемого модуля ядра: • **Использовать технологию fanotify** (значение по умолчанию). Если выбран этот вариант, приложение переходит к использованию технологии fanotify для перехвата системных событий. • **Выключить перехват системных событий**. Если приложение не использует перехват системных событий, проверка файлов в режиме реального времени не выполняется, уровень защиты устройства снижается. Параметр доступен, если выбран механизм перехвата **Обновляемый модуль ядра**. Параметр применяется только на устройствах, где операционная система поддерживает технологию fanotify. Параметр неприменим для устройств с процессором Эльбрус.

Параметр	Описание
Включить режим игнорирования ошибок менеджера пакетов	Установите флажок, чтобы при установке приложения игнорировать ошибки менеджера пакетов. По умолчанию флажок снят. Параметр используется, если не удается установить приложение в штатном режиме. Рекомендуется включать этот параметр только под руководством Службы технической поддержки

Параметры первоначальной настройки в Консоли администрирования

Параметры первоначальной настройки приложения

Параметр	Описание
Язык событий в KSC	Язык, который должен использоваться для локализации событий приложения, отправляемых в Kaspersky Security Center: • **Системный** (значение по умолчанию) – язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация не поддерживается, для локализации событий используется английский язык. • Один из национальных языков, поддерживаемых приложением Kaspersky Endpoint Security: английский (США), испанский (Мексика), китайский традиционный, китайский упрощенный, немецкий, португальский (Бразилия), русский, французский, японский. Для отображения графического интерфейса и командной строки приложения используется локализация, указанная в переменной окружения `LANG`. Если приложение не поддерживает указанную локализацию, то используется английская локализация.
Код активации	Если вы хотите активировать приложение во время установки, введите код активации. Параметр применяется, только если приложение используется в стандартном режиме.
Выбор источника обновлений	По нажатию на кнопку **Настроить** открывается окно, в котором вы можете выбрать источник обновлений баз и модулей приложения: • **Серверы обновлений "Лаборатории Касперского"** (значение по умолчанию). • **Kaspersky Security Center**. • **Другой источник в локальной или глобальной сети**. Если вы выбрали этот вариант, введите адрес источника обновлений в поле **Адрес**. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-агента.
Запустить задачу обновления баз после установки	Если флажок установлен, после установки приложения запускается задача обновления баз и модулей приложения. По умолчанию флажок установлен. Снимите этот флажок, если вы добавили в инсталляционный пакет предварительно скачанные базы приложения. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-агента.

Параметр	Описание
Адрес прокси-сервера	Если вы используете прокси-сервер для доступа в интернет, введите адрес прокси-сервера в одном из следующих форматов: • `[<connection protocol>://]<address of the proxy server>:<port>`, если для подключения к прокси-серверу не требуется аутентификация; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, если для подключения к прокси-серверу требуется аутентификация. Если вы указываете IP-адрес в формате IPv6, то вводите адрес в квадратных скобках. Подключение к прокси-серверу по протоколу HTTPS не поддерживается. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-агента.
Установить исходный код ядра	Если флажок установлен, в операционных системах, не поддерживающих технологию fanotify, при запуске защиты от файловых угроз автоматически запускается компиляция модуля ядра. По умолчанию флажок установлен. Параметр применяется только на операционных системах, не поддерживающих технологию fanotify. Параметр неприменим для устройств с процессором Эльбрус.
Использовать графический пользовательский интерфейс	Установите флажок, если вы планируете установить и использовать графический интерфейс приложения. Файлы для установки графического интерфейса должны быть добавлены в инсталляционный пакет. По умолчанию флажок снят. Параметр применяется, только если приложение используется в стандартном режиме или в режиме EDR-агента.
Пользователь с ролью администратора (admin)	Имя пользователя, которому назначается роль администратора (admin). Роль администратора позволяет управлять параметрами приложения и параметрами задач через графический интерфейс и командную строку приложения без использования команды `sudo`.
Выполнить автоматическую настройку SELinux	Если флажок установлен, во время первоначальной настройки приложения выполняется автоматическая настройка SELinux для работы с Kaspersky Endpoint Security. По умолчанию флажок установлен.
Удалить пользователей из привилегированных групп	Установите флажок, чтобы перед установкой приложения автоматически удалить пользователей из привилегированных групп kesladmin и keslaudit. По умолчанию флажок снят. Если флажок установлен и группа nogroup отсутствует, то установка будет прервана и вам будет предложено удалить пользователей из привилегированных групп вручную.
Выключить компоненты защиты и задачи проверки при первом запуске приложения после установки	Установите флажок, если вы хотите после установки запустить приложение с выключенными компонентами защиты и задачами проверки. Установка с выключенными компонентами защиты может быть удобна, например, для воспроизведения проблемы в работе приложения с целью создания файла трассировки. Если вы включите нужные компоненты и задачи, то после перезапуска приложения включенные компоненты и задачи продолжат работу.
Включить трассировку приложения при первом запуске после установки	Установите флажок, если вы хотите включить создание файла трассировки при первом запуске приложения после установки. Для записи трассировки автоматически создается файл kesl_startup.log в директории /var/log/kaspersky/kesl/. К этому файлу не применяется ограничение на размер, заданное для обычных файлов трассировки приложения. Запись трассировки останавливается после запуска задачи Защита от файловых угроз или через пять минут после начала записи трассировки.

Параметр	Описание
Режим использования приложения	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Режим использования приложения**. В этом окне вы можете выбрать режим использования приложения. • **Стандартный режим для защиты рабочих станций и серверов** (значение по умолчанию). Если выбран этот вариант, приложение используется как автономное приложение для защиты рабочих станций и серверов под управлением операционных систем Linux. • **Агент Endpoint Detection and Response**. Если выбран этот вариант, приложение используется для совместной работы решений Detection and Response от "Лаборатории Касперского" и антивирусных решений сторонних поставщиков на защищаемых устройствах. • **Легкий агент для защиты виртуальных сред**. Если выбран этот вариант, приложение используется в режиме Легкого агента (в составе решения Kaspersky Security для виртуальных сред Легкий агент). Режим EDR-агента и режим Легкого агента недоступны для устройств с процессором Эльбрус.
Включить Endpoint Detection and Response Expert (cloud)	Установите флажок, чтобы использовать интеграцию с Endpoint Detection and Response Expert (cloud). В стандартном режиме приложение поддерживает интеграцию с Endpoint Detection and Response Expert (cloud) и Endpoint Detection and Response Expert (on-premises). Если флажок снят, используется интеграция с Endpoint Detection and Response Expert (on-premises). Параметр применяется, только если приложение используется в стандартном режиме. Параметр неприменим для устройств с процессором Эльбрус.
Защищаемая виртуальная машина используется как сервер	Роль виртуальной машины, на которую будет установлено приложение: сервер или рабочая станция. По умолчанию флажок установлен (виртуальная машина используется в виртуальной инфраструктуре как сервер). Параметр применяется, только если приложение используется в режиме Легкого агента. Параметр неприменим для устройств с процессором Эльбрус.
Включить режим защиты инфраструктуры VDI	Установите флажок, чтобы включить режим защиты инфраструктуры VDI. Рекомендуется в случае установки приложения на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. По умолчанию флажок снят. Параметр применяется, только если приложение используется в режиме Легкого агента. Параметр неприменим для устройств с процессором Эльбрус.
Перехват системных событий	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Параметры перехвата системных событий**. В этом окне вы можете выбрать механизм перехвата системных событий, который приложение использует в своей работе: • **Технология fanotify** (значение по умолчанию). Если выбран этот вариант, приложение использует технологию fanotify для перехвата системных событий. • **Обновляемый модуль ядра**. Если выбран этот вариант, в ходе установки приложения устанавливается обновляемый модуль ядра. Приложение использует этот модуль для перехвата системных событий. Параметр применяется только на устройствах, где операционная система поддерживает технологию fanotify. Параметр неприменим для устройств с процессором Эльбрус.

Параметр	Описание
Если обновляемый модуль ядра не запускается (окно **Параметры перехвата системных событий**)	Действие, которое приложение будет выполнять в случае ошибки запуска обновляемого модуля ядра: • **Использовать технологию fanotify** (значение по умолчанию). Если выбран этот вариант, приложение переходит к использованию технологии fanotify для перехвата системных событий. • **Выключить перехват системных событий**. Если приложение не использует перехват системных событий, проверка файлов в режиме реального времени не выполняется, уровень защиты устройства снижается. Параметр доступен, если выбран механизм перехвата **Обновляемый модуль ядра**. Параметр применяется только на устройствах, где операционная система поддерживает технологию fanotify. Параметр неприменим для устройств с процессором Эльбрус.
Включить режим игнорирования ошибок менеджера пакетов	Установите флажок, чтобы при установке приложения игнорировать ошибки менеджера пакетов. По умолчанию флажок снят. Параметр используется, если не удается установить приложение в штатном режиме. Рекомендуется включать этот параметр только под руководством Службы технической поддержки

Предустановленные конфигурационные файлы

После первоначальной настройки в приложении создаются следующие конфигурационные файлы:

- /var/opt/kaspersky/kesl/common/agreements.ini

  Конфигурационный файл agreements.ini содержит параметры, связанные с Лицензионным соглашением, Политикой конфиденциальности и Положением о Kaspersky Security Network.

- /var/opt/kaspersky/kesl/common/kesl.ini

  Конфигурационный файл kesl.ini содержит параметры, приведенные в таблице ниже.

Если требуется, вы можете изменять значения параметров в файле kesl.ini.

Изменять значения по умолчанию в этих файлах рекомендуется только под руководством специалистов Службы технической поддержки по полученным от них инструкциям.

Чтобы измененные параметры в конфигурационном файле вступили в силу, перезапустите приложение Kaspersky Endpoint Security.

Если параметр отсутствует в файле или указано некорректное значение параметра, то приложение будет использовать значение по умолчанию.

Параметр	Описание	Значения
Секция **[General]** содержит следующие параметры:		
`Locale`	Языковой стандарт, используемый для локализации событий, передаваемых приложением Kaspersky Endpoint Security в Kaspersky Security Center. Для отображения графического интерфейса и командной строки приложения используется локализация, указанная в переменной окружения `LANG`. Если приложение не поддерживает указанную локализацию, то используется английская локализация.	Языковой стандарт в формате, определенном в RFC 3066. Если параметр `Locale` не указан, используется язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация не поддерживается, для локализации событий используется английский язык (en_US.UTF-8 в формате стандарта RFC 3066).
`PackageType`	Формат установленного пакета приложения. Не рекомендуется изменять значение этого параметра вручную. Значение заполняется автоматически во время первоначальной настройки приложения.	`rpm` – установлен пакет формата RPM. `deb` – установлен пакет формата DEB.
`UseFanotify`	Использование технологии fanotify для перехвата файловых операций. Не рекомендуется изменять значение этого параметра вручную. Параметр настраивается во время первоначальной настройки приложения. Параметр неприменим для устройств с процессором Эльбрус.	`true/yes` – для перехвата файловых операций приложение использует технологию fanotify. `false/no` – технология fanotify не используется.
`KsvlaMode`	Использование Kaspersky Endpoint Security в режиме Легкого агента. Не рекомендуется изменять значение этого параметра вручную. Параметр настраивается во время первоначальной настройки приложения. Параметр неприменим для устройств с процессором Эльбрус.	`true/yes` – приложение используется в режиме Легкого агента. `false/no` – приложение используется в стандартном режиме.
`EndpointAgentMode`	Использование Kaspersky Endpoint Security в режиме EDR-агента. Параметр неприменим для устройств с процессором Эльбрус.	`true/yes` – приложение используется в режиме EDR-агента. `false/no` – приложение используется в стандартном режиме.

Параметр	Описание	Значения
`KcsMode`	Использование приложения Kaspersky Endpoint Security в составе решения Kaspersky Security для контейнеров в качестве компонента Защита от файловых угроз. Не рекомендуется изменять значение этого параметра вручную. Параметр используется только в работе решения Kaspersky Security для контейнеров. Параметр неприменим для устройств с процессором Эльбрус.	`true/yes` – приложение используется в качестве компонента Защита от файловых угроз в составе решения Kaspersky Security для контейнеров. `false/no` (значение по умолчанию) – приложение используется в одном из режимов приложения Kaspersky Endpoint Security (в стандартном режиме, режиме EDR-агента или в режиме Легкого агента).
`StartupTraces`	Включение создания файлов трассировки при запуске приложения.	`true/yes` – создавать файлы трассировки при запуске приложения. `false/no` (значение по умолчанию) – не создавать файлы трассировки при запуске приложения.
`RevealSensitiveInfoInTraces`	Отображение в файлах трассировки информации, которая может содержать персональные данные (например, пароли).	`true/yes` – отображать информацию, которая может содержать персональные данные, в файлах трассировки приложения. `false/no` (значение по умолчанию) – не отображать информацию, которая может содержать персональные данные, в файлах трассировки.
`AsyncTraces`	Включение асинхронной трассировки, при которой запись информации в файлы трассировки происходит в асинхронном режиме.	`true/yes` – включить асинхронную трассировку. `false/no` (значение по умолчанию) – не включать асинхронную трассировку.
`MinFreeDiskSpace`	Минимальное количество памяти на диске, которое останется после записи файла дампа, в мегабайтах.	Значение по умолчанию: 300.
`ScanMemoryLimit`	Ограничение на использование памяти приложением в мегабайтах.	Значение по умолчанию: 8192. Рекомендуется указывать значение параметра `ScanMemoryLimit` ниже значения параметра `MaxMemory`, чтобы избежать использования всей доступной памяти задачами проверки и перезапуска приложения.
`MachineId`	Уникальный идентификатор устройства пользователя.	Значение параметра заполняется автоматически во время установки приложения.
`SocketPath`	Путь к сокету для удаленного подключения, по которому подключаются, например, графический интерфейс и утилита kesl-control.	Значение по умолчанию: /var/run/bl4control.
`MaxInotifyWatches`	Ограничение количества подписок на изменения в файлах и директориях (user watches), указанное в файле /proc/sys/fs/inotify/max_user_watches. Если значение параметра в операционной системе меньше значения параметра `MaxInotifyWatches`, приложение изменит значение параметра в операционной системе на значение параметра `MaxInotifyWatches`.	Значение по умолчанию: 299987.

Параметр	Описание	Значения
`MaxInotifyInstances`	Ограничение количества подписок на изменения в файлах и директориях на одного пользователя, указанное в файле /proc/sys/fs/inotify/max_user_instances. Если значение параметра в операционной системе меньше значения параметра `MaxInotifyInstances`, приложение изменит значение параметра в операционной системе на значение параметра `MaxInotifyInstances`.	Значение по умолчанию: 4047.
`ExecEnvMax`	Количество переменных окружения, которые приложение будет захватывать из вызова команды.	Значение по умолчанию: 50.
`ExecArgMax`	Количество аргументов, которые приложение будет захватывать из вызова exec.	Значение по умолчанию: 20.
`AdditionalDNSLookup`	Использование публичного DNS. При сбоях доступа к серверам через системный DNS приложение будет использовать публичный DNS. Это нужно для обновления баз приложения и поддержки уровня безопасности устройства. Приложение 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).	`true/yes` – использовать публичный DNS для доступа к серверам "Лаборатории Касперского". `false/no` (значение по умолчанию) – не использовать публичный DNS для доступа к серверам "Лаборатории Касперского". Запросы приложения могут содержать адреса доменов и внешний IP-адрес пользователя, так как приложение устанавливает с DNS-сервером TCP/UDP-соединение. Эти данные нужны, например, для проверки сертификата веб-ресурса при обращении по HTTPS. Если приложение использует публичный DNS-сервер, правила обработки данных регламентируются Политикой конфиденциальности этого сервиса.
`PanicThreshold`	Максимальное количество нештатных остановок приложения при использовании обновляемого модуля ядра. При достижении указанного значения приложение переходит в "безопасный" режим, в котором обновляемый модуль ядра не запускается. Параметр неприменим для устройств с процессором Эльбрус.	Значение по умолчанию: 3.
`SafeMode`	Включение "безопасного" режима работы приложения при использовании обновляемого модуля ядра. В этом режиме приложение не запускает обновляемый модуль ядра. "Безопасный" режим включается автоматически, если достигнуто максимальное количество нештатных остановок приложения, заданное параметром `PanicThreshold`. Параметр неприменим для устройств с процессором Эльбрус.	`true/yes` – включен "безопасный" режим работы приложения. `false/no` (значение по умолчанию) – "безопасный" режим работы приложения выключен, приложение работает в штатном режиме.

