kaspersky

Kaspersky Endpoint Security для Linux

© 2026 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Endpoint Security 12.4 для Linux

О Kaspersky Endpoint Security 12.4 для Linux

- О режимах использования приложения Kaspersky Endpoint Security
  - Использование приложения в режиме Легкого агента
  - Использование приложения в режиме Агента Endpoint Detection and Response
- Комплект поставки
- Аппаратные и программные требования
  - Аппаратные требования
  - Программные требования
  - Дополнительные программные требования для режима Легкого агента
  - Поддерживаемые версии Kaspersky Security Center
  - Поддерживаемые версии решений на платформах KATA и OSMP

Что нового

Исправленные ошибки

Подготовка к установке приложения Kaspersky Endpoint Security

Установка и первоначальная настройка приложения Kaspersky Endpoint Security

- Установка и первоначальная настройка Агента администрирования Kaspersky Security Center
- Установка плагинов управления Kaspersky Endpoint Security
  - Установка веб-плагина Kaspersky Endpoint Security
  - Установка MMC-плагина Kaspersky Endpoint Security
- Установка и первоначальная настройка приложения с помощью Kaspersky Security Center
  - Создание инсталляционного пакета в Web Console
  - Параметры первоначальной настройки в Web Console
  - Создание инсталляционного пакета в Консоли администрирования
  - Параметры первоначальной настройки в Консоли администрирования
  - Подготовка архива с базами приложения для создания инсталляционного пакета с интегрированными базами
  - Параметры конфигурационного файла autoinstall.ini
  - Подготовка приложения к работе с помощью Kaspersky Security Center
- Установка и первоначальная настройка приложения с помощью командной строки
  - Установка приложения с помощью командной строки
  - Первоначальная настройка приложения в интерактивном режиме
    - Выбор режима использования: стандартный или Легкий агент
    - Определение роли виртуальной машины
    - Включение режима защиты инфраструктуры VDI
    - Выбор режима использования: стандартный или Агент Endpoint Detection and Response
    - Выбор языкового стандарта
    - Просмотр Лицензионного соглашения и Политики конфиденциальности
    - Принятие Лицензионного соглашения
    - Принятие Политики конфиденциальности
    - Использование Kaspersky Security Network
    - Удаление пользователей из привилегированных групп
    - Назначение пользователю роли администратора
    - Настройка механизма перехвата системных событий

Включение автоматической настройки SELinux
Настройка источника обновлений
Настройка параметров прокси-сервера
Запуск обновления баз приложения
Включение автоматического обновления баз приложения
Активация приложения
Первоначальная настройка приложения в автоматическом режиме
Параметры конфигурационного файла первоначальной настройки
Настройка разрешающих правил в системе SELinux
Запуск приложения в ОС Astra Linux в режиме замкнутой программной среды
Запуск приложения в ОС Альт СП в режиме замкнутой программной среды
Настройка ОС ОСнова для работы приложения
Оптимизация потребления ресурсов приложением
Рекомендации для типовых серверных ролей
Анализ работы приложения на устройстве
Анализ потребления ресурсов задачей Защита от файловых угроз
Определение наиболее часто проверяемых объектов
Рекомендации для Защиты от файловых угроз и задач проверки
Настройка исключений из проверки
Настройка исключений из перехвата файловых операций
Установка ограничения на использование памяти приложением
Рекомендации для Защиты от веб-угроз и Защиты от сетевых угроз
Обновление предыдущей версии приложения
Об обновлении плагинов управления Kaspersky Endpoint Security
Обновление приложения с помощью Kaspersky Security Center
Обновление приложения с помощью командной строки
Особенности установки значений параметров при обновлении приложения
Удаление приложения
Об удалении приложения и Агента администрирования с помощью Kaspersky Security Center
Удаление приложения с помощью командной строки
Удаление Агента администрирования с помощью командной строки
Удаление плагинов управления Kaspersky Endpoint Security
Лицензирование приложения
О Лицензионном соглашении
О лицензии
О Лицензионном сертификате
О лицензионном ключе
О коде активации
О файле ключа
О подписке
Сравнение функций приложения в зависимости от лицензии
Активация приложения и управление лицензионными ключами
Активация приложения с помощью Kaspersky Security Center
Управление лицензионными ключами в командной строке