Параметр	Описание	Значения
`GetContainerName`	Передача в данных телеметрии следующей информации о контейнере при интеграции с Kaspersky Managed Detection and Response: • признак того, что событие произошло в контейнере; • идентификатор пространства имен контейнера; • имя контейнера. Имя контейнера передается только при наличии лицензии на использование задачи Проверка контейнеров и при достаточном времени жизни контейнера. Параметр неприменим для устройств с процессором Эльбрус.	`true/yes` (значение по умолчанию) – передавать расширенную информацию о контейнере в данных телеметрии при интеграции с Kaspersky Managed Detection and Response. `false/no` – не передавать расширенную информацию о контейнере в данных телеметрии при интеграции с Kaspersky Managed Detection and Response.
`UseIncreasedXdrEventsCache`	Управление кешем событий при интеграции с решениями Detection and Response. Вы можете выбрать между высокой производительностью и объемом используемой оперативной памяти.	`true/yes` (значение по умолчанию) – в щадящем режиме работать с диском, но при этом расходовать больше памяти (100 МБ). `false/no` – расходовать меньше памяти (около 5 МБ), но активнее читать с диска и записывать на диск.
`FastShutdown`	Ускоренное завершение процесса kesl при остановке или перезапуске приложения.	`true/yes` – включить ускоренное завершение процесса kesl при остановке приложения. `false/no` (значение по умолчанию) – выключить ускоренное завершение процесса kesl при остановке приложения.
Секция **[Network]** содержит следующие параметры:		
`WtpFwMark`	Метка в правилах утилиты iptables для перенаправления трафика в приложение для обработки компонентом Защита от веб-угроз. Вам может потребоваться изменить эту метку, если на одном устройстве с установленным приложением работает другое ПО, которое использует девятый бит маски TCP-пакета, и возникает конфликт.	Значение задается десятеричным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 0x100. Во избежание цикличной проверки трафика при работе приложения на узлах, используемых в составе распределенных систем, таких как Kubernetes, требуется изменить значения меток сетевых пакетов, используя более старшие биты. Например: 0x1000 или 0x10000 (значение метки ограничено 32-битным целым числом).
`NtpFwMark`	Метка в правилах утилиты iptables для перенаправления трафика в приложение для обработки компонентом Защита от сетевых угроз. Вам может потребоваться изменить эту метку, если на одном устройстве с установленным приложением работает другое ПО, которое использует девятый бит маски TCP-пакета, и возникает конфликт.	Значение задается десятеричным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 0x200. Во избежание цикличной проверки трафика при работе приложения на узлах, используемых в составе распределенных систем, таких как Kubernetes, требуется изменить значения меток сетевых пакетов, используя более старшие биты. Например: 0x2000 или 0x20000 (значение метки ограничено 32-битным целым числом).

Параметр	Описание	Значения
`BypassFwMark`	Метка, которой маркируются пакеты, созданные или проверенные приложением, чтобы они снова не попали в приложение на проверку.	Значение задается десятеричным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 0x400. Во избежание цикличной проверки трафика при работе приложения на узлах, используемых в составе распределенных систем, таких как Kubernetes, требуется изменить значения меток сетевых пакетов, используя более старшие биты. Например: 0x4000 или 0x40000 (значение метки ограничено 32-битным целым числом).

`BypassNFlogMark`	Метка для маркировки пакетов, которые приложение будет игнорировать при проверке.	Значение задается десятеричным или шестнадцатеричным числом с префиксом 0x.
		Значение по умолчанию: 0x800.
		Примеры:
		Игнорировать весь сетевой трафик по протоколу TCP с указанным устройством:
		`iptables -t mangle -A PREROUTING -s <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -d <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		Игнорировать трафик HTTPS-сервера:
		`iptables -t mangle -A PREROUTING -p tcp -m tcp --dport 443 -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -p tcp -m tcp --sport 443 -j MARK --set-xmark 0x800/0x800`
		Во избежание цикличной проверки трафика при работе приложения на узлах, используемых в составе распределенных систем, таких как Kubernetes, требуется изменить значения меток сетевых пакетов, используя более старшие биты. Например: 0x8000 или 0x80000 (значение метки ограничено 32-битным целым числом).

`ProxyRouteTable`	Номер таблицы маршрутизации.	Значение по умолчанию: 101.
Секция **[ScannerImpactStats]** содержит следующие параметры:		
`CollectFileScanStatistics`	Включение подсчета статистики проверки файлов и процессов приложением.	`true/yes` (значение по умолчанию) – включить подсчет статистики проверки файлов и процессов. `false/no` – не включать подсчет статистики проверки файлов и процессов.
`StatCollectionPeriod`	Интервал времени, в течение которого приложение считает статистику проверенных файлов и обнаруженных процессов перед сохранением в файл трассировки и в отчеты.	Значение по умолчанию: 10 минут.
`StatCollectionCount`	Количество проверенных файлов и обнаруженных процессов, которые были посчитаны приложением за интервал времени, указанный параметром `StatCollectionPeriod`, и которые попадут в отчет и в файлы трассировки.	Значение по умолчанию: 10.
`ReportStatAmount`	Количество записей, которые будут выведены в отчеты о наиболее часто проверяемых файлах и процессах за сутки.	Значение по умолчанию: 20.
Секция **[Virtualization]** содержит следующие параметры:		

Параметр	Описание	Значения
`ServerMode`	Роль защищенной виртуальной машины, на которой приложение Kaspersky Endpoint Security используется в режиме Легкого агента: сервер или рабочая станция. Не рекомендуется изменять значение этого параметра вручную. Параметр настраивается во время первоначальной настройки приложения. Параметр неприменим для устройств с процессором Эльбрус.	`true/yes` – виртуальная машина используется как сервер. `false/no` – виртуальная машина используется как рабочая станция.
`VdiMode`	Включение режима защиты инфраструктуры VDI в случае использования приложения в режиме Легкого агента. Не рекомендуется изменять значение этого параметра вручную. Параметр настраивается во время первоначальной настройки приложения. Параметр неприменим для устройств с процессором Эльбрус.	`true/yes` – режим защиты инфраструктуры VDI включен. `false/no` – режим защиты инфраструктуры VDI выключен.
Секция **[Watchdog]** содержит следующие параметры:		
`TimeoutAfterHeadshot`	Максимальное время ожидания завершения процесса kesl от момента отправки сигнала HEADSHOT Watchdog-сервером процессу kesl.	Значение по умолчанию: 2 минуты.
`StartupTimeout`	Максимальное время ожидания запуска приложения (в минутах), после которого Watchdog-сервер начинает процедуру перезапуска процесса kesl.	Значение по умолчанию: 3 минуты.
`TimeoutAfterKill`	Максимальное время ожидания завершения управляемого процесса kesl от момента отправки сигнала SIGKILL Watchdog-сервером процессу kesl. Если по истечении этого времени процесс kesl не завершился, выполняется действие, заданное параметром `--failed-kill`.	Значение по умолчанию: 2 дня.
`PingInterval`	Периодичность, с которой приложение пытается отправить Watchdog-серверу сообщение PONG в ответ на принятое сообщение PING.	Значение по умолчанию: 2000 миллисекунд.
`MaxRestartCount`	Максимальное количество неудачных последовательных попыток запуска приложения.	Значение по умолчанию: 5.
`ActivityTimeout`	Максимальный интервал времени, в течение которого приложение должно отправить сообщение Watchdog-серверу. Если в течение этого интервала времени от приложения не будет сообщения, Watchdog-сервер начинает процедуру перезапуска процесса kesl.	Значение по умолчанию: 2 минуты.
`ConnectTimeout`	Максимальное время ожидания соединения приложения с Watchdog-сервером от момента запуска процесса kesl. Если приложение не успевает создать соединение за этот интервал времени, Watchdog-сервер начинает процедуру перезапуска процесса kesl.	Значение по умолчанию: 3 минуты.

Параметр	Описание	Значения
`RegisterTimeout`	Максимальный интервал времени от момента соединения приложения с Watchdog-сервером до получения сервером сообщения REGISTER.	Значение по умолчанию: 500 миллисекунд.
`TimeoutAfterShutdown`	Максимальное время ожидания завершения процесса kesl от момента отправки сигнала SHUTDOWN Watchdog-сервером процессу kesl.	Значение по умолчанию: 2 минуты.
`MaxMemory`	Ограничение на использование резидентной памяти процесса kesl. Если резидентная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру перезапуска процесса kesl.	`off` – использование резидентной памяти не ограничено. `<value>%` – значение от 1 до 100 в процентах от объема памяти. `<value>MB` – значение в мегабайтах. `lowest/<value>%/<value>MB` – наименьшее значение между значением в процентах и значением в мегабайтах. `highest/<value>%/<value>MB` – наибольшее значение между значением в процентах и значением в мегабайтах. `auto` – до 50% доступной памяти, но не менее 2ГБ и не более 16ГБ. Значение по умолчанию: `auto`.
`MaxVirtualMemory`	Ограничение на использование виртуальной памяти процесса kesl. Если виртуальная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру перезапуска процесса kesl.	`off` (значение по умолчанию) – использование виртуальной памяти не ограничено. `<value>MB` – значение в мегабайтах.
`MaxSwapMemory`	Ограничение на размер swap-файла управляемого процесса kesl. Если swap-файл управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру перезапуска процесса kesl.	`off` (значение по умолчанию) – размер swap-файла не ограничен. `<value>%` – значение от 0 до 100 в процентах от объема памяти. `<value>MB` – значение в мегабайтах. `lowest/<value>%/<value>MB` – наименьшее значение между значением в процентах и значением в мегабайтах. `highest/<value>%/<value>MB` – наибольшее значение между значением в процентах и значением в мегабайтах.
`TrackProductCrashes`	Включение отправки статуса устройства от приложения Kaspersky Endpoint Security в Kaspersky Security Center при нестабильной работе приложения.	`true/yes` – включить отправку статуса устройства от приложения Kaspersky Endpoint Security в Kaspersky Security Center. `false/no` (значение по умолчанию) – выключить отправку статуса устройства от приложения Kaspersky Endpoint Security в Kaspersky Security Center.
`ProductHealthLogFile`	Путь к файлу, с помощью которого осуществляется мониторинг стабильности приложения.	Значение по умолчанию: /var/opt/kaspersky/kesl/private/kesl_health.log.
`WarnThreshold`	Интервал времени (в секундах), за который приложение должно посчитать количество нештатных остановок, прежде чем вывести уведомление о нестабильной работе.	Значение по умолчанию: 3600 секунд.
`WarnAfter_#_crash`	Максимальное количество нештатных остановок приложения, по достижении которого отображается уведомление о нестабильной работе приложения.	Значение по умолчанию: 10. Если указано значение 0, уведомление о нестабильной работе приложения не отображается.
`WarnRemovingThreshold`	Интервал времени (в секундах), по истечении которого статус о нестабильной работе приложения будет снят.	Значение по умолчанию: 86400 секунд.

Параметр	Описание	Значения
`SyscallHangProbePeriod`	Периодичность, с которой Watchdog-сервер вызывает системные функции open и execve и увеличивает счетчики успешного вызова этих функций.	Значение по умолчанию: 3 секунды.
`SyscallHangCheckPeriod`	Периодичность, с которой Watchdog-сервер проверяет счетчики успешного вызова функций open и execve. Если по истечении этого времени значение счетчиков не изменилось, Watchdog-сервер начинает процедуру перезапуска процесса kesl.	Значение по умолчанию: 32 секунды.
`DumpSuspendPeriod`	Максимальное время ожидания завершения создания файла дампа приложения, в течение которого Watchdog-сервер приостанавливает проверку активности приложения. Если по истечении этого времени создание файла дампа не завершилось, Watchdog-сервер начинает процедуру перезапуска процесса kesl.	Возможные значения: 1 – 30 минут. Значение по умолчанию: 2 минуты.
`TimeoutAfterCoredump`	Максимальный интервал времени, в течение которого Watchdog-сервер приостанавливает отправку других сигналов процессу kesl после отправки сигнала SIGTRAP, который отправляется в ходе процедуры нештатной остановки процесса.	Значение по умолчанию: 2 минуты. Рекомендуется указывать значение параметра `TimeoutAfterCoredump` больше или равным значению параметра `DumpSuspendPeriod`. Вы можете указать значение параметра в следующих единицах измерения: • `<n> day|days|d` – дни; • `<n> hour|hours|hr|h` – часы; • `<n> minute|minutes|min|m` – минуты; • `<n> second|seconds|sec|s` – секунды; • `<n> [msec|ms]` – миллисекунды. Если единица измерения не указана, приложение по умолчанию будет использовать значение в миллисекундах.
`TimeoutMaxCleanPeriod`	Максимальный интервал времени, которое дается процессу очистки правил сетевого экрана операционной системы. Если в течение этого интервала времени от процесса нет сообщения о завершении работы, то Watchdog-сервер считает, что процесс завис.	Значение по умолчанию: 10 секунд.
`TimeoutAfterClean`	Максимальный интервал времени, которое дается процессу очистки правил сетевого экрана операционной системы на завершение работы после того, как Watchdog-сервер отправил процессу очистки сигнал SIGTERM.	Значение по умолчанию: 10 секунд.
Секция **[Environment]** по умолчанию отсутствует в конфигурационном файле.		

Параметр	Описание	Значения
`ExperimentalContainerdSupport`	Включение поддержки среды containerd при работе компонента Мониторинг контейнеров. Этот параметр по умолчанию отсутствует в конфигурационном файле. Если вы хотите использовать среду containerd при работе компонента Мониторинг контейнеров, вам нужно вручную добавить в конфигурационный файл секцию `[Environment]` и добавить в нее параметр `ExperimentalContainerdSupport`. Параметр неприменим для устройств с процессором Эльбрус.	`true/yes` – включить поддержку среды containerd в работе компонента Мониторинг контейнеров. `false/no` – не включать поддержку среды containerd в работе компонента Мониторинг контейнеров.
`ReduceSWMemoryConsumption`	Ограничение памяти, потребляемой компонентом Анализ поведения на обработку очереди событий. Включение ограничение памяти негативно сказывается на обнаружении угроз и в том числе на качестве телеметрии, передаваемой при интеграции с решениями Detection and Response. Рекомендуется включать ограничение только на высоконагруженных системах под руководством специалистов Службы технической поддержки по полученным от них инструкциям при отсутствии других вариантов решения проблемы высокого потребления памяти.	1 – включить ограничение памяти, потребляемой компонентом Анализ поведения на обработку очереди событий. 0 (значение по умолчанию) – не включать ограничение памяти. После изменения значения этого параметра требуется перезапустить приложение.

Параметры задач командной строки по умолчанию

Этот раздел содержит параметры по умолчанию всех предустановленных задач, которые предусмотрены для управления приложением Kaspersky Endpoint Security с помощью командной строки.

Задачи `Rollback` и `License` не имеют параметров.

Параметры по умолчанию задачи File_Threat_Protection (ID:1)

```
ScanArchived=No

ScanSfxArchived=No

ScanMailBases=No

ScanPlainMail=No

SkipPlainTextFiles=No
```

SkipDatabaseJournals=No

TimeLimit=60

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanByAccessType=SmartCheck

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*

Параметры по умолчанию задачи Scan_My_Computer (ID:2)

ScanFiles=Yes

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

```
TimeLimit=0

SizeLimit=0

QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Параметры по умолчанию задачи Scan_File (ID:3)

```
ScanFiles=Yes

ScanBootSectors=No

ScanComputerMemory=No

ScanStartupObjects=No

ScanArchived=Yes

ScanSfxArchived=Yes
```

```
ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Параметры по умолчанию задачи Critical_Areas_Scan (ID:4)

```
ScanFiles=No

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes
```

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

QueueScanTasks=No

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*

Параметры по умолчанию задачи Update (ID:6)

ConnectionTimeout=10

ApplicationUpdateMode=DownloadOnly

```
[Sources.item_0000]

Enabled=Yes

SourceType=KLServers

URL=
```

Параметры по умолчанию задачи System_Integrity_Monitoring (ID:11)

```
UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=Kaspersky internal objects

UseScanArea=Yes

Path=/opt/kaspersky/kesl/

AreaMask.item_0000=*
```

Параметры по умолчанию задачи Firewall_Management (ID:12)

```
DefaultIncomingAction=Allow

DefaultIncomingPacketAction=Allow

OpenNagentPorts=Yes

[NetworkZonesTrusted]

[NetworkZonesLocal]

[NetworkZonesPublic]
```

Параметры по умолчанию задачи Anti_Cryptor (ID:13)

```
ActionOnDetect=Block

BlockTime=30

UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=All shared directories

UseScanArea=Yes
```

```
Path=AllShared

AreaMask.item_0000=*
```

Параметры по умолчанию задачи Web_Threat_Protection (ID:14)

```
UseTrustedAddresses=Yes

ActionOnDetect=Block

CheckMalicious=Yes

CheckPhishing=Yes

UseHeuristicForPhishing=Yes

CheckAdware=No

CheckOther=No
```

Параметры по умолчанию задачи Device_Control (ID:15)

```
OperationMode=Block

AllowToRequestTemporaryAccess=No

[DeviceClass]

HardDrive=DependsOnBus

RemovableDrive=DependsOnBus

Printer=DependsOnBus

FloppyDrive=DependsOnBus

OpticalDrive=DependsOnBus

Modem=DependsOnBus

TapeDrive=DependsOnBus

MultifuncDevice=DependsOnBus

SmartCardReader=DependsOnBus

PortableDevice=DependsOnBus

WiFiAdapter=DependsOnBus

NetworkAdapter=DependsOnBus
```

```
BluetoothDevice=DependsOnBus

ImagingDevice=DependsOnBus

SerialPortDevice=DependsOnBus

ParallelPortDevice=DependsOnBus

InputDevice=DependsOnBus

SoundAdapter=DependsOnBus

[DeviceBus]

USB=Allow

FireWire=Allow

[Schedules.item_0000]

ScheduleName=Default

DaysHours=All

[HardDrivePrincipals.item_0000]

Principal=\Everyone

[HardDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[RemovableDrivePrincipals.item_0000]

Principal=\Everyone

[RemovableDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[FloppyDrivePrincipals.item_0000]

Principal=\Everyone

[FloppyDrivePrincipals.item_0000.AccessRules.item_0000]
```

```
UseRule=Yes

ScheduleName=Default

Access=Allow

[OpticalDrivePrincipals.item_0000]

Principal=\Everyone

[OpticalDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow
```

Параметры по умолчанию задачи Removable_Drives_Scan (ID:16)

```
ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No
```

Параметры по умолчанию задачи Network_Threat_Protection (ID:17)

```
ActionOnDetect=Block

BlockAttackingHosts=Yes

BlockDurationMinutes=60

UseExcludeIPs=No
```

Параметры по умолчанию задач Container_Scan (ID:18) и Custom_Container_Scan (ID:19)

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0
```

```
SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanContainers=Yes

ContainerNameMask=*

ScanImages=Yes

ImageNameMask=*

DeepScan=No

ContainerScanAction=StopContainerIfFailed

ImageAction=Skip

UseGlobalExclusions=Yes

QueueScanTasks=No
```

Вы можете использовать параметры этого конфигурационного файла также для задачи Выборочная проверка контейнеров.

Параметры по умолчанию задачи Behavior_Detection (ID:20)

```
UseTrustedPrograms=No

TaskMode=Block

UseAEP=No

AEPMode=Block
```

```
UseTelemetryMonopolyMode=Yes

TelemetrySource=Default
```

Параметры по умолчанию задачи Application_Control (ID:21)

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules
```

Параметры по умолчанию задачи Inventory_Scan (ID:22)

```
ScanScripts=Yes

ScanBinaries=Yes

ScanAllExecutable=Yes

GoldenImageAction=DoNothing

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

Параметры по умолчанию задачи KATAEDR (ID:24)

```
Mode=EDRKATA

UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=127.0.0.1

Port=443
```

```
[EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

[TelemetrySettings]

UseClientPinnedCertificate=No

ConnectionTimeout=10

RequestTimeout=10

OnlyTaggedEvents=No

[TelemetrySettings.Endpoints.item_#]

Address=

Port=443

[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Параметры по умолчанию задачи Web_Control (ID:26)

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

Параметры по умолчанию задачи Standalone_Sandbox (ID:29)

```
ConnectionTimeout=10

RequestTimeout=10

UseClientCertificate=No

SendingMode=AutoOnly
```

```
QuarantineFile=Yes

ScanCriticalAreas=Yes

CreateIocScanTask=Yes

QuarantineFileOnIocDetected=Yes

ScanCriticalAreasOnIocDetected=Yes

Drives=Critical

ScheduleMode=Manually

[Servers.item_0000]

Address=127.0.0.1

Port=443

[SandboxTransferSettings]

SandboxQueue=1024
```

Параметры по умолчанию задачи KATANDR (ID:31)

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

[Endpoints.item_0000]

Address=127.0.0.1

Port=8081

[EventTransferSettings]

MaximumDataTransferTime=30

MaximumNumberOfEventsInPackage=1024

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

PingPeriod=450
```

Параметры по умолчанию задачи KUMA (ID:33)

```
UseClientCertificate=No

UseTls=No

ConnectionTimeout=5

[Servers.item_0000]

Address=127.0.0.1

Port=443

Protocol=TCP

[SiemTransferSettings]

EventTransferTimeMax=30
```

Параметры по умолчанию задачи Защита от почтовых угроз (ID: 35)

```
CheckIncomingMessagesOnly=No

ActionOnThreat=DisinfectDeleteIfNotPossible

ScanFileArchive=Yes

ScanFileOffice=Yes

UseTimeLimit=No

TimeLimit=8

UseSizeLimit=No

SizeLimit=5

ExtensionFilter=Rename

UseAnalyzer=Yes

AnalyzerLevel=Medium

[ExtensionMasks.item_0000]

UseExtensionMask=Yes

ExtensionMask=*.txt
```

```
[ExtensionMasks.item_0001]

UseExtensionMask=Yes

ExtensionMask=*.run

[ExtensionMasks.item_0002]

UseExtensionMask=Yes

ExtensionMask=*.exe

[ExtensionMasks.item_0003]

UseExtensionMask=Yes

ExtensionMask=*.js

[ExtensionMasks.item_0004]

UseExtensionMask=Yes

ExtensionMask=*.jse

[ExtensionMasks.item_0005]

UseExtensionMask=Yes

ExtensionMask=*.msi

[ExtensionMasks.item_0006]

UseExtensionMask=Yes

ExtensionMask=*.scr

[ExtensionMasks.item_0007]

UseExtensionMask=Yes

ExtensionMask=*.vbe

[ExtensionMasks.item_0008]

UseExtensionMask=Yes

ExtensionMask=*.vbs

[ExtensionMasks.item_0009]

UseExtensionMask=Yes

ExtensionMask=*.sh
```

Параметры по умолчанию задачи Защита от атак BadUSB (ID:37)

```
MaxAuthAttempts=5

TimeoutAfterAttempts=5

ProhibitOnScreenKeyboard=No

ProhibitBarcodeScanner=Yes
```

Параметры по умолчанию задачи KATANDR (ID:31)

```
ConnectionTimeout=10

RequestTimeout=10

SynchronizationPeriod=5

UseTunnel=No

TunnelAddress=127.0.0.1

TunnelPort=443

[Endpoints.item_0000]

Address=127.0.0.1
Port=443
EnableTelemetry=Yes
[TelemetrySettings]

ConnectionTimeout=10
RequestTimeout=10
OnlyTaggedEvents=No
UseTunnel=No
TunnelAddress=127.0.0.1
TunnelPort=443
[TelemetrySettings.Endpoints.item_0000]

Address=127.0.0.1
Port=443
[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30
UseRequestCountLimits=Yes
MaximumNumberOfEventsInHour=3000
```