Просмотр информации об используемых лицензионных ключах
Просмотр информации о ключах на устройстве через Web Console
Просмотр информации о ключах на устройстве через Консоль администрирования
Просмотр информации о лицензии и ключе в командной строке
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-premise)
Данные, предоставляемые при интеграции с компонентом Kaspersky Network Detection and Response (KATA)
Данные, предоставляемые при интеграции с решением Kaspersky Unified Monitoring and Analysis Platform
Концепция управления приложением
Управление приложением через Kaspersky Security Center
О плагинах управления Kaspersky Endpoint Security
О политиках Kaspersky Security Center
О задачах для Kaspersky Endpoint Security, созданных в Kaspersky Security Center
Вход и выход из Web Console и Cloud Console
Управление политиками в Web Console
Создание политики в Web Console
Изменение параметров политики в Web Console
Параметры политики в Web Console
Управление политиками в Консоли администрирования
Создание политики с помощью Консоли администрирования
Изменение параметров политики в Консоли администрирования Kaspersky Security Center
Параметры политики в Консоли администрирования
Управление задачами в Web Console
Создание задач в Web Console
Изменение параметров задач в Web Console
Запуск, остановка, приостановка и возобновление задач в Web Console
Управление задачами в Консоли администрирования
Создание задач в Консоли администрирования
Изменение параметров задач в Консоли администрирования
Запуск, остановка, приостановка и возобновление задач в Консоли администрирования
Управление приложением через командную строку
Включение автоматического дополнения команды kesl-control (bash completion)
Управление задачами в командной строке
Просмотр списка задач в командной строке
Просмотр состояния задачи в командной строке
Создание задачи в командной строке
Запуск, остановка, приостановка и возобновление задачи в командной строке
Удаление задачи в командной строке

Вывод параметров задачи в командной строке
Изменение параметров задачи в командной строке
Изменение параметров задачи с помощью конфигурационного файла
Изменение параметров задачи с помощью ключей командной строки
Восстановление параметров задачи по умолчанию в командной строке
Настройка расписания задачи в командной строке
Управление общими параметрами приложения в командной строке
Вывод общих параметров приложения
Изменение общих параметров приложения
Использование фильтра для ограничения результатов запросов
Экспорт и импорт параметров приложения
Управление ролями пользователей с помощью командной строки
Просмотр списка пользователей и ролей
Назначение роли пользователю
Отзыв роли у пользователя
Запуск и остановка приложения
Запуск и остановка приложения с помощью Web Console
Запуск и остановка приложения с помощью Консоли администрирования
Запуск и остановка приложения с помощью командной строки
Просмотр состояния защиты устройства и информации о работе приложения
Просмотр состояния защиты устройства в Web Console
Просмотр состояния защиты устройства в Консоли администрирования
Просмотр информации о работе приложения в Web Console
Просмотр информации о работе приложения в Консоли администрирования
Просмотр информации о работе приложения в командной строке
Просмотр статистики работы приложения
Просмотр статистики работы приложения в Web Console
Просмотр статистики работы приложения в Консоли администрирования
Просмотр списка точек монтирования в Web Console
Просмотр списка точек монтирования в Консоли администрирования
Просмотр статистики работы приложения и списка точек монтирования в командной строке
Сбор метрик о состоянии системы
Обновление баз и модулей приложения
Об обновлении баз и модулей
Об источниках и схемах обновления
Обновление баз и модулей приложения в Web Console
Обновление баз и модулей приложения в Консоли администрирования
Обновление баз и модулей приложения в командной строке
Обновление с помощью Kaspersky Update Utility
Откат обновления баз и модулей приложения
Защита от файловых угроз
Настройка защиты от файловых угроз в Web Console
Настройка защиты от файловых угроз в Консоли администрирования
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
Настройка защиты от файловых угроз в командной строке
Параметры задачи Защита от файловых угроз
Оптимизация проверки сетевых директорий
Особенности проверки символических и жестких ссылок
Поиск вредоносного ПО
Поиск вредоносного ПО в Web Console
Окно добавления области проверки
Раздел Области проверки
Окно Области проверки
Раздел Области исключения
Окно Области исключения
Окно добавления области исключения
Окно Исключения по маске
Окно Исключения по названию угрозы
Поиск вредоносного ПО в Консоли администрирования
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
Поиск вредоносного ПО в командной строке
Параметры предустановленной задачи Поиск вредоносного ПО
Выборочная проверка файлов и директорий в командной строке
Проверка важных областей
Проверка важных областей в Web Console
Окно добавления области проверки
Раздел Области проверки
Окно Области проверки
Раздел Области исключения
Окно Области исключения
Окно добавления области исключения
Окно Исключения по маске
Окно Исключения по названию угрозы