```
EventLimitExceededPercentage=15
MaximumNumberOfEventsInPackage=1024
```

Приложение 2. Настройка совместной работы с Антивирусом Касперского для Linux Mail Server

Чтобы настроить совместную работу приложения Kaspersky Endpoint Security с Антивирусом Касперского для Linux Mail Server:

1. Сохраните параметры задачи Защита от файловых угроз в конфигурационном файле с помощью следующей команды:

   ```
   kesl-control --get-settings 1 --file <полный путь к файлу>
   ```

2. Откройте созданный конфигурационный файл для редактирования.

3. Добавьте в созданный файл следующий раздел:

   ```
   [ExcludedFromScanScope.item_<номер элемента>]
   Path=/var/opt/kaspersky/klms
   ```

4. Повторите указанный выше раздел для всех почтовых агентов, интегрированных с Антивирусом Касперского для Linux Mail Server.

5. Для исключения из проверки временной директории фильтров и служб Антивируса Касперского для Linux Mail Server добавьте в созданный файл следующую секцию:

   ```
   [ExcludedFromScanScope.item_<номер элемента>]
   Path=/tmp/klmstmp
   ```

6. Сохраните изменения в конфигурационном файле.

7. Импортируйте параметры из конфигурационного файла в задачу Защита от файловых угроз с помощью следующей команды:

   ```
   kesl-control --set-settings 1 --file <полный путь к файлу>
   ```

Приложение 3. Параметры для взаимодействия с внешними службами

Приложение Kaspersky Endpoint Security использует следующие сетевые параметры и параметры, использующиеся для шифрования для взаимодействия с внешними службами.

Параметры для взаимодействия с внешними службами

Сетевой адрес службы и протокол	Описание
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Протокол: `HTTPS` Порт: `443`	Активация приложения.

Сетевой адрес службы и протокол	Описание

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
Протокол: HTTPS
Порт: 443
	Обновление баз и модулей приложения.

Сетевой адрес службы и протокол	Описание

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
Протокол: `HTTP`
Порт: `80`
	Обновление баз и модулей приложения.

`downloads.upd.kaspersky.com` Протокол: `HTTPS` Порт: `443`	• Обновление баз и модулей приложения. • Проверка доступа к серверам "Лаборатории Касперского". При сбоях доступа к серверам через системный DNS приложение будет использовать публичный DNS. Это нужно для обновления баз приложения и поддержки уровня безопасности устройства. Приложение будет использовать следующие публичные DNS в порядке их обхода: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Запросы приложения могут содержать адреса доменов и внешний IP-адрес пользователя, так как приложение устанавливает с DNS-сервером TCP/UDP-соединение. Эти данные нужны, например, для проверки сертификата веб-ресурса при обращении по HTTPS. Если приложение использует публичный DNS-сервер, правила обработки данных регламентируются Политикой конфиденциальности этого сервиса.
`ds.kaspersky.com` Протокол: `HTTPS` Порт: `443`	Использование Kaspersky Security Network.

Сетевой адрес службы и протокол	Описание

`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-cinfo-geo.kaspersky-labs.com`
Протокол: `KSN`
Порт: `443`, `1443`
	Использование Kaspersky Security Network.

`click.kaspersky.com` Протокол: `HTTPS` Порт: `443`	Переход по ссылкам из интерфейса.

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Протокол: `HTTP`
Порт: `80`
	Инфраструктура открытых ключей (англ. Public Key Infrastructure, PKI).
	Эти серверы (crl.kaspersky.com) являются частью инфраструктуры открытых ключей (PKI) и необходимы для проверки статуса действительности сертификатов цифровой подписи "Лаборатории Касперского". Сервер CRL предоставляет список отозванных сертификатов. Служба OCSP позволяет запрашивать статус конкретного сертификата в режиме реального времени. Работа этих компонентов обеспечивает безопасность взаимодействия с цифровыми сертификатами и защиту от возможных атак.

Приложение 4. Расширения файлов для быстрой проверки съемных дисков

com – исполняемый файл приложения размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив;

sys – системный файл Microsoft Windows;

prg – текст приложения dBase™, Clipper или Microsoft Visual FoxPro®, приложение пакета WAVmaker;

bin – бинарный файл;

bat – файл пакетного задания;

cmd – командный файл Microsoft Windows NT (аналогичен bat-файлу для DOS), OS/2;

dpl – упакованная библиотека Borland Delphi;

dll – библиотека динамической загрузки;

scr – файл-заставка экрана Microsoft Windows;

cpl – модуль панели управления (control panel) в Microsoft Windows;

ocx – объект Microsoft OLE (Object Linking and Embedding);

tsp – приложение, работающее в режиме разделения времени;

drv – драйвер некоторого устройства;

vxd – драйвер виртуального устройства Microsoft Windows;

pif – файл с информацией о приложении;

lnk – файл-ссылка в Microsoft Windows;

reg – файл регистрации ключей системного реестра Microsoft Windows;

ini – файл конфигурации, который содержит данные настроек для Microsoft Windows, Windows NT и некоторых приложений;

cla – класс Java;

vbs – скрипт Visual Basic®;

vbe – видеорасширение BIOS;

js, jse – исходный текст JavaScript;

htm – гипертекстовый документ;

htt – гипертекстовая заготовка Microsoft Windows;

hta – гипертекстовое приложение для Microsoft Internet Explorer®;

asp – скрипт Active Server Pages;

chm – скомпилированный HTML-файл;

pht – HTML-файл со встроенными скриптами PHP;

php – скрипт, встраиваемый в HTML-файлы;

wsh – файл Microsoft Windows Script Host;

wsf – скрипт Microsoft Windows;

the – файл заставки для рабочего стола Microsoft Windows 95;

hlp – файл справки формата Win Help;

msg – сообщение электронной почты Microsoft Mail;

plg – сообщение электронной почты;

mbx – сохраненное сообщение электронной почты Microsoft Office Outlook;

doc* – документы Microsoft Office Word, такие как: doc – документ Microsoft Office Word, docx – документ Microsoft Office Word 2007 с поддержкой языка XML, docm – документ Microsoft Office Word 2007 с поддержкой макросов;

dot* – шаблоны документа Microsoft Office Word, такие как: dot – шаблон документа Microsoft Office Word, dotx – шаблон документа Microsoft Office Word 2007, dotm – шаблон документа Microsoft Office Word 2007 с поддержкой макросов;

fpm – приложение баз данных, стартовый файл Microsoft Visual FoxPro;

rtf – документ в формате Rich Text Format;

shs – фрагмент Windows Shell Scrap Object Handler;

dwg – база данных чертежей AutoCAD®;

msi – пакет Microsoft Windows Installer;

otm – VBA-проект для Microsoft Office Outlook;

pdf – документ Adobe Acrobat;

swf – объект пакета Shockwave® Flash;

jpg, jpeg – файл графического формата хранения сжатых изображений;

emf – файл формата Enhanced Metafile;

ico – файл значка объекта;

ov? – исполняемые файлы Microsoft Office Word;

xl* – документы и файлы Microsoft Office Excel, такие как: xla – расширение Microsoft Office Excel, xlc – диаграмма, xlt – шаблон документа, xlsx – рабочая книга Microsoft Office Excel 2007, xltm – рабочая книга Microsoft Office Excel 2007 с поддержкой макросов, xlsb – рабочая книга Microsoft Office Excel 2007 в бинарном (не XML) формате, xltx – шаблон Microsoft Office Excel 2007, xlsm – шаблон Microsoft Office Excel 2007 с поддержкой макросов, xlam – надстройка Microsoft Office Excel 2007 с поддержкой макросов;

pp* – документы и файлы Microsoft Office PowerPoint®, такие как: pps – слайд Microsoft Office PowerPoint, ppt – презентация, pptx – презентация Microsoft Office PowerPoint 2007, pptm – презентация Microsoft Office PowerPoint 2007 с поддержкой макросов, potx – шаблон презентации Microsoft Office PowerPoint 2007, potm – шаблон презентации Microsoft Office PowerPoint 2007 с поддержкой макросов, ppsx – слайд-шоу Microsoft Office PowerPoint 2007, ppsm – слайд-шоу Microsoft Office PowerPoint 2007 с поддержкой макросов, ppam – надстройка Microsoft Office PowerPoint 2007 с поддержкой макросов;

md* – документы и файлы Microsoft Office Access®, такие как: mda – рабочая группа Microsoft Office Access, mdb – база данных;

sldx – слайд Microsoft Office PowerPoint 2007;

sldm – слайд Microsoft Office PowerPoint 2007 с поддержкой макросов;

thmx – тема Microsoft Office 2007.

Приложение 5. Переменные в шаблонах сообщений

В компонентах Контроль устройств и Веб-Контроль предусмотрены шаблоны сообщений, которые Kaspersky Endpoint Security покажет пользователю при попытке доступа к заблокированному устройству, приложению или ресурсу или при попытке выполнить потенциально опасное действие.

Для работы с шаблонами сообщений предусмотрены специальные переменные (например, `%USER_NAME%`). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров. При формировании сообщения Kaspersky Endpoint Security определяет значение переменной из настроек операционной системы и подставляет это значение в сообщение, соответствующие конкретному компьютеру, пользователю и событию.

Переменные в шаблонах сообщений Контроля устройств

В шаблонах сообщений пользователю или администратору вы можете использовать следующие переменные:

- **Пользователь** – `%USER_NAME%`.

  Имя текущей учетной записи компьютера, на котором появилось сообщение, в формате `<device name>\<user alias>` (например, `DESKTOP-123\John.Smith`).

- **Имя компьютера** – `%COMPUTER_NAME%`.

  Название компьютера, на котором было заблокировано устройство.

- **Имя правила** – `%RULE%`.

  Название правила, в соответствии с которым заблокировано устройство.

- **Дата срабатывания правила** – `%DATE%`.

  Дата блокировки устройства в формате ДД.ММ.ГГГГ.

- **Время срабатывания правила** – `%TIME%`.

  Время блокировки устройства в формате в формате ЧЧ:ММ.

- **Имя устройства** – `%DEVICE_NAME%`.

  Название заблокированного устройства.

- **Тип устройства** – `%DEVICE_TYPE%`.

  Тип заблокированного устройства (например, принтеры, съемные диски, CD/DVD-приводы).

- **Модель устройства** – `%DEVICE_VIDPID%`.

  Модель заблокированного устройства (например, VID_1234&PID_5678).

- **Идентификатор устройства** – `%DEVICE_ID%`.

  Идентификатор заблокированного устройства (например, `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`).

- **Операции с устройствами** – `%OPERATION%`.

  Тип запрещенной операции с устройством.

Переменные в шаблонах сообщений Веб-Контроля

В шаблонах сообщений пользователю или администратору вы можете использовать следующие переменные:

- **Пользователь** – `%USER_NAME%`.

  Имя текущей учетной записи компьютера, на котором появилось сообщение, в формате `<device name>\<user alias>` (например, `DESKTOP-123\John.Smith`).

- **Адрес веб-ресурса** – `%CANONIC_REQUEST_URL%`.

  Адрес заблокированного веб-ресурса.

- **Имя правила** – `%RULE%`.

  Название правила, в соответствии с которым заблокирован веб-ресурс.

- **Адрес для отправки сообщения** – `%COMPLAIN_EMAIL%`.

  Адрес электронной почты для отправки отзыва о блокировании веб-ресурса. При нажатии на адрес электронной почты приложение открывает окно, в котором пользователь может написать сообщение администратору.

- **Название категории содержания** – `%CONTENT_CATEGORY_LIST%`.

  Категория веб-сайта, в которую включен заблокированный веб-ресурс (например, *Платежные системы*).

- **Название категории типа данных** – `%TYPE_CATEGORY_LIST%`.

  Категория типа данных, размещенных на заблокированном веб-ресурсе (например, *Графические файлы*).

- **Ссылка на запрошенный веб-ресурс** – `%CONTINUE_PAGE%`.

  Ссылка на запрошенную веб-страницу (например, `http://www.example.com/pagename.html`).

- **Ссылка на сайт** – `%CONTINUE_SITE%`.

  Ссылка на веб-сайт, на котором расположена запрошенная веб-страница (например, `http://www.example.com/`).

- **Ссылка для доступа к доменам** – `%CONTINUE_DOMAIN%`.

  Ссылка, переход по которой открывает доступ ко всем существующим веб-страницам доменного имени. Например, если адрес заблокированной веб-страницы `http://www.example.com`, то переменная `%CONTINUE_DOMAIN%` заменяется ссылкой `http://*.example.com`. Переход по этой ссылке открывает доступ ко всем веб-адресам основного доменного имени `http://www.example.com/`, включая его поддомены, например, `http://start.example.com/*` или `http://domain.domain.example.com/*`, где символ `*` обозначает любую последовательность символов (в том числе пустую).

Приложение 6. События в работе приложения

Информация о работе каждого компонента Kaspersky Endpoint Security, о событиях шифрования данных, о выполнении каждой задачи поиска вредоносного ПО, задачи обновления и задачи проверки целостности, а также о работе приложения в целом сохраняется в журнале событий Kaspersky Security Center и в журнал операционной системы (syslog).

Критическое

Нарушена целостность системы

Статус	!
Компонент	Контроль целостности системы
Идентификатор события Linux	0
Идентификатор события Kaspersky Security Center	`GNRL_EV_FIM_ALARM`
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запуск приложения запрещен

Статус	!
Компонент	Контроль приложений
Идентификатор события Linux	122
Идентификатор события Kaspersky Security Center	`GNRL_EV_APPLICATION_LAUNCH_DENIED`
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружен вредоносный объект (локальные базы)

Статус	!
Компонент	Защита от файловых угроз Защита от почтовых угроз Анализ поведения Защита от эксплойтов Sandbox
Идентификатор события Linux	6
Идентификатор события Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Превышено ограничение на количество отправленных событий Контроля целостности системы

Статус	!
Компонент	Контроль целостности системы
Идентификатор события Linux	70
Идентификатор события Kaspersky Security Center	`GNRL_EV_FIM_ALARM_OVERFLOW`
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Операция с устройством запрещена

Статус	!
Компонент	Контроль устройств
Идентификатор события Linux	94
Идентификатор события Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Обнаружена сетевая атака

Статус	!
Компонент	Защита от сетевых угроз
Идентификатор события Linux	102
Идентификатор события Kaspersky Security Center	GNRL_EV_ATTACK_DETECTED
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Доступ запрещен (локальные базы)

Статус	!
Компонент	Веб-Контроль
Идентификатор события Linux	190
Идентификатор события Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Предупреждение

Лечение невозможно

Статус	⚠
Компонент	Защита от файловых угроз Защита от почтовых угроз
Идентификатор события Linux	10
Идентификатор события Kaspersky Security Center	GNRL_EV_OBJECT_NOTCURED
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Предупреждение о нежелательном содержимом (локальные базы)

Статус	⚠
Компонент	Веб-Контроль
Идентификатор события Linux	192
Идентификатор события Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING

Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Сообщение администратору о запрете доступа к веб-странице

Статус	⚠
Компонент	Веб-Контроль
Идентификатор события Linux	196
Идентификатор события Kaspersky Security Center	`GNRL_EV_WC_USER_REQUEST`
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Информационное сообщение

Объект вылечен

Статус	ⓘ
Компонент	Защита от файловых угроз Защита от почтовых угроз
Идентификатор события Linux	9
Идентификатор события Kaspersky Security Center	`GNRL_EV_OBJECT_CURED`
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Объект удален

Статус	ⓘ
Компонент	Защита от файловых угроз Защита от почтовых угроз
Идентификатор события Linux	8
Идентификатор события Kaspersky Security Center	`GNRL_EV_OBJECT_DELETED`
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запуск приложения разрешен

Статус	ⓘ
Компонент	Контроль приложений
Идентификатор события Linux	120
Идентификатор события Kaspersky Security Center	`GNRL_EV_APPLICATION_LAUNCHED`
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center	не настраивается

Запуск приложения разрешен в тестовом режиме

Статус	ⓘ
Компонент	Контроль приложений
Идентификатор события Linux	121
Идентификатор события Kaspersky Security Center	`GNRL_EV_APP_LAUNCH_TESTED_ALLOW`
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Запуск приложения запрещен в тестовом режиме

Статус	ⓘ
Компонент	Контроль приложений
Идентификатор события Linux	123
Идентификатор события Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Устройство подключено

Статус	ⓘ
Компонент	Контроль устройств
Идентификатор события Linux	90
Идентификатор события Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_PLUGGED`
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Устройство отключено

Статус	ⓘ
Компонент	Контроль устройств
Идентификатор события Linux	91
Идентификатор события Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_UNPLUGGED`
Журнал (syslog) (по умолчанию)	–
Журнал событий Kaspersky Security Center (по умолчанию)	✓

Приложение 7. Коды возврата

Коды возврата мастера первоначальной настройки приложения

0 – Установка успешно завершена.

Критические ошибки

1 – Неизвестная ошибка (все остальные критические ошибки, кроме перечисленных ниже, например: системные ошибки, нехватка памяти, ошибка открытия файлов и другие).

2 – Конфигурационный файл первоначальной настройки содержит некорректные параметры.

3 – Не удалось установить или обновить приложение.

4 – Не удалось удалить приложение.

5 – Не удалось запустить приложение. Возможная причина: неправильная настройка прав доступа. Проверьте, что только учетная запись root имеет право на запись в директориях /, /opt, /opt/kaspersky, /var, /var/opt, /var/opt/kaspersky, /usr, /usr/lib64.

6 – Не выполнены необходимые действия перед установкой.

7 – Не удалось обновить приложение. Обновление приложения до более ранней версии не поддерживается.

8 – Не удалось удалить пользователей из привилегированных групп.

9 – Не удалось создать уникальный идентификатор MachineID для установки приложения.

10 – Не удалось запустить или перезапустить приложение.

11 – Не приняты условия Лицензионного соглашения и Политики конфиденциальности.

12 – Приложение не может одновременно использоваться в режиме Легкого агента и в режиме EDR-агента.

13 – Не найден пакет astra-digsig-oldkeys для режима ЗПС в ОС Астра.

14 – Первоначальная настройка уже запущена.

15 – Требуется удалить компонент Легкий агент для Linux, установленный в составе решения Kaspersky Security для виртуальных сред 5.2 Легкий агент.

16 – Требуется установить Агент администрирования Kaspersky Security Center.

17 – Не удалось запустить мастер первоначальной настройки в связи с уже имеющимся активным процессом приложения.

18 – Технология fanotify не поддерживается. Не удалось скомпилировать модуль ядра для защиты от файловых угроз.

19 – Для установки требуются права администратора.

20 – Служба приложения не запущена.

21 – Выполнен откат обновления приложения.

22 – Не поддерживается интеграция приложения в режиме EDR-агента или Легкого агента с решением Kaspersky Endpoint Detection and Response Expert (cloud).

Предупреждения

71 – Во время установки получено несколько предупреждений. Подробнее см. в журнале установки.

72 – Не удалось обновить базы приложения.

75 – Требуется перезагрузка операционной системы.

76 – Не удалось применить параметры использования KSN или не приняты условия Положения о KSN.

77 – Не удалось запустить обновляемый модуль ядра.

79 – Не удалось установить или обновить пакет графического интерфейса приложения.

80 – Не удалось скачать базы приложения.

81 – Активация приложения завершилась с ошибкой из-за сетевых проблем.

82 – Приложение работает под управлением политики.

83 – Запуск графического интерфейса приложения не выполнен.

84 – Не удалось назначить роль администратора. Указанный пользователь не найден.

85 – Пакет приложения удалось установить или обновить только в режиме игнорирования ошибок менеджера пакетов.

86 – Не удалось удалить пакет графического интерфейса приложения.

87 – Пакет приложения удалось удалить только в режиме игнорирования ошибок менеджера пакетов.

88 – Не удалось назначить пользователю роль администратора.

89 – Недействительный лицензионный ключ.

90 – Не удалось установить расписание для задачи обновления.

Коды возврата консольной утилиты kesl-control

0 – Команда/задача выполнена успешно.

1 – Общая ошибка в синтаксисе команды.

2 – Ошибка в переданных параметрах приложения.

64 – Приложение Kaspersky Endpoint Security не запущено.

66 – Базы приложения не загружены (используется только командой `kesl-control --app-info`).

67 – Активация приложения завершилась с ошибкой из-за сетевых проблем.

68 – Выполнение команды невозможно, так как приложение работает под управлением политики.

69 – Приложение находится в инфраструктуре Amazon Paid Ami.

70 – Попытка запуска уже запущенной задачи, удаления запущенной задачи, изменения параметров запущенной задачи, остановки остановленной задачи, приостановки приостановленной задачи или возобновления выполняющейся задачи.

71 – Не приняты условия Положения о Kaspersky Security Network.

72 – При выполнении задачи Выборочная проверка или Выборочная проверка контейнеров обнаружены угрозы.

73 – Попытка задать параметры задачи Контроль приложений, влияющие на работу приложения, без их подтверждения с помощью ключа `--accept`.

74 – Требуется перезапуск приложения Kaspersky Endpoint Security после обновления.

75 – Требуется перезагрузка устройства.

76 – Соединение запрещено, так как только пользователи с правами root должны иметь права на запись по указанному пути.

77 – Указанный лицензионный ключ уже используется на устройстве.

78 – Команда/задача не может быть выполнена, так как приложение используется в режиме Легкого агента.

79 – Команда не может быть выполнена, так как приложение используется в стандартном режиме.

80 – Операция скачивания обновлений завершилась с ошибкой из-за сетевых проблем.

81 – Компонент не поддерживается в той версии операционной системы, которая установлена на устройстве.

128 – Неизвестная ошибка.

65 – все остальные ошибки.

Приложение 8. Подготовка архива с базами приложения

Создавая вручную инсталляционный пакет Kaspersky Endpoint Security, вы можете добавить в него предварительно скачанные базы приложения. Если для установки используется инсталляционный пакет с интегрированными базами, приложение устанавливается с рабочими базами, и обновлять базы сразу после установки не требуется.

Добавление баз приложения в инсталляционный пакет увеличивает размер пакета.

Для каждого типа архитектуры и разрядности операционной системы на ваших защищаемых устройствах требуется отдельный набор баз приложения. Вы можете поместить в инсталляционный пакет архив, содержащих один или несколько наборов баз приложения. Для подготовки каждого набора баз приложения вам понадобится экземпляр уже установленного приложения Kaspersky Endpoint Security на устройстве с соответствующим типом архитектуры и разрядности операционной системы.

Чтобы подготовить архив с базами:

1. Выполните установку и первоначальную настройку приложения Kaspersky Endpoint Security на устройстве с помощью Kaspersky Security Center или с помощью командной строки.

2. Обновите базы приложения на устройстве. Вы можете обновить базы в ходе первоначальной настройки приложения или после установки, запустив задачу типа *Update* в командной строке или задачу *Обновление* в Kaspersky Security Center.

3. Создайте директорую для баз в зависимости от архитектуры и разрядности операционной системы на защищаемом устройстве:

   - x86_64 – если приложение установлено на 64-битной операционной системе;
   - i386 – если приложение установлено на 32-битной операционной системе;
   - arm64 – если приложение установлено на 64-битной операционной системе для архитектуры Arm;
   - e2k – если приложение установлено на 64-битной операционной системе для архитектуры Эльбрус.

4. Скопируйте содержимое директории /var/opt/kaspersky/kesl/private/updates/ в созданную директорию для баз.

5. Поместите созданную директорию с базами в архив kesl-bases.tgz.

   Если вы планируете создать инсталляционный пакет для установки на несколько операционных систем с разной архитектурой и разрядностью, вам нужно подготовить несколько директорий с базами и поместить их в архив kesl-bases.tgz.

По умолчанию после установки приложения Kaspersky Endpoint Security запускается задача обновления баз. Если вы устанавливаете приложение из инсталляционного пакета с интегрированными базами, выключите запуск задачи обновления баз после установки приложения. Вы можете настроить этот параметр в свойствах созданного инсталляционного пакета или в конфигурационном файле autoinstall.ini (`UPDATE_EXECUTE=No`).

Приложение 9. Требования к IOC-файлам

При создании задач поиска IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- Приложение поддерживает IOC-файлы с расширением .IOC и .XML открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.
- Семантические ошибки и неподдерживаемые IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов приложение фиксирует отсутствие совпадения.
- Идентификаторы всех IOC-файлов, которые используются в одной задаче поиска IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи *Поиск IOC*.

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC.

ЗАГРУЗИТЬ ФАЙЛ IOC TERMS.XLSX

Особенности и ограничения поддержки стандарта OpenIOC приложением приведены в таблице ниже.

Особенности и ограничения поддержки стандарта OpenIOC версий 1.0 и 1.1

Поддерживаемые условия	OpenIOC 1.0: • `is` • `isnot` (как исключение из множества) • `contains` • `containsnot` (как исключение из множества) OpenIOC 1.1: • `is` • `contains` • `starts-with` • `ends-with` • `matches` • `greater-than` • `less-than`
Поддерживаемые атрибуты условий	OpenIOC 1.1: • `preserve-case` • `negate`
Поддерживаемые операторы	`AND` `OR`
Поддерживаемые типы данных	`"date"`: дата (применимые условия: `is`, `greater-than`, `less-than`) `"int"`: целое число (применимые условия: `is`, `greater-than`, `less-than`) `"string"`: строка (применимые условия: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: продолжительность в секундах (применимые условия: `is`, `greater-than`, `less-than`)

Особенности интерпретации типов данных	Типы данных `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` интерпретируются как строка (string).
	Приложение поддерживает интерпретацию параметра `Content` для типов данных `int` и `date`, заданного в виде промежутков:
	• OpenIOC 1.0:
	С использованием оператора `TO` в поле `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	• OpenIOC 1.1:
	• С помощью условий `greater-than` и `less-than`
	• С использованием оператора `TO` в поле `Content`
	Приложение поддерживает интерпретацию типов данных `date` и `duration`, если индикаторы заданы в формате `ISO 8601, Zulu time zone, UTC`.

Юридическая информация

Предоставление данных

Этот раздел содержит информацию о данных, которые приложение Kaspersky Endpoint Security может сохранять на устройстве и передавать в автоматическом режиме в "Лабораторию Касперского" в ходе своей работы.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Более подробная информация об обработке, хранении и уничтожении информации, полученной во время использования приложения и переданной в "Лабораторию Касперского", приведена в Лицензионном соглашении, Положении о Kaspersky Security Network и Политике конфиденциальности на веб-сайте "Лаборатории Касперского". Файлы license.<идентификатор языка> и ksn_license.<идентификатор языка> с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки приложения.

Данные, предоставляемые при использовании кода активации

Если приложение Kaspersky Endpoint Security используется в стандартном режиме или в режиме EDR-Агента и было активировано с использованием кода активации, с целью проверки законности использования приложения и получения статистической информации о распространении и использовании приложения вы соглашаетесь предоставлять в "Лабораторию Касперского" в автоматическом режиме следующую информацию:

- тип, версию и локализацию установленного приложения;
- версии установленных обновлений приложения;
- идентификатор устройства и идентификатор установки приложения на устройстве;
- код активации, с помощью которого активировано приложение;
- идентификатор действующей лицензии;
- дату и время создания лицензионного ключа приложения;
- дату и время на устройстве пользователя;
- дату и время окончания срока действия лицензии на использование приложения;
- тип, версию и разрядность операционной системы.

Данные, предоставляемые при загрузке обновлений с серверов обновлений "Лаборатории Касперского"

Если приложение Kaspersky Endpoint Security используется в стандартном режиме или в режиме EDR-Агента и вы используете серверы обновлений "Лаборатории Касперского" для загрузки обновлений, с целью повышения эффективности процедуры обновления и для получения статистической информации о распространении и использовании приложения, вы соглашаетесь предоставлять в "Лабораторию Касперского" в автоматическом режиме следующую информацию:

- идентификатор приложения, полученный из лицензии;
- полную версию приложения;
- идентификатор лицензии приложения;
- тип используемой лицензии;
- идентификатор установки приложения (PCID);
- идентификатор запуска обновления приложения;
- обрабатываемый веб-адрес.

Данные, передаваемые при использовании приложения в режиме Легкого агента

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент, во время работы приложение сохраняет и передает другим компонентам решения следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Для активации приложение Kaspersky Endpoint Security передает Серверу защиты следующие данные: срок действия подтверждения статуса лицензионного ключа, идентификатор (BIOS ID) защищенной виртуальной машины, информацию о лицензии, необходимой Легкому агенту для работы.
- Для обновления баз Легкого агента приложение Kaspersky Endpoint Security передает Серверу защиты следующие данные: идентификатор ПО, полученный из лицензии; полную версию ПО; идентификатор лицензии ПО; идентификатор установки ПО (PCID); обрабатываемый веб-адрес; тип лицензии; идентификатор запуска обновления.
- Для обеспечения защиты и в ходе выполнения задач проверки приложение Kaspersky Endpoint Security передает Серверу защиты информацию, необходимую для выполнения проверки объектов. В том числе могут передаваться имена файлов и пути к ним в файловой системе, хеши файлов, веб-адреса, а также проверяемые объекты или их фрагменты.
- В инфраструктуре под управлением VMware vCenter Server и VMware NSX Manager приложение Kaspersky Endpoint Security может передавать Серверу интеграции информацию о тегах безопасности (Security Tags), которые назначаются защищенной виртуальной машине при обнаружении вирусов, вредоносных программ и активности, характерной для сетевых атак. В том числе передаются идентификаторы защищенных виртуальных машин.

- Для получения информации, которая используется при выборе SVM для подключения, приложение Kaspersky Endpoint Security передает идентификатор защищенной виртуальной машины Серверу интеграции и Серверу защиты.

- При использовании решения Kaspersky Security для виртуальных сред Легкий агент в режиме мультитенантности информация, необходимая для формирования отчетов о защите тенантов, может передаваться от приложения Kaspersky Endpoint Security Серверу защиты. В том числе могут передаваться: идентификатор защищенной виртуальной машины; тип и версия гостевой операционной системы на защищенной виртуальной машине; периоды времени, когда приложение Kaspersky Endpoint Security было подключено к SVM.

- Для получения статистики приложение Kaspersky Endpoint Security передает Серверу защиты следующую информацию: информацию о версии ОС защищенной виртуальной машины; локализацию приложения Kaspersky Endpoint Security; названия активных компонентов приложения Kaspersky Endpoint Security; идентификатор (BIOS ID) защищенной виртуальной машины.

Указанная информация, кроме информации, необходимой для выполнения проверки объектов, и информации, которая используется при выборе SVM, передается по зашифрованным каналам передачи данных. Соединение между приложением Kaspersky Endpoint Security и Серверами защиты по умолчанию не защищено. Вы можете включить шифрование канала передачи данных между Легкими агентами и Серверами защиты в параметрах приложения Kaspersky Endpoint Security.

Данные, передаваемые приложению Kaspersky Security Center

Во время работы приложение Kaspersky Endpoint Security сохраняет и передает приложению Kaspersky Security Center следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Информацию о базах, используемых в приложении:
  - список категорий баз, необходимых приложению;
  - дату и время выпуска и загрузки используемых баз в приложение;
  - дату выпуска загруженных обновлений баз приложения;
  - время последнего обновления баз приложения;
  - количество записей в текущих используемых базах приложения.
- Информацию о лицензии на использование приложения:
  - серийный номер и тип лицензии;
  - срок действия лицензии в днях;
  - количество устройств, на которые распространяется лицензия;
  - даты начала и окончания срока действия лицензии;
  - статус лицензионного ключа;
  - дату и время последней удачной синхронизации с серверами активации в случае, если приложение активировано с помощью кода активации;

- идентификатор приложения, для активации которого предоставлена лицензия;
- доступную по лицензии функциональность;
- название организации, которой предоставлена лицензия;
- дополнительную информацию в случае использования приложения по подписке (признак подписки, дату истечения периода подписки и количество дней, доступных для продления подписки, веб-адрес провайдера подписки, текущий статус и причину перехода в этот статус), дату и время активации приложения на устройстве;
- дату и время окончания срока действия лицензии на устройстве.

- Информацию об обновлениях приложения:
  - список обновлений, которые требуется установить или удалить;
  - дату выпуска обновления и наличие статуса *Критическое*;
  - название, версию и краткое описание обновления;
  - ссылку на статью с полным описанием обновления;
  - идентификатор и текст Лицензионного соглашения и Политики конфиденциальности для обновления приложения;
  - идентификатор и текст Положения о Kaspersky Security Network для обновления приложения;
  - признак возможности удаления обновления;
  - версии политики и плагина управления приложения;
  - веб-адрес для загрузки плагина управления приложения;
  - названия установленных обновлений приложения, версии и даты их установки;
  - код и описание ошибки, если установка или удаление обновления завершились с ошибкой;
  - признак и причину необходимости перезагрузки устройства или приложения по причине обновления приложения.
- Согласие или несогласие пользователя с условиями Положения о Kaspersky Security Network, Лицензионного соглашения и Политики конфиденциальности.
- Список тегов, назначенных устройству.
- Список статусов устройства и причины их назначения.
- Общий статус приложения и статус всех его компонентов; информацию о соответствии политике, статус постоянной защиты устройства, статус стабильности работы приложения, информация об остановке приложения.
- Дату и время последней проверки устройства; количество проверенных объектов; количество обнаруженных вредоносных объектов; количество заблокированных, удаленных и вылеченных объектов; количество объектов, которые не удалось вылечить; количество ошибок проверки; количество обнаруженных сетевых атак.

- Данные о текущих примененных значениях параметров приложения.
- Текущий статус и результат выполнения групповых и локальных задач и значения их параметров.
- Информацию о внешних устройствах, подключенных к клиентскому устройству (идентификатор, имя, тип, производитель, описание, серийный номер и VID/PID).
- Информацию о резервных копиях файлов, помещенных в резервное хранилище (имя, путь, размер и тип объекта, описание объекта, имя обнаруженной угрозы, версию баз приложения, с помощью которых была обнаружена угроза, дату и время помещения объекта в резервное хранилище, действия над объектом в резервном хранилище (удален, восстановлен)), а также сами файлы по запросу администратора.
- Информацию о работе каждого компонента приложения и о выполнении каждой задачи в виде событий:
  - дату и время возникновения события;
  - название и тип события;
  - уровень важности события;
  - название задачи или компонента приложения, во время работы которых произошло событие;