- Проверка важных областей в Консоли администрирования
  - 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 в командной строке

Проверка съемных дисков
- Настройка проверки съемных дисков в Web Console
- Настройка проверки съемных дисков в Консоли администрирования
- Настройка проверки съемных дисков в командной строке

Проверка контейнеров
- Мониторинг контейнеров
  - Настройка мониторинга контейнеров в Web Console
  - Настройка мониторинга контейнеров в Консоли администрирования
    - Окно Параметры проверки контейнеров
  - Настройка мониторинга контейнеров в командной строке
- Проверка контейнеров и образов по требованию
  - Проверка контейнеров в Web Console
    - Раздел Области исключения
    - Окно Исключения по маске
    - Окно Исключения по названию угрозы
  - Проверка контейнеров в Консоли администрирования
    - Окно Параметры проверки контейнеров
    - Окно Параметры проверки
    - Окно Действия при обнаружении угрозы
    - Раздел Исключения
    - Окно Исключения по маске
    - Окно Исключения по названию угрозы
  - Проверка контейнеров в командной строке
    - Параметры задачи Проверка контейнеров
    - Выборочная проверка контейнеров и образов
    - Интеграция с Jenkins

Управление сетевым экраном
- О сетевых пакетных правилах
- О динамических правилах
- О предустановленных доступных сетях
- Управление сетевым экраном в Web Console
- Управление сетевым экраном в Консоли администрирования
  - Окно Сетевые пакетные правила
  - Окно Добавление сетевого пакетного правила

Окно Добавление IP-адресов
Окно Доступные сети
Окно Сетевое соединение
Управление сетевым экраном в командной строке
Настройка списка сетевых пакетных правил в командной строке
Настройка сетевых зон в командной строке
Защита от веб-угроз
Настройка защиты от веб-угроз в Web Console
Настройка защиты от веб-угроз в Консоли администрирования
Окно Доверенные веб-адреса
Окно Параметры проверки
Настройка защиты от веб-угроз в командной строке
Проверка сетевого трафика
О режимах перехвата сетевого трафика
Настройка проверки сетевого трафика в Web Console
Настройка проверки сетевого трафика в Консоли администрирования
Окно Доверенные домены
Окно Доверенные корневые сертификаты
Окно Исключения из перехвата трафика
Окно Исключение из перехвата трафика
Окно Контролируемые порты
Настройка проверки сетевого трафика в командной строке
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
Исключения из перехвата трафика средствами операционной системы
Защита от сетевых угроз
Настройка защиты от сетевых угроз в Web Console
Настройка защиты от сетевых угроз в Консоли администрирования
Окно Исключения
Настройка защиты от сетевых угроз в командной строке
Защита от почтовых угроз
Настройка защиты от почтовых угроз в Web Console
Настройка защиты от почтовых угроз в Консоли администрирования
Окно Параметры защиты от почтовых угроз
Окно Фильтр вложений
Настройка защиты от почтовых угроз в командной строке
Защита от атак BadUSB
Настройка защиты от атак BadUSB в Web Console
Настройка защиты от атак BadUSB в Консоли администрирования
Настройка защиты от атак BadUSB в командной строке
Защита от удаленного вредоносного шифрования
Настройка защиты от шифрования в Web Console
Настройка защиты от шифрования в Консоли администрирования
Окно Области проверки
Окно Новая область проверки