  - информацию о приложении, которое вызвало событие: название приложения, путь к файлу на диске, идентификатор процесса, значения параметров в случае публикации события о запуске или изменении параметров работы приложения;
  - идентификатор пользователя;
  - имя инициатора (планировщика задач, или приложения, или Kaspersky Security Center, или имя пользователя), действия которого привели к возникновению события;
  - имя и идентификатор пользователя, инициировавшего доступ к файлу;
  - результат обработки объекта или действия (описание, тип, название, уровень угрозы и точность, имя файла и тип операции над устройством, решение приложения по этой операции);
  - информацию об объекте (имя и тип объекта, путь к объекту на диске, версия объекта, размер, информация о выполненном действии, описание причины возникновения события, описание причины необработки и пропуска объекта);
  - информацию об устройстве (имя производителя, имя устройства, путь, тип устройства, тип шины, идентификатор, VID/PID, признак системного устройства, название расписания правила доступа к устройству);
  - информацию о блокировке и разблокировке устройства; информацию о заблокированных подключениях (название, описание, имя устройства, протокол, удаленный адрес и порт, локальный адрес и порт, пакетные правила, действия);
  - информацию о запрошенном веб-адресе;
  - информацию об обнаруженных объектах;
  - тип, метод и идентификатор обнаружения;
  - информацию о выполненном действии;

- информацию о базах приложения (дату выпуска загруженных обновлений баз, информацию о применении баз, ошибки применения баз, информацию об отмене установленных обновлений баз);
- информацию об обнаружении шифрования (имя шифровальщика; имя устройства, на котором обнаружено шифрование; информацию о блокировке и разблокировке устройства);
- параметры приложения и сетевые параметры;
- информацию о сработавшем правиле Контроля приложений (имя и тип) и результат применения правила;
- информацию о контейнерах и образах контейнеров (имена контейнеров или образов контейнеров, пути к контейнерам или образам контейнеров, веб-адрес репозитория);
- информацию об активных и заблокированных подключениях (название, описание и тип);
- информацию о блокировке и разблокировке доступа к недоверенным устройствам;
- информацию об использовании KSN (статус подключения к KSN, инфраструктура KSN, идентификатор Положения о KSN в расширенном режиме, принятие Положения о KSN в расширенном режиме, идентификатор Положения о KSN, принятие Положения о KSN);
- информацию о сертификатах (доменное имя, название субъекта, название издателя, дату окончания срока действия, статус сертификата, тип сертификата, время добавления сертификата, дату выпуска, серийный номер, отпечаток SHA256);
- информацию о внешних системах, входящих в состав корпоративных программных решений (адрес сервера интеграции);
- информацию о включении и выключении сетевой изоляции для устройства;
- информацию о работе в режиме Легкого агента: имя шаблона виртуальной машины, адрес Сервера интеграции;
- имя устройства, для которого включена или выключена сетевая изоляция;
- статистику выполнения задачи проверки: количество проверенных объектов; количество найденных угроз; количество зараженных объектов; количество возможно зараженных объектов; количество вылеченных объектов; количество объектов, добавленных в резервное хранилище; количество удаленных объектов; количество невылеченных объектов; количество ошибок проверки; количество объектов, защищенных паролем; количество пропущенных объектов; количество проверенных контейнеров и образов;
- информацию о версии компонента EDR Optimum, используемого в приложении;
- информацию о цепочках развития угрозы: имя сетевого списка цепочек развития угрозы, идентификатор цепочки развития угрозы.

- Информацию о работе задачи проверки целостности системы (имя, тип, путь) и информацию о снимке состояния системы.
- Информацию о сетевой активности, о пакетных правилах и о сетевых атаках.

- Информацию о роли пользователя:
  - имя и идентификатор пользователя, инициировавшего изменение роли пользователя;
  - роль пользователя;
  - имя пользователя, которому назначена или у которого отозвана роль.
- Информацию об исполняемых файлах приложений, обнаруженных на клиентском устройстве (имя, путь, тип и хеш файла; список категорий, к которым отнесено приложение; KL-категория, к которой отнесено приложение; группу доверия, к которой отнесено приложение; первое время запуска файла; название и версию приложения; название производителя приложения; информацию о сертификате, которым подписано приложение: серийный номер, отпечаток, издатель, субъект, дату выпуска, дату окончания действия и открытый ключ).
- Информацию о сетевом списке цепочек развития угрозы: идентификатор цепочки развития угрозы, время создания цепочки развития угрозы в виде метки времени, формат цепочки развития угрозы (текст или архив), размер тела цепочки развития угрозы в байтах.

Данные, предоставляемые при переходе по ссылкам из интерфейса приложения

При переходе по ссылкам из интерфейса приложения Kaspersky Endpoint Security вы соглашаетесь предоставлять в "Лабораторию Касперского" в автоматическом режиме следующую информацию:

- полную версию приложения;
- локализацию приложения;
- идентификатор приложения (PID);
- имя ссылки.

Данные, предоставляемые при использовании Kaspersky Security Network

Набор данных, которые Kaspersky Security Network передает в "Лабораторию Касперского", зависит от режима использования Kaspersky Security Network.

Файл ksn_license.<ID языка> с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения.

Предоставление данных при использовании KSN в стандартном режиме

Если вы используете Kaspersky Security Network в стандартном режиме (в веб-консоли включен переключатель **Использование Kaspersky Security Network (KSN)** и снят флажок **Использовать расширенный режим KSN**, в Консоли администрирования выбран вариант **Стандартный режим KSN**) принимая условия Положении о Kaspersky Security Network, вы соглашаетесь предоставлять в "Лабораторию Касперского" в автоматическом режиме следующую информацию.

Предоставление данных при использовании KSN в расширенном режиме

Если вы используете Kaspersky Security Network в расширенном режиме (в веб-консоли включен переключатель **Использование Kaspersky Security Network (KSN)** и установлен флажок **Использовать расширенный режим KSN**, в Консоли администрирования выбран вариант **Расширенный режим KSN**), принимая условия Положении о Kaspersky Security Network, вы соглашаетесь предоставлять в "Лабораторию Касперского" в автоматическом режиме дополнительно к перечисленному выше следующую информацию.

Предоставление данных при использовании KSN в расширенном режиме при интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises)

Если вы используете Kaspersky Endpoint Security как часть решения Kaspersky Endpoint Detection and Response Expert (on-premises) и используете Kaspersky Security Network в расширенном режиме, принимая условия Положении о Kaspersky Security Network, вы соглашаетесь предоставлять в "Лабораторию Касперского" в автоматическом режиме дополнительно к перечисленному выше следующую информацию.

Предоставление данных при использовании Kaspersky Endpoint Security в стандартном режиме и режиме Агента Endpoint Detection and Response

Если вы используете Kaspersky Endpoint Security в стандартном режиме или режиме Агента Endpoint Detection and Response и используете Kaspersky Security Network в расширенном режиме, принимая условия Положении о Kaspersky Security Network, вы соглашаетесь предоставлять в "Лабораторию Касперского" в автоматическом режиме дополнительно к перечисленному выше следующую информацию.

Данные, предоставляемые при интеграции с решением Kaspersky Endpoint Detection and Response Optimum

Данные, передаваемые вместе с результатами выполнения задач *Поиск IOC*

Kaspersky Endpoint Security автоматически передает данные о результатах выполнения задач *Поиск IOC* в Kaspersky Security Center.

Данные о результатах выполнения задач *Поиск IOC* могут содержать следующую информацию:

- Сетевую информацию:
  - IP-адрес из таблицы протокола разрешения адресов (Address Resolution Protocol, ARP);
  - MAC-адрес из таблицы протокола разрешения адресов;
  - тип и имя записи DNS;
  - IP-адрес защищаемого устройства;
  - MAC-адрес защищаемого устройства;
  - IP-адрес удаленного соединения и порт;
  - IP-адрес локального сетевого адаптера;
  - номер порта, открытого на локальном адаптере;
  - номер протокола согласно стандарту Internet Assigned Numbers Authority (IANA).
- Информацию о процессах:
  - имя процесса;
  - аргументы процесса;
  - путь к исполняемому файлу процесса;
  - идентификатор процесса (PID);
  - идентификатор родительского процесса (PPID);
  - имя пользователя, запустившего процесс;
  - дату и время запуска процесса.
- Информацию о службах:
  - имя службы;
  - описание службы;
  - путь и имя исполняемого файла службы;
  - идентификатор службы;
  - тип службы (драйвер ядра, адаптер и т.д.);
  - статус службы;
  - режим запуска службы;
  - имя пользователя, под которым запущена служба.

- Информацию о файловой системе:
  - имя тома;
  - букву тома;
  - тип тома.
- Информацию об операционной системе:
  - имя и версию операционной системы;
  - сетевое имя защищаемого устройства;
  - домен или группу, к которым принадлежит устройство.
- Информацию о веб-активности:
  - имя браузера;
  - версию браузера;
  - время последнего обращения к веб-ресурсу;
  - веб-адрес HTTP-запроса;
  - имя пользователя, выполнившего HTTP-запрос;
  - имя процесса, выполнившего HTTP-запрос;
  - путь к исполняемому файлу процесса, выполнившего HTTP-запрос;
  - идентификатор процесса, выполнившего HTTP-запрос;
  - веб-адрес источника HTTP-запроса;
  - веб-адрес запрошенного ресурса;
  - агент пользователя обрабатываемого веб-запроса (HTTP User-Agent);
  - время выполнения HTTP-запроса;
  - уникальный идентификатор процесса, выполнившего HTTP-запрос.

Данные для построения цепочки развития угрозы

Данные для построения цепочки развития угрозы могут содержать следующую информацию:

- Общую информацию об алерте:
  - дату и время алерта;
  - имя объекта;
  - режим проверки;
  - статус последнего действия, связанного с алертом;
  - причину неудачной обработки алерта.
- Информацию об обрабатываемом объекте:
  - идентификатор процесса;
  - идентификатор родительского процесса;
  - идентификатор файла процесса;
  - командную строку процесса;
  - имя пользователя, запустившего процесс;
  - идентификатор сеанса, в котором запущен процесс;
  - тип сеанса, в котором запущен процесс;
  - уровень целостности обрабатываемого процесса;
  - принадлежность пользователя к привилегированным группам;
  - идентификатор обрабатываемого объекта;
  - полное имя обрабатываемого объекта;
  - идентификатор защищаемого устройства;
  - полное имя объекта (локальный файл или веб-адрес);
  - хеш-суммы MD5 и SHA256 обрабатываемого объекта;
  - тип обрабатываемого объекта;
  - дату создания и последнего изменения объекта;
  - размер обрабатываемого объекта;
  - атрибуты обрабатываемого объекта;

- информацию об организации, подписавшей объект;
- результат проверки цифрового сертификата объекта;
- идентификатор безопасности (SID) объекта;
- идентификатор часового пояса объекта;
- веб-адрес загрузки объекта (только для файлов);
- название приложения, загрузившего файл;
- хеш-суммы MD5 и SHA256 приложения, загрузившего файл;
- название приложения, последний раз изменившего файл;
- хеш-суммы MD5 и SHA256 приложения, последний раз изменившего файл;
- количество запусков обрабатываемого объекта;
- дату и время первого запуска объекта;
- уникальный идентификатор файла;
- полное имя файла (локальный файл или веб-адрес);
- веб-адрес обрабатываемого веб-запроса;
- источник ссылок обрабатываемого веб-запроса (HTTP referer);
- агент пользователя обрабатываемого веб-запроса;
- тип обрабатываемого веб-запроса (GET или POST);
- локальный IP-порт для обрабатываемого веб-запроса;
- удаленный IP-порт для обрабатываемого веб-запроса;
- направление соединения (входящее или исходящее) обрабатываемого веб-запроса;
- идентификатор процесса, в который произошло внедрение вредоносного кода.

Данные, предоставляемые при интеграции с компонентом Kaspersky Endpoint Detection and Response (KATA)

При интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA) – компонентом решения Kaspersky Anti Targeted Attack Platform – приложение Kaspersky Endpoint Security сохраняет следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Адреса серверов с компонентом Central Node, обеспечивающих взаимодействие с Kaspersky Endpoint Detection and Response (KATA) (далее также *серверы KATA*).
- Открытый ключ сертификата сервера для интеграции с Kaspersky Endpoint Detection and Response (KATA).

- Сертификат клиента для интеграции с Kaspersky Endpoint Detection and Response (KATA).
- Учетные данные для авторизации на прокси-сервере.
- Параметры частоты синхронизации с сервером KATA и параметры передачи данных на сервер KATA.
- Статус соединения с сервером KATA и сведения об ошибках сертификата клиента и сертификата сервера.
- Параметры задач, поступающих от серверов KATA:
  - Параметры расписания запуска задач.
  - Имена и пароли учетных записей, под которыми требуется запускать задачи.
  - Версии параметров.
  - Тип запуска служб.
  - Названия служб.
  - Командную строку запуска процесса с аргументами.
  - MD5 и SHA256-хеши объектов.
  - Пути к объектам.
  - IOC-файлы.
- Параметры изоляции, в соответствии с которыми устройству будет запрещено осуществлять соединение с другими устройствами, кроме указанных в исключениях.

При интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response (KATA) приложение Kaspersky Endpoint Security сохраняет и может передавать серверу KATA следующие данные:

- Данные из запросов на синхронизацию к компоненту EDR Expert (on-premise):
  - Уникальный идентификатор.
  - Базовую часть веб-адреса сервера.
  - Имя устройства.
  - IP-адрес устройства.
  - MAC-адрес устройства.
  - Локальное время на устройстве.
  - Название и версию операционной системы, установленной на устройстве.
  - Версию Kaspersky Endpoint Security.
  - Дату выпуска используемых баз приложения.
  - Статус лицензионного ключа.

- Данные из запросов к компоненту EDR Expert (on-premise) в отчетах о результатах выполнения задач:
  - IP-адрес устройства.
  - Уникальный идентификатор.
  - Базовую часть веб-адреса сервера.
  - MAC-адрес устройства.
  - Ошибки выполнения задач и коды возврата.
  - Статусы, с которыми завершались задачи.
  - Время завершения задач.
  - Версии параметров, с которыми выполнялись задачи.
  - Информацию о процессах, запущенных или остановленных на устройстве по запросу сервера: PID и UniquePID, код ошибки, хеш-суммы MD5 и SHA256 объектов.
  - Файлы, запрошенные сервером.
  - Данные об ошибках получения информации об объектах: полное имя объекта, при обработке которого возникла ошибка; код ошибки.
  - Статус применения сетевой изоляции.
  - Для индикаторов IOC возвращаются результаты поиска (сработал или не сработал каждый индикатор; найденные объекты и информация о том, какая ветка индикатора сработала).
  - Для объектов, вызвавших срабатывания индикаторов IOC, возвращаются разные значения в зависимости от типа индикаторов:
    - ArpEntry: IP-адрес из ARP-таблицы (в том числе ipv6), физический адрес из ARP-таблицы.
    - File: MD5-хеш файла, SHA-256-хеш файла, полное имя файла (включая путь), размер файла.
    - Port: удаленный IP-адрес и порт, с которым в момент проверки установлено соединение; IP-адрес и порт локального адаптера; тип протокола (TCP, UDP, IP, RAWIP).
    - Process: имя процесса; аргументы процесса; путь к файлу процесса; системный PID процесса; системный PID родительского процесса; имя пользователя, от имени которого запущен процесс; дата и время запуска процесса.
    - SystemInfo: имя ОС, версия ОС, сетевое имя устройства без домена, домен или рабочая группа.
    - User: имя пользователя.
  - Для объектов, помещенных на карантин:
    - Путь к файлу.
    - Размер файла.

    - Идентификатор файла, присвоенный ему при помещении на карантин.
    - Флаг об удалении оригинального файла.
  - Для файлов, полученных из карантина:
    - Идентификатор файла, присвоенный ему при помещении на карантин.
  - Для запрещенных запусков исполняемых файлов или скриптов:
    - Идентификатор процесса.
    - Идентификатор родительского процесса.
    - Системный идентификатор.
    - Идентификатор сеанса входа в систему.
    - Состояние процесса.
    - Дата и время перехвата запуска.
  - Для запрещенных открытий документов с помощью офисных приложений:
    - Идентификатор процесса.
    - Идентификатор файла.
    - Дата и время перехвата запуска.
- Данные о файлах:
  - Уникальный идентификатор файла.
  - MD5-хеш объекта.
  - Содержимое файла.
- Данные в пакетах телеметрии:
  - Данные о файлах:
    - Уникальный идентификатор файла.
    - Путь к файлу.
    - Имя файла.
    - Размер файла.
    - Атрибуты файла.
    - Дату и время создания файла.
    - Дату и время последнего изменения файла.

    - MD5 и SHA256-хеши объекта.
    - Информацию о пользователе и группе, владеющих файлом (имя и идентификатор).
- Данные о запущенных процессах:
    - Идентификатор файла процесса.
    - Идентификатор процесса.
    - Параметры запуска процесса.
    - Идентификатор сессии.
    - Дату и время запуска процесса.
    - Информацию о пользователе и группе, от имени которых запущен процесс (имя и идентификатор).
- Данные о процессе, получающем доступ к памяти другого процесса:
    - Идентификатор процесса.
    - Метод и адрес внедрения (injection).
    - Командную строку изменения процесса с аргументами.
    - Аргументы системного вызова процесса.
- Информацию об обнаруженных и обработанных угрозах:
    - Название обнаруженной угрозы и технологии, обнаружившей угрозу, согласно классификации "Лаборатории Касперского".
    - Версию баз приложения.
    - Веб-адрес, с которого был загружен зараженный объект.
    - Статус обработки угрозы.
    - Причину невозможности устранения угрозы.