Окно Параметры защиты
Окно Области исключения
Окно Новая область исключения
Окно Исключения по маске
Настройка защиты от шифрования в командной строке
Управление заблокированными устройствами
Контроль приложений
О правилах контроля приложений
Режим тестирования правил контроля приложений
Настройка контроля приложений в Web Console
Настройка контроля приложений в Консоли администрирования
Окно Правила Контроля приложений
Окно Добавление правила
Окно Категории приложений
Окно Пользователь или группа
Настройка контроля приложений в командной строке
Параметры задачи Контроль приложений
Создание и изменение списка категорий
Просмотр списка категорий
Настройка списка правил контроля приложений
Экспорт и импорт параметров Контроля приложений
Инвентаризация
Настройка инвентаризации в Web Console
Окно добавления области проверки
Раздел Области исключения
Окно Области исключения
Окно добавления области исключения
Настройка инвентаризации в Консоли администрирования
Окно Области проверки
Окно Новая область проверки
Раздел Исключения
Окно Области исключения
Окно Новая область исключения
Настройка инвентаризации в командной строке
Параметры задачи Инвентаризация
Просмотр списка обнаруженных приложений
Контроль устройств
Настройка контроля устройств в Web Console
Настройка контроля устройств в Консоли администрирования
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
Настройка шаблона сообщений Контроля устройств
Настройка Контроля устройств в командной строке
Параметры задачи Контроль устройств
Просмотр и экспорт списка подключенных устройств в командной строке
Управление списком доверенных устройств в командной строке
Предоставление временного доступа к устройству
Предоставление доступа к устройству в Web Console
Получение временного доступа к устройству в командной строке
Веб-Контроль
О правилах доступа к веб-ресурсам
Настройка Веб-Контроля в Web Console
Настройка Веб-Контроля в Консоли администрирования
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
Настройка шаблонов сообщений Веб-Контроля
Настройка Веб-Контроля в командной строке
Параметры задачи Веб-Контроль
Просмотр и изменение параметров Веб-Контроля
Правила формирования масок адресов веб-ресурсов
Контроль целостности системы
Контроль целостности системы в реальном времени
Настройка контроля целостности системы в Web Console
Настройка контроля целостности системы в Консоли администрирования
Окно Области проверки
Окно Новая область проверки
Окно Области исключения
Окно Новая область исключения
Окно Исключения по маске
Настройка контроля целостности системы в командной строке
Проверка целостности системы
Проверка целостности системы в Web Console
Окно добавления области проверки
Раздел Области исключения
Окно Области исключения
Окно добавления области исключения
Окно Исключения по маске

Проверка целостности системы в Консоли администрирования
Окно Области проверки
Окно Новая область проверки
Раздел Области исключения
Окно Области исключения
Окно Новая область исключения
Окно Исключения по маске
Проверка целостности системы в командной строке
Анализ поведения
Настройка анализа поведения в Web Console
Настройка анализа поведения в Консоли администрирования
Окно Исключения по процессам
Окно Доверенный процесс
Настройка анализа поведения в командной строке
Защита от эксплойтов
Настройка защиты от эксплойтов в Web Console
Настройка защиты от эксплойтов в Консоли администрирования
Окно Исключения Защиты от эксплойтов
Окно Исключение Защиты от эксплойтов
Настройка защиты от эксплойтов в командной строке
Использование Kaspersky Security Network
Настройка использования Kaspersky Security Network в Web Console
Настройка использования Kaspersky Security Network в Консоли администрирования
Параметры Kaspersky Security Network
Положение о Kaspersky Security Network
Положение о Kaspersky Private Security Network
Настройка использования Kaspersky Security Network в командной строке
Проверка подключения к Kaspersky Security Network с помощью командной строки
Включение и выключение облачного режима с помощью командной строки
Дополнительные параметры работы приложения
Настройка прокси-сервера
Настройка параметров прокси-сервера в Web Console
Настройка параметров прокси-сервера в Консоли администрирования
Окно Исключения для прокси-сервера
Настройка параметров прокси-сервера в командной строке
Настройка глобальных исключений
Настройка глобальных исключений в Web Console
Настройка глобальных исключений в Консоли администрирования
Окно Путь к точке монтирования
Настройка глобальных исключений в командной строке
Исключение памяти процессов из проверки
Выбор режима перехвата файловых операций
Настройка обнаружения приложений, которые злоумышленники могут использовать для нанесения вреда
Включение мониторинга стабильности работы приложения
Настройка параметров запуска приложения
Ограничение на использование резидентной памяти приложением
Ограничение на использование памяти и ресурсов процессора

Ограничение на количество задач выборочной проверки
Настройка отправки информации в хранилище Kaspersky Security Center
Настройка разрешений на управление задачами
Отмена запуска задач при работе от аккумулятора
Настройка параметров перехвата системных событий
Проверка возможности установки обновляемого модуля ядра
"Безопасный" режим при использовании обновляемого модуля ядра
Настройка параметров перехвата в Web Console
Настройка параметров перехвата в Консоли администрирования
Настройка параметров перехвата в командной строке
Настройка дополнительных параметров телеметрии
Резервное хранилище
Настройка параметров резервного хранилища в Web Console
Настройка параметров резервного хранилища в Консоли администрирования
Настройка параметров резервного хранилища в командной строке
Работа с объектами резервного хранилища в командной строке
Интеграция с решениями Detection and Response
О действиях по реагированию по командам от решений Detection and Response
Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise)
Как подготовить эталонный образ для корректной интеграции с EDR Expert (on-premise)
Настройка интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) в Web Console
Настройка интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) в командной строке
Параметры интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise)
Управление сертификатами для подключения к серверам OSMP
Интеграция с Kaspersky Anti Targeted Attack Platform
Настройка интеграции с Kaspersky Endpoint Detection and Response (KATA) в Web Console
Настройка интеграции с Kaspersky Endpoint Detection and Response (KATA) в Консоли администрирования
Настройка подключения к серверам KATA
Настройка общих параметров подключения к серверам KATA
Настройка параметров передачи данных на серверы KATA
Настройка интеграции с Kaspersky Endpoint Detection and Response (KATA) в командной строке
Параметры интеграции с Kaspersky Endpoint Detection and Response (KATA)
Управление сертификатами для подключения к серверу KATA
Настройка интеграции с Kaspersky Network Detection and Response (KATA) в Web Console
Настройка интеграции с Kaspersky Network Detection and Response (KATA) в Консоли администрирования
Настройка подключения к серверам NDR
Настройка общих параметров подключения к серверам NDR
Настройка параметров передачи данных на серверы NDR
Настройка интеграции с Kaspersky Network Detection and Response (KATA) в командной строке
Параметры интеграции с Kaspersky Network Detection and Response (KATA)
Управление сертификатами для подключения к серверу NDR
Интеграция с Sandbox
Настройка интеграции с Sandbox в Web Console
Настройка интеграции с Sandbox в командной строке
Параметры интеграции с Sandbox
Управление сертификатами для подключения к серверу Sandbox

Интеграция с Kaspersky Endpoint Detection and Response Optimum
Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum
Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console
Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в командной строке
Просмотр статуса интеграции с Kaspersky Endpoint Detection and Response Optimum
Просмотр информации об обнаруженной угрозе и действиях по реагированию
Интеграция с Kaspersky Managed Detection and Response
Рекомендации по созданию эталонного образа для корректной интеграции с MDR
Загрузка конфигурационного файла KPSN для интеграции с Kaspersky Managed Detection and Response
Настройка интеграции с Kaspersky Managed Detection and Response в Web Console
Настройка интеграции с Kaspersky Managed Detection and Response в Консоли администрирования
Настройка интеграции с Kaspersky Managed Detection and Response в командной строке
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
Настройка исключений из сетевой изоляции в автоматическом режиме
Окно добавления исключения из сетевой изоляции
Окно Словарь сетевых профилей
Управление сетевой изоляцией устройства в командной строке
Работа с карантином
Помещение файла на карантин с помощью Web Console
Настройка параметров карантина в Web Console
Настройка параметров карантина в Консоли администрирования
Настройка параметров карантина в командной строке
Работа с файлами карантина в командной строке
Запуск процесса
Завершение процесса
Получение файла с устройства
Удаление файла с устройства
Поиск индикаторов компрометации
Поиск индикаторов компрометации в Web Console
Поиск индикаторов компрометации в командной строке
Требования к IOC-файлам
Запрет запуска объектов
Настройка запрета запуска объектов в Web Console
Настройка запрета запуска объектов в Консоли администрирования
Управление запретом запуска объектов в командной строке
Cloud Sandbox
Интеграция с Kaspersky Unified Monitoring and Analysis Platform
Настройка интеграции с KUMA в Web Console
Настройка интеграции с KUMA в Консоли администрирования
Окно Серверы KUMA
Окно Сервер KUMA
Окно Параметры подключения к серверам KUMA

Окно добавления сертификата сервера
Окно добавления сертификата клиента
Настройка интеграции с KUMA в командной строке
Параметры задачи Интеграция с Kaspersky Unified Monitoring and Analysis Platform
Управление сертификатами для подключения к серверу KUMA
Настройка параметров использования приложения в режиме Легкого агента
Настройка параметров Легкого агента в Web Console
Настройка параметров Легкого агента в Консоли администрирования
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
Просмотр в командной строке информации об использовании приложения в режиме Легкого агента
Просмотр событий и отчетов
Настройка записи событий в журнал операционной системы
Настройка параметров журнала событий приложения
Просмотр событий в Kaspersky Security Center
Просмотр событий в командной строке
Настройка всплывающих уведомлений в графическом интерфейсе
Управление приложением через графический интерфейс
Графический интерфейс
Включение и выключение компонентов приложения
Запуск и остановка задач проверки
Запуск выборочной проверки и проверки в Sandbox
Запуск и остановка задачи обновления
Настройка использования Kaspersky Security Network
Просмотр отчетов
Просмотр объектов резервного хранилища
Управление лицензионными ключами
Добавление лицензионного ключа
Удаление лицензионного ключа
Просмотр информации о лицензии
Получение временного доступа к устройству
Просмотр информации о приложении
Создание файла трассировки
Проверка целостности компонентов приложения
Обращение в Службу технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Получение информации для Службы технической поддержки
О файлах трассировки приложения
Настройка параметров трассировки приложения
О файлах трассировки плагинов управления приложением

О файлах дампов
Настройка параметров записи дампов
Удаленная диагностика устройства с помощью Kaspersky Security Center
Приложения
Приложение 1. Команды управления Kaspersky Endpoint Security
Команды управления параметрами и задачами приложения
Команды управления общими параметрами приложения
Команды управления параметрами задач
Команды управления задачами
Команды управления запретом запуска объектов
Команды управления общими параметрами проверки контейнеров
Команды управления параметрами проверки сетевого трафика
Команды статистики
Команды вывода событий
Команды управления событиями приложения
Команды управления лицензионными ключами
Команды управления сетевым экраном
Команды управления заблокированными устройствами
Команды управления Контролем устройств
Команды управления Контролем приложений
Команды управления Веб-Контролем
Команды управления резервным хранилищем
Команды управления карантином
Команды управления пользователями и ролями
Команды управления компонентом EDR Expert (on-premise)
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 для защиты виртуальных сред
Команды управления сбором метрик о состоянии системы
Приложение 2. Конфигурационные файлы и параметры приложения по умолчанию
Правила редактирования конфигурационных файлов задач приложения
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)
Общие параметры приложения
Общие параметры проверки контейнеров
Параметры проверки сетевого трафика
Параметры расписания задач
Приложение 3. Коды возврата командной строки
Приложение 4. Настройка совместной работы с Антивирусом Касперского для Linux Mail Server
Приложение 5. Параметры приложения в политике в Web Console
Защита устройств от угроз
Защита от файловых угроз
Защита от атак BadUSB
Проверка съемных дисков
Анализ поведения
Защита от шифрования
Защита от эксплойтов
Защита сетевых соединений и средств коммуникации
Защита от почтовых угроз
Защита от веб-угроз
Защита от сетевых угроз
Сетевой экран
Контроль безопасности
Контроль устройств
Веб-Контроль
Контроль приложений
Контроль целостности системы
Доверенная зона
Общие настройки
Настройки обнаружения
Kaspersky Security Network
Взаимодействие с пользователем
Производительность
Настройки сети
Проверка контейнеров
Служба технической поддержки
Отчеты и хранилище
Интеграция с KSC