    - Уникальный идентификатор файла угрозы.
- Данные об изменении файлов:
    - Уникальный идентификатор изменившегося файла.
    - Уникальный идентификатор процесса, совершившего изменения.
    - Информацию о произошедшем изменении.

- Данные об изменениях в системе:
  - Уникальный идентификатор процесса, совершившего изменения.
  - Информация о произошедшем изменении.
- Информацию о входе пользователя в систему:
  - Идентификатор сессии.
  - Информация о пользователе (имя и идентификатор).
  - IP адрес устройства, с которого установлена сессия.
- Данные о завершающихся процессах: уникальный идентификатор процесса.
- Информацию о загрузке библиотеки в адресное пространство процесса: идентификатор загруженной библиотеки.
- Информацию об установлении сетевого соединения:
  - Локальный IP-адрес.
  - Удаленный IP-адрес.
  - Направление соединения.
  - Протокол.
- Информация о процессе, который "прослушивает" внешние сетевые соединения на определенном порту:
  - Локальный адрес (порт и IP-адрес).
  - Протокол.
- Информация об обращении к DNS-серверу:
  - Доменное имя запрашиваемого ресурса.
  - IP-адреса запрашиваемого ресурса.
  - IP-адрес DNS-сервера.
  - Тип запроса.

Также указанная информация может сохраняться в файлах трассировки и файлах дампов.

Данные, предоставляемые при интеграции с компонентом Kaspersky Endpoint Detection and Response Expert (on-premises)

При интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (on-premises) приложение Kaspersky Endpoint Security сохраняет следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Адреса серверов, обеспечивающих интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises).
- Открытый ключ сертификата сервера, обеспечивающего интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises).
- Сертификат клиента для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premises).
- Учетные данные для авторизации на прокси-сервере.
- Параметры частоты синхронизации с сервером, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises), и параметры передачи данных на сервер.
- Статус соединения с сервером, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises), и сведения об ошибках сертификата клиента и сертификата сервера.
- Параметры задач, поступающих от серверов, обеспечивающих интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premises):
  - Параметры расписания запуска задач.
  - Имена и пароли учетных записей, под которыми требуется запускать задачи.
  - Версии параметров.
  - Тип запуска служб.
  - Названия служб.
  - Командную строку запуска процесса с аргументами.
  - MD5 и SHA256-хеши объектов.
  - Пути к объектам.
  - IOC-файлы.
- Параметры изоляции, в соответствии с которыми устройству будет запрещено осуществлять соединение с другими устройствами, кроме указанных в исключениях.

При интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Expert (on-premises) приложение сохраняет и может передавать серверу, обеспечивающему интеграцию, следующие данные:

- Данные из запросов на синхронизацию к компоненту EDR Expert (on-premises):
  - Уникальный идентификатор.
  - Базовую часть веб-адреса сервера.
  - Имя устройства.
  - IP-адрес устройства.
  - MAC-адрес устройства.
  - Локальное время на устройстве.
  - Название и версию операционной системы, установленной на устройстве.
  - Версию Kaspersky Endpoint Security.
  - Дату выпуска используемых баз приложения.
  - Статус лицензионного ключа.
- Данные из запросов к компоненту EDR Expert (on-premises) в отчетах о результатах выполнения задач:
  - IP-адрес устройства.
  - Уникальный идентификатор.
  - Базовую часть веб-адреса сервера.
  - MAC-адрес устройства.
  - Ошибки выполнения задач и коды возврата.
  - Статусы, с которыми завершались задачи.
  - Время завершения задач.
  - Версии параметров, с которыми выполнялись задачи.
  - Информацию о процессах, запущенных или остановленных на устройстве по запросу сервера: PID и UniquePID, код ошибки, хеш-суммы MD5 и SHA256 объектов.
  - Файлы, запрошенные сервером.
  - Данные об ошибках получения информации об объектах: полное имя объекта, при обработке которого возникла ошибка; код ошибки.
  - Статус применения сетевой изоляции.

- Для индикаторов IOC возвращаются результаты поиска (сработал или не сработал каждый индикатор; найденные объекты и информация о том, какая ветка индикатора сработала).
- Для правил YARA возвращаются результаты поиска (сработало или не сработало правило, найденные объекты и информация о том, какое правило сработало).
- Для объектов, вызвавших срабатывания индикаторов IoC, правил Yara, возвращаются разные значения в зависимости от типа:
  - ArpEntry: IP-адрес из ARP-таблицы (в том числе ipv6), физический адрес из ARP-таблицы.
  - File: MD5-хеш файла, SHA-256-хеш файла, полное имя файла (включая путь), размер файла.
  - Port: удаленный IP-адрес и порт, с которым в момент проверки установлено соединение; IP-адрес и порт локального адаптера; тип протокола (TCP, UDP, IP, RAWIP).
  - Process: имя процесса; аргументы процесса; путь к файлу процесса; системный PID процесса; системный PID родительского процесса; имя пользователя, от имени которого запущен процесс; дата и время запуска процесса.
  - SystemInfo: имя ОС, версия ОС, сетевое имя устройства без домена, домен или рабочая группа.
  - User: имя пользователя.
- Для объектов, помещенных на карантин:
  - Путь к файлу.
  - Размер файла.
  - Идентификаторы файла, присвоенные ему при помещении на карантин.
  - Флаг об удалении оригинального файла.
- Для файлов, полученных, восстановленных или удаленных из карантина:
  - Идентификаторы файла, присвоенные ему при помещении на карантин.
- Для запрещенных запусков исполняемых файлов или скриптов:
  - Идентификатор процесса.
  - Идентификатор родительского процесса.
  - Системный идентификатор.
  - Идентификатор сеанса входа в систему.
  - Состояние процесса.
  - Дата и время перехвата запуска.

- Для запрещенных открытий документов с помощью офисных приложений:
  - Идентификатор процесса.
  - Идентификатор файла.
  - Дата и время перехвата запуска.
- Перечень файлов в указанной директории:
  - Имя файла.
  - Абсолютный путь к файлу.
  - Размер файла.
  - Тип файла.
  - Имя и идентификатор владельца и группы владельца.
  - Права доступа к файлу.
  - Специальные флаги файловой системы, распространяемые на каждый файл.
  - Метаданные о файле.
  - Количество жестких ссылок на файл.
  - Время создания, изменения и последнего доступа к файлу.
- Перечень запущенных процессов на устройстве:
  - Имя процесса.
  - Время запуска процесса.
  - Статус процесса.
  - Идентификатор процесса (PID) и идентификатор родительского процесса.
  - Текущая рабочая директория процесса.
  - Параметры запуска процесса.
  - Переменные окружения.
  - Путь к исполняемому файлу процесса.
  - Идентификатор сессии пользователя, запустившего процесс.
  - Идентификатор пользователя и группы, запустивших процесс.
  - Идентификатор пользователя и группы, с правами которых процесс имеет доступ к файлам и ресурсам в системе.

- Перечень точек автозапуска:
    - Тип точки автозапуска.
    - Имя файла.
    - Абсолютный путь к файлу.
    - Права доступа к файлу.
    - Специальные флаги файловой системы, распространяемые на каждый файл.
    - Имя и идентификатор владельца и группы владельца.
    - Время создания, изменения и последнего доступа к файлу.
- Образ памяти процесса:
    - Имя процесса.
    - Полный путь к файлу процесса.
    - Файл дампа процесса.
    - Размер файла дампа процесса.
- Образ памяти устройства: файл дампа оперативной памяти устройства.
- Образ диска устройства.

- Данные о файлах:
    - Уникальный идентификатор файла.
    - MD5-хеш объекта.
    - Содержимое файла.
- Данные в пакетах телеметрии:
    - Данные о событиях телеметрии:
        - Идентификатор события.
        - Порядковый номер события в последовательности отправляемых пакетов телеметрии.
        - Тип события.
        - Время возникновения события.
    - Информацию о защищаемом устройстве:
        - Имя защищаемого устройства.
        - Идентификатор защищаемого устройства в Kaspersky Security Center.

    - Идентификатор защищаемого устройства в Kaspersky Endpoint Detection and Response Expert (on-premises).
    - Название, версию, семейство операционной системы, установленной на защищаемом устройстве.
    - Время запуска и выключения операционной системы, установленной на защищаемом устройстве.
- Данные о файлах:
    - Уникальный идентификатор файла.
    - Путь к файлу.
    - Имя файла.
    - Размер файла.
    - Атрибуты файла.
    - Дату и время создания файла.
    - Дату и время последнего изменения файла.
    - MD5 и SHA256-хеши объекта.
    - Информацию о пользователе и группе, владеющих файлом (имя и идентификатор).
- Данные о запущенных процессах:
    - Идентификатор файла процесса.
    - Идентификатор процесса.
    - Параметры запуска процесса.
    - Идентификатор сессии.
    - Дату и время запуска процесса.
    - Информацию о пользователе и группе, от имени которых запущен процесс (имя и идентификатор).
- Данные о процессе, получающем доступ к памяти другого процесса:
    - Идентификатор процесса.
    - Метод и адрес внедрения (injection).
    - Командную строку изменения процесса с аргументами.
    - Аргументы системного вызова процесса.

- Информацию об обнаруженных и обработанных угрозах:
  - Название обнаруженной угрозы и технологии, обнаружившей угрозу, согласно классификации "Лаборатории Касперского".
  - Дату выпуска и версию баз приложения.
  - Веб-адрес, с которого был загружен зараженный объект.
  - Статус обработки угрозы.
  - Причину невозможности устранения угрозы.
  - Уникальный идентификатор файла угрозы.
- Данные об изменении файлов:
  - Уникальный идентификатор изменившегося файла.
  - Уникальный идентификатор процесса, совершившего изменения.
  - Информацию о произошедшем изменении.
- Данные об изменениях в системе:
  - Уникальный идентификатор процесса, совершившего изменения.
  - Информация о произошедшем изменении.
- Информацию о входе пользователя в систему:
  - Идентификатор сессии.
  - Информация о пользователе (имя и идентификатор).
  - IP-адрес устройства, с которого установлена сессия.
- Данные о завершающихся процессах: уникальный идентификатор процесса.
- Информацию о загрузке библиотеки в адресное пространство процесса: идентификатор загруженной библиотеки.
- Информацию об установлении и завершении сетевого соединения:
  - Локальный IP-адрес.
  - Удаленный IP-адрес.
  - Направление соединения.
  - Протокол.
  - Время начала соединения.
  - Время завершения соединения.

    - Длительность соединения.
    - Количество отправленных байт за время соединения.
    - Количество полученных байт за время соединения.
- Информацию о процессе, который "прослушивает" внешние сетевые соединения на определенном порту:
    - Локальный адрес (порт и IP-адрес).
    - Протокол.
- Информацию об обращении к DNS-серверу:
    - Доменное имя запрашиваемого ресурса.
    - IP-адреса запрашиваемого ресурса.
    - IP-адрес DNS-сервера.
    - Тип запроса.
- Информацию о подключаемых внешних устройствах:
    - Тип операции (подключение устройства).
    - Тип устройства.
    - Уникальный идентификатор устройства.
    - Имя устройства.
    - Путь к устройству.
- Информация о приложении и о его модулях:
    - Версию приложения.
    - Время установки, запуска, остановки и удаления приложения.
    - Инициатор действия над приложением.
    - Причина остановки приложения в случае внештатной остановки.
    - Коды возврата в случае внештатной остановки.
- Информацию о взаимодействии с планировщиками задач (создание и удаление задач):
    - Имя задачи.
    - Путь к команде, которая выполняется по расписанию.
    - Расписание запуска задачи.

    - Имя учетной записи пользователя, создавшего задачу.
    - Имя учетной записи, от имени которой запускается задача.
    - Имя учетной записи пользователя, удалившего задачу.
- Информацию о создании, удалении и изменении службы:
    - Имя службы (в том числе предыдущее в случае изменения).
    - Тип службы (в том числе предыдущий в случае изменения).
    - Путь к исполняемому файлу (в том числе предыдущий в случае изменения).
    - Зависимости службы (в том числе предыдущие в случае изменения).
    - Имя учетной записи, от имени которой запускается служба (в том числе предыдущее в случае изменения).
    - Отображаемое имя службы (в том числе предыдущее в случае изменения).
    - Имя учетной записи пользователя, создавшего, удалившего или изменившего службу.
    - Признак отложенного удаления.
- Информацию о вводе в консоль:
    - Идентификатор и тип процесса, инициировавшего ввод в консоль.
    - Содержимое ввода в консоль.
- Информацию о смонтированных устройствах:
    - Системное имя тома.
    - Точка монтирования.
- Информацию об изменении в памяти процесса:
    - Аргументы системного вызова процесса.
    - Информацию о процессе, осуществившем внедрение кода, и о его родительском процессе.
        - Идентификатор процесса и уникальный идентификатор процесса и родительского процесса.
        - Командную строку, из которой был запущен процесс и родительский процесс.
        - Переменные окружения процесса.
        - Вид учетной записи пользователя, от имени которого был запущен процесс и родительский процесс.
        - Системный вызов, с помощью которого был создан процесс.
        - Идентификатор пользователя и группы, запустивших процесс.

    - Имя и полное имя процесса и родительского процесса.
    - Полный путь к процессу и родительскому процессу.
    - MD5 и SHA256-хеши процесса и родительского процесса.
    - Идентификатор сессии.
    - Имя, доменное имя и идентификатор пользователя, запустившего процесс и родительский процесс.
  - Информацию о процессе, через который был загружен процесс, осуществивший внедрение кода.
    - Уникальный идентификатор процесса, через который был загружен процесс.
    - Имя и полное имя файла, через который был загружен процесс.
    - Полный путь к процессу, через который был загружен процесс.
    - MD5-хеш процесса, через который был загружен процесс.
  - Информацию о процессе, являющемся инициатором процесса.
    - Идентификатор процесса и уникальный идентификатор процесса, являющегося инициатором процесса.
    - Командную строку процесса, являющегося инициатором процесса.
    - Имя и доменное имя пользователя, запустившего процесс, являющийся инициатором процесса.
    - Имя и полное имя процесса, являющегося инициатором процесса.
    - Полный путь к процессу, являющемуся инициатором процесса.
    - MD5 и SHA256-хеши процесса, являющегося инициатором процесса.

Также указанная информация может сохраняться в файлах трассировки и файлах дампов.

Данные, предоставляемые при интеграции с компонентом Kaspersky Endpoint Detection and Response Expert (cloud)

При интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (cloud) приложение Kaspersky Endpoint Security сохраняет следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Адреса серверов, обеспечивающих интеграцию с Kaspersky Endpoint Detection and Response Expert (cloud).
- Адреса туннелей серверов телеметрии и реагирования Kaspersky Endpoint Detection and Response Expert (cloud).

- Сертификат сервера, обеспечивающего интеграцию с Kaspersky Endpoint Detection and Response Expert (cloud).
- Сертификат клиента для интеграции с Kaspersky Endpoint Detection and Response Expert (cloud).
- Параметры частоты синхронизации с сервером, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (cloud), и параметры передачи данных на сервер.
- Статус соединения с сервером, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (cloud), и сведения об ошибках сертификата клиента и сертификата сервера.
- Параметры задач, поступающих от серверов, обеспечивающих интеграцию с Kaspersky Endpoint Detection and Response Expert (cloud):
  - Параметры расписания запуска задач.
  - Имена и пароли учетных записей, под которыми требуется запускать задачи.
  - Версии параметров.
  - Тип запуска служб.
  - Названия служб.
  - Командную строку запуска процесса с аргументами.
  - MD5 и SHA256-хеши объектов.
  - Пути к объектам.
  - IOC-файлы.
- Параметры изоляции, в соответствии с которыми устройству будет запрещено осуществлять соединение с другими устройствами, кроме указанных в исключениях.

При интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Expert (cloud) приложение сохраняет и может передавать серверу, обеспечивающему интеграцию, следующие данные:

- Данные из запросов на синхронизацию к компоненту EDR Expert (cloud):
  - Уникальный идентификатор.
  - Базовую часть веб-адреса сервера.
  - Имя устройства.
  - IP-адрес устройства.
  - MAC-адрес устройства.
  - Локальное время на устройстве.
  - Название и версию операционной системы, установленной на устройстве.
  - Версию Kaspersky Endpoint Security.

    - Дату выпуска используемых баз приложения.
    - Статус лицензионного ключа.
- Данные из запросов к компоненту EDR Expert (cloud) в отчетах о результатах выполнения задач:
    - IP-адрес устройства.
    - Уникальный идентификатор.
    - Базовую часть веб-адреса сервера.
    - MAC-адрес устройства.
    - Ошибки выполнения задач и коды возврата.
    - Статусы, с которыми завершались задачи.
    - Время завершения задач.
    - Версии параметров, с которыми выполнялись задачи.
    - Информацию о процессах, запущенных на устройстве по запросу сервера:
        - Код завершения процесса.
        - Уникальный идентификатор файла с содержимым стандартного вывода процесса.
        - Уникальный идентификатор файла с содержимым стандартного вывода ошибок процесса.
    - Информацию о процессах, запущенных или остановленных на устройстве по запросу сервера:
        - PID (Идентификатор системного процесса).
        - UniquePID (Уникальный идентификатор процесса).
        - Код ошибки.
    - Копию файла, запрошенного сервером, а также путь к файлу и его идентификатор.
    - Признак удаления файла после перезапуска ОС.
    - Данные об ошибках получения информации об объектах: полное имя объекта, при обработке которого возникла ошибка; код ошибки.
    - Статус применения сетевой изоляции.
    - Для индикаторов IOC возвращаются результаты поиска (сработал или не сработал каждый индикатор; найденные объекты и информация о том, какая ветка индикатора сработала).