Настройки взаимодействия с ОС
Настройки уведомлений
Настройки телеметрии
Встроенные агенты
Managed Detection and Response
Endpoint Detection and Response Optimum
Endpoint Detection and Response Expert (on-premise)
Network Detection and Response (KATA)
Sandbox
Интеграция с KUMA
Режим Легкого агента
Настройки обнаружения SVM
Настройки подключения к Серверу интеграции
Тег для подключения к SVM
Алгоритм выбора SVM
Защита соединения
Приложение 6. Параметры для взаимодействия с внешними службами
Совместная работа с решениями "Лаборатории Касперского"
Kaspersky Security Center Linux
Kaspersky Unified Monitoring and Analysis Platform
Источники информации о Kaspersky Endpoint Security
Глоссарий
SIEM-система
SVM
Активация приложения
Активная политика
Активный ключ
База вредоносных веб-адресов
База фишинговых веб-адресов
Базы приложения
Группа администрирования
Групповая задача
Групповая политика
Доверенное устройство
Зараженный объект
Защита от шифрования
Исключение
Легкий агент
Лечение объектов
Лицензионный сертификат
Лицензия
Ложное срабатывание
Маска файла
Объекты автозапуска
Параметры приложения
Подписка
Политика

Прокси-сервер
Резервный ключ
Сервер администрирования
Сервер интеграции
Серверы обновлений "Лаборатории Касперского"
Информация о стороннем коде
Уведомления о товарных знаках

Справка Kaspersky Endpoint Security 12.4 для Linux

Новые функции

Что нового в версии Kaspersky Endpoint Security 12.4 для Linux

Аппаратные и программные требования

Аппаратные и программные требования для приложения

Сравнение функций

- Сравнение функций приложения в зависимости от лицензии
- Особенности использования приложения в режиме Легкого агента
- Особенности использования приложения в режиме Агента Endpoint Detection and Response

Начало работы

- Краткое руководство по установке и первоначальной настройке приложения через командную строку (приложение используется в стандартном режиме)
- Обновление предыдущей версии приложения
- Подготовка к установке приложения
- Установка и первоначальная настройка приложения
- Обновление баз и модулей приложения в командной строке во время первоначальной настройки
- Обновление баз приложения в командной строке с помощью предустановленной задачи обновления (после первоначальной настройки)
- Подготовка приложения к работе с помощью Kaspersky Security Center

Лицензирование

- Лицензирование приложения
- Активация приложения и управление лицензионными ключами
- Активация приложения во время первоначальной настройки в командной строке
- Активация приложения и управление лицензионными ключами в командной строке (после первоначальной настройки)
- Активация приложения с помощью Kaspersky Security Center

Мониторинг и отчеты

- Просмотр состояния защиты устройства и информации о работе приложения
- Просмотр информации о работе приложения в командной строке
- Просмотр событий и отчетов

Предоставление данных и защита личной информации

- Предоставление данных

Дополнительные возможности

- Настройка параметров использования приложения в режиме Легкого агента
- Настройка дополнительных параметров работы приложения
- Использование Kaspersky Security Network
- Резервное хранилище
- Интеграция с решениями Detection and Response

Оптимизация потребления ресурсов операционной системы

- Оптимизация потребления ресурсов

Обращение в Службу технической поддержки

- Основные шаги диагностики проблем с приложением
- Обращение в Службу технической поддержки

О Kaspersky Endpoint Security 12.4 для Linux

Приложение Kaspersky Endpoint Security 12.4 для Linux (далее также Kaspersky Endpoint Security, приложение) предназначено для защиты устройств под управлением операционных систем Linux® от различного вида угроз, сетевых и мошеннических атак.

Приложение позволяет защищать как физические устройства, так и виртуальные машины. Вы можете использовать приложение Kaspersky Endpoint Security в составе решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.

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.

Основные функции защиты и контроля устройств обеспечиваются следующими функциональными компонентами и задачами приложения:

- **Защита от файловых угроз** позволяет избежать заражения файловой системы устройства пользователя. Компонент *Защита от файловых угроз* запускается автоматически при запуске Kaspersky Endpoint Security и в реальном времени проверяет все открываемые, сохраняемые и запускаемые файлы.

  Вы также можете выполнять проверку защищаемых устройств по требованию с помощью следующих задач проверки:

  - **Поиск вредоносного ПО**. Приложение проверяет на наличие вредоносного ПО объекты файловой системы, расположенные на локальных дисках устройства, а также смонтированные и разделяемые ресурсы, доступ к которым предоставляется по протоколам SMB и NFS. Вы можете использовать эту задачу для полной или выборочной проверки устройства.

  - **Проверка важных областей**. Приложение проверяет загрузочные секторы, объекты автозапуска, память процессов и память ядра.

- **Проверка съемных дисков**. Компонент *Проверка съемных дисков* позволяет в реальном времени контролировать подключение съемных дисков к устройству и проверять съемный диск и его загрузочные секторы на наличие вредоносного ПО. Kaspersky Endpoint Security может проверять следующие съемные диски: CD/DVD-приводы, Blu-ray диски, флеш-накопители (включая USB-модемы), внешние жесткие диски и дискеты.

- **Проверка контейнеров**. Компонент *Мониторинг контейнеров (Проверка контейнеров, Мониторинг контейнеров)* позволяет в реальном времени проверять пространства имен и запущенные контейнеры на наличие вредоносного ПО. Поддерживается интеграция с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc. С помощью задачи *Проверка контейнеров* вы можете выполнять проверку контейнеров и образов по требованию.

- **Защита от веб-угроз**. Компонент *Защита от веб-угроз* позволяет проверять входящий трафик, не допускать загрузки вредоносных файлов из интернета, а также блокировать фишинговые, рекламные и прочие опасные веб-сайты. Kaspersky Endpoint Security может проверять защищенные соединения.

- **Защита от сетевых угроз**. Компонент *Защита от сетевых угроз* позволяет проверять входящий сетевой трафик на действия, характерные для сетевых атак.

- **Управление сетевым экраном**. Компонент *Управление сетевым экраном* позволяет контролировать параметры сетевого экрана операционной системы и фильтровать всю сетевую активность в соответствии с сетевыми пакетными правилами, которые вы настроили.

- **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.

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

- **Защита от шифрования**. Компонент *Защита от шифрования* позволяет проверять обращения удаленных устройств к файлам, расположенным в локальных директориях с сетевым доступом по протоколам SMB/NFS, и защищать файлы от удаленного вредоносного шифрования.

- **Контроль устройств**. Компонент *Контроль устройств* позволяет управлять доступом пользователей к устройствам, которые установлены на клиентском устройстве или подключены к нему (например, жестким дискам, камерам или модулям Wi-Fi). Это позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных. Доступ пользователей к устройствам регулируется с помощью режимов доступа и правил доступа, которые вы настроили.

- **Контроль приложений**. Компонент *Контроль приложений* позволяет управлять запуском приложений на устройствах пользователей. Это снижает риск заражения устройства за счет ограничения доступа к приложениям. Запуск приложений регулируется с помощью правил контроля приложений, которые вы настроили.

- **Инвентаризация**. Задача *Инвентаризация* позволяет получить информацию обо всех исполняемых файлах приложений, хранящихся на клиентских устройствах. Эта информация может быть полезна, например, для создания правил контроля приложений.

- **Веб-Контроль**. Компонент *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.

- **Анализ поведения**. Компонент *Анализ поведения* позволяет контролировать вредоносную активность приложений в операционной системе. При обнаружении вредоносной активности Kaspersky Endpoint Security может завершать процесс приложения, осуществляющего вредоносную активность.

- **Контроль целостности системы** позволяет отслеживать изменения файлов и директорий операционной системы. Компонент *Контроль целостности системы* в реальном времени отслеживает действия, выполняемые с объектами из области мониторинга, указанной в параметрах компонента. С помощью задачи *Проверка целостности системы* вы можете выполнять проверку целостности системы по требованию. Проверка осуществляется путем сравнения текущего состояния объектов, включенных в область мониторинга, с исходным состоянием этих