- Для объектов, вызвавших срабатывания индикаторов IoC, возвращаются разные значения в зависимости от типа:
  - ArpEntry: IP-адрес из ARP-таблицы (в том числе ipv6), физический адрес из ARP-таблицы.
  - File: MD5-хеш файла, SHA-256-хеш файла, полное имя файла (включая путь), размер файла.
  - Port: удаленный IP-адрес и порт, с которым в момент проверки установлено соединение; IP-адрес и порт локального адаптера; тип протокола (TCP, UDP, IP, RAWIP).
  - Process: имя процесса; аргументы процесса; путь к файлу процесса; системный PID процесса; системный PID родительского процесса; имя пользователя, от имени которого запущен процесс; дата и время запуска процесса.
  - SystemInfo: имя ОС, версия ОС, сетевое имя устройства без домена, домен или рабочая группа.
  - User: имя пользователя.
- Для объектов, помещенных на карантин:
  - Путь к файлу.
  - Размер файла.
  - Идентификаторы файла, присвоенные ему при помещении на карантин.
  - Флаг об удалении оригинального файла.
- Для файлов, полученных, восстановленных или удаленных из карантина:
  - Идентификаторы файла, присвоенные ему при помещении на карантин.
- Для запрещенных запусков исполняемых файлов или скриптов:
  - Идентификатор процесса.
  - Идентификатор родительского процесса.
  - Системный идентификатор.
  - Идентификатор сеанса входа в систему.
  - Состояние процесса.
  - Дата и время перехвата запуска.
- Для запрещенных открытий документов с помощью офисных приложений:
  - Идентификатор процесса.
  - Идентификатор файла.
  - Дата и время перехвата запуска.

- Перечень файлов в указанной директории:
  - Имя файла.
  - Абсолютный путь к файлу.
  - Размер файла.
  - Тип файла.
  - Имя и идентификатор владельца и группы владельца.
  - Права доступа к файлу.
  - Специальные флаги файловой системы, распространяемые на каждый файл.
  - Метаданные о файле.
  - Количество жестких ссылок на файл.
  - Время создания, изменения и последнего доступа к файлу.
- Перечень запущенных процессов на устройстве:
  - Имя процесса.
  - Время запуска процесса.
  - Статус процесса.
  - Идентификатор процесса (PID) и идентификатор родительского процесса.
  - Текущая рабочая директория процесса.
  - Параметры запуска процесса.
  - Переменные окружения.
  - Путь к исполняемому файлу процесса.
  - Идентификатор сессии пользователя, запустившего процесс.
  - Идентификатор пользователя и группы, запустивших процесс.
  - Идентификатор пользователя и группы, с правами которых процесс имеет доступ к файлам и ресурсам в системе.
- Перечень точек автозапуска:
  - Тип точки автозапуска.
  - Имя файла.
  - Абсолютный путь к файлу.

    - Права доступа к файлу.
    - Специальные флаги файловой системы, распространяемые на каждый файл.
    - Имя и идентификатор владельца и группы владельца.
    - Время создания, изменения и последнего доступа к файлу.
    - MD5-хеш и SHA-256-хеш исполняемого файла или загружаемого модуля.
  - Образ памяти процесса:
    - Имя файла образа памяти процесса.
    - Полный путь к файлу процесса.
    - Уникальный идентификатор файла образа памяти процесса.
    - Размер файла образа памяти процесса.
  - Образ памяти устройства:
    - Дату и время начала формирования дампа.
    - Полный путь к файлу дампа.
    - Размер файла образа памяти устройства.
  - Образ диска устройства:
    - Дату и время начала формирования дампа.
    - Массив полных путей к файлам дампа.
    - Размер файла образа диска устройства.
    - Логический диск.
    - Физический диск.
- Данные в пакетах телеметрии:
  - Данные о событиях телеметрии:
    - Идентификатор события.
    - Порядковый номер события в последовательности отправляемых пакетов телеметрии.
    - Тип события.
    - Время возникновения события.

- Информацию о защищаемом устройстве:
  - Имя защищаемого устройства.
  - Идентификатор защищаемого устройства в Kaspersky Security Center.
  - Идентификатор защищаемого устройства в Kaspersky Endpoint Detection and Response Expert (on-premises).
  - Название, версию, семейство операционной системы, установленной на защищаемом устройстве.
  - Время запуска и выключения операционной системы, установленной на защищаемом устройстве.
- Данные о файлах:
  - Уникальный идентификатор файла.
  - Путь к файлу.
  - Имя файла.
  - Размер файла.
  - Атрибуты файла.
  - Дату и время создания файла.
  - Дату и время последнего изменения файла.
  - MD5 и SHA256-хеши объекта.
  - Информацию о пользователе и группе, владеющих файлом (имя и идентификатор).
- Данные о запущенных процессах:
  - Идентификатор файла процесса.
  - Идентификатор процесса.
  - Параметры запуска процесса.
  - Идентификатор сессии.
  - Дату и время запуска процесса.
  - Информацию о пользователе и группе, от имени которых запущен процесс (имя и идентификатор).
- Данные о процессе, получающем доступ к памяти другого процесса:
  - Идентификатор процесса.
  - Метод и адрес внедрения (injection).

    - Командную строку изменения процесса с аргументами.
    - Аргументы системного вызова процесса.
- Информацию об обнаруженных и обработанных угрозах:
    - Название обнаруженной угрозы и технологии, обнаружившей угрозу, согласно классификации "Лаборатории Касперского".
    - Дату выпуска и версию баз приложения.
    - Веб-адрес, с которого был загружен зараженный объект.
    - Статус обработки угрозы.
    - Причину невозможности устранения угрозы.
    - Уникальный идентификатор файла угрозы.
- Данные об изменении файлов:
    - Уникальный идентификатор изменившегося файла.
    - Уникальный идентификатор процесса, совершившего изменения.
    - Информацию о произошедшем изменении.
- Данные об изменениях в системе:
    - Уникальный идентификатор процесса, совершившего изменения.
    - Информация о произошедшем изменении.
- Информацию о входе пользователя в систему:
    - Идентификатор сессии.
    - Информация о пользователе (имя и идентификатор).
    - IP-адрес устройства, с которого установлена сессия.
- Данные о завершающихся процессах: уникальный идентификатор процесса.
- Информацию о загрузке библиотеки в адресное пространство процесса: идентификатор загруженной библиотеки.
- Информацию об установлении и завершении сетевого соединения:
    - Локальный IP-адрес.
    - Удаленный IP-адрес.
    - Направление соединения.
    - Протокол.

    - Время начала соединения.
    - Время завершения соединения.
    - Длительность соединения.
    - Количество отправленных байт за время соединения.
    - Количество полученных байт за время соединения.
- Информацию о процессе, который "прослушивает" внешние сетевые соединения на определенном порту:
    - Локальный адрес (порт и IP-адрес).
    - Протокол.
- Информацию об обращении к DNS-серверу:
    - Доменное имя запрашиваемого ресурса.
    - IP-адреса запрашиваемого ресурса.
    - IP-адрес DNS-сервера.
    - Тип запроса.
- Информацию о подключаемых внешних устройствах:
    - Тип операции (подключение устройства).
    - Тип устройства.
    - Уникальный идентификатор устройства.
    - Имя устройства.
    - Путь к устройству.
- Информация о приложении и о его модулях:
    - Версию приложения.
    - Время установки, запуска, остановки и удаления приложения.
    - Инициатор действия над приложением.
    - Причина остановки приложения в случае внештатной остановки.
    - Коды возврата в случае внештатной остановки.

- Информацию о взаимодействии с планировщиками задач (создание и удаление задач):
  - Имя задачи.
  - Путь к команде, которая выполняется по расписанию.
  - Расписание запуска задачи.
  - Имя учетной записи пользователя, создавшего задачу.
  - Имя учетной записи, от имени которой запускается задача.
  - Имя учетной записи пользователя, удалившего задачу.
- Информацию о создании, удалении и изменении службы:
  - Имя службы (в том числе предыдущее в случае изменения).
  - Тип службы (в том числе предыдущий в случае изменения).
  - Путь к исполняемому файлу (в том числе предыдущий в случае изменения).
  - Зависимости службы (в том числе предыдущие в случае изменения).
  - Имя учетной записи, от имени которой запускается служба (в том числе предыдущее в случае изменения).
  - Отображаемое имя службы (в том числе предыдущее в случае изменения).
  - Имя учетной записи пользователя, создавшего, удалившего или изменившего службу.
  - Признак отложенного удаления.
- Информацию о вводе в консоль:
  - Идентификатор и тип процесса, инициировавшего ввод в консоль.
  - Содержимое ввода в консоль.
- Информацию о смонтированных устройствах:
  - Системное имя тома.
  - Точка монтирования.
- Информацию об изменении в памяти процесса:
  - Аргументы системного вызова процесса.
  - Информацию о процессе, осуществившем внедрение кода, и о его родительском процессе.
    - Идентификатор процесса и уникальный идентификатор процесса и родительского процесса.
    - Командную строку, из которой был запущен процесс и родительский процесс.

    - Переменные окружения процесса.
    - Вид учетной записи пользователя, от имени которого был запущен процесс и родительский процесс.
    - Системный вызов, с помощью которого был создан процесс.
    - Идентификатор пользователя и группы, запустивших процесс.
    - Имя и полное имя процесса и родительского процесса.
    - Полный путь к процессу и родительскому процессу.
    - MD5 и SHA256-хеши процесса и родительского процесса.
    - Идентификатор сессии.
    - Имя, доменное имя и идентификатор пользователя, запустившего процесс и родительский процесс.
- Информацию о процессе, через который был загружен процесс, осуществивший внедрение кода.
    - Уникальный идентификатор процесса, через который был загружен процесс.
    - Имя и полное имя файла, через который был загружен процесс.
    - Полный путь к процессу, через который был загружен процесс.
    - MD5-хеш процесса, через который был загружен процесс.
- Информацию о процессе, являющемся инициатором процесса.
    - Идентификатор процесса и уникальный идентификатор процесса, являющегося инициатором процесса.
    - Командную строку процесса, являющегося инициатором процесса.
    - Имя и доменное имя пользователя, запустившего процесс, являющийся инициатором процесса.
    - Имя и полное имя процесса, являющегося инициатором процесса.
    - Полный путь к процессу, являющемуся инициатором процесса.
    - MD5 и SHA256-хеши процесса, являющегося инициатором процесса.

Также указанная информация может сохраняться в файлах трассировки и файлах дампов.

Данные, предоставляемые при интеграции с компонентом Kaspersky Network Detection and Response (KATA)

При интеграции приложения Kaspersky Endpoint Security с компонентом Kaspersky Network Detection and Response (KATA) – компонентом решения Kaspersky Anti Targeted Attack Platform – приложение Kaspersky Endpoint Security сохраняет следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Адреса серверов NDR.
- Открытый ключ сертификата сервера для интеграции с Kaspersky Network Detection and Response (KATA).
- Сертификат клиента для интеграции с Kaspersky Network Detection and Response (KATA).
- Учетные данные для авторизации на прокси-сервере.
- Параметры частоты синхронизации с сервером NDR и параметры передачи данных на сервер NDR.
- Статус соединения с сервером NDR и сведения об ошибках сертификата клиента и сертификата сервера.

При интеграции приложения Kaspersky Endpoint Security с компонентом Kaspersky Network Detection and Response (KATA) приложение Kaspersky Endpoint Security сохраняет и передает серверу NDR следующие данные:

- Данные из запросов на синхронизацию к серверу NDR:
  - Уникальный идентификатор.
  - Базовую часть веб-адреса сервера.
  - Имя устройства.
  - IP-адрес устройства.
  - MAC-адрес устройства.
  - Локальное время на устройстве.
  - Название, семейство и версию операционной системы, установленной на устройстве.
  - Версию Kaspersky Endpoint Security.
  - Дату выпуска используемых баз приложения.
  - Статус лицензионного ключа.
  - Модель и производитель устройства пользователя.

- Данные в пакетах телеметрии:
  - Информацию об устройстве и пользователях:
    - Имя устройства и время на устройстве.
    - Семейство, имя и версию операционной системы.
    - Информацию о сетевых интерфейсах (описание, список IP-адресов с маской подсети, MAC-адрес, номер метрики, имя DNS-домена, данные о маршрутизации, номера прослушиваемых портов).
    - Внутренний уникальный идентификатор устройства.
    - Имена и идентификаторы пользователей.
    - Имена и идентификаторы групп пользователей.
  - Информацию о приложении Kaspersky Endpoint Security:
    - Имя и версию приложения.
    - Дату последнего обновления приложения.
    - Информацию о лицензионных ключах (серийный номер, тип, срок действия лицензии, статус ключа).
    - Версию баз приложения.
    - Список поддерживаемых версий API.
  - Информацию об установленных соединениях:
    - Локальный IP-адрес, порт и MAC-адрес.
    - Удаленный IP-адрес, порт и MAC-адрес.
    - IP-адрес шлюза.
    - Тип протокола (по IANA), номер протокола и EtherType.
    - Количество принятых и переданных пакетов.
  - Информацию об обрабатываемых файлах:
    - Имя и уникальный идентификатор файла.
    - Тип и размер файла.
    - Полный путь к образу файла.
    - Маску атрибутов файловой системы.
    - Время создания и изменения файла.

    - Контрольные суммы (MD5 и SHA256).
    - Привилегии файла, в том числе унаследованные и эффективные.
- Информацию о запущенных и завершающихся процессах:
    - UID и PID процесса.
    - Тип процесса.
    - Идентификатор сеанса.
    - Выполняемую команду.
    - Переменные окружения.
- Информацию об обнаруженных и обработанных угрозах:
    - Название обнаруженной угрозы и технологии, обнаружившей угрозу, согласно классификации "Лаборатории Касперского".
    - Версию баз приложения.
    - Веб-адрес, с которого был загружен зараженный объект.
    - Статус обработки угрозы.
    - Причину невозможности устранения угрозы.

Также указанная информация может сохраняться в файлах трассировки и файлах дампов.

Данные, предоставляемые при интеграции с решением Kaspersky Unified Monitoring and Analysis Platform

При интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Unified Monitoring and Analysis Platform приложение Kaspersky Endpoint Security сохраняет следующую информацию, которая может содержать персональные и конфиденциальные данные:

- Адреса серверов KUMA.
- Открытый ключ сертификата сервера для интеграции с Kaspersky Unified Monitoring and Analysis Platform (кроме случая, когда для подключения к серверу KUMA используется протокол UDP).
- Сертификат клиента для интеграции с Kaspersky Unified Monitoring and Analysis Platform.
- Учетные данные для авторизации на прокси-сервере.
- Параметры частоты синхронизации с сервером KUMA и параметры передачи данных на сервер KUMA.
- Статус соединения с сервером KUMA и сведения об ошибках сертификата клиента и сертификата сервера.

При интеграции приложения Kaspersky Endpoint Security с Kaspersky Unified Monitoring and Analysis Platform приложение Kaspersky Endpoint Security сохраняет и передает серверу KUMA следующие данные в пакетах телеметрии:

- Информацию об изменении файлов:
  - Уникальный идентификатор файла до изменения.
  - Уникальный идентификатор изменившегося файла.
  - Уникальный идентификатор процесса, совершившего изменения.
  - Тип и флаг операции с файлом.
  - Дату и время изменения файла.
- Информацию о запущенных и завершающихся процессах:
  - Идентификатор файла процесса.
  - UID и PID процесса.
  - Параметры запуска процесса.
  - Идентификатор сессии.
  - Дату и время запуска процесса.
  - Информацию о пользователе и группе, от имени которых запущен процесс (имя и идентификатор).
- Информацию о событиях в журнале событий:
  - Дату и время возникновения события.
  - UID процесса, связанного с событием.
  - Тип и описание события.
  - Результат выполнения операции.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Acrobat, Flash, Shockwave являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

AMD64 – товарный знак или зарегистрированный товарный знак Advanced Micro Devices, Inc.

Amazon является товарным знаком Amazon.com, Inc. или аффилированных лиц компании.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

AutoCAD – товарный знак или зарегистрированный в США и/или других странах товарный знак, принадлежащий Autodesk, Inc. и / или дочерним / аффилированным компаниям.

Borland – товарный знак или зарегистрированный товарный знак Borland Software Corporation.

dBase – товарный знак dataBased Intelligence, Inc.

FireWire – товарный знак Apple Inc.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Ubuntu и LTS являются зарегистрированными товарными знаками Canonical Ltd.

XenServer является зарегистрированным товарным знаком или товарным знаком Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Словесный знак Grafana и логотип Grafana являются зарегистрированными товарными знаками/знаками обслуживания или товарными знаками/знаками обслуживания Coding Instinct AB в США и других странах и используются с разрешения Coding Instinct. Мы не являемся аффилированной, поддерживаемой или спонсируемой со стороны Coding Instinct или сообщества Grafana компанией.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Chrome, Chromium, Google Chrome, Google Public DNS – товарные знаки Google LLC.

HUAWEI, EulerOS, FusionSphere являются товарными знаками Huawei Technologies Co., Ltd.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Microsoft Edge, Active Directory, Hyper-V, Outlook, Visual Basic, Visual FoxPro, Visual C++, PowerPoint, Excel, Internet Explorer, Windows и Windows Server являются товарными знаками группы компаний Microsoft.

OpenStack – зарегистрированный товарный знак OpenStack Foundation в США и других странах.

Oracle, Java, JavaScript – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Red Hat Enterprise Linux, CentOS, Fedora – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Kubernetes является зарегистрированным товарным знаком The Linux Foundation в США и других странах.

Rocky Linux является товарным знаком The Rocky Enterprise Software Foundation.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Zabbix – зарегистрированный товарный знак Zabbix SIA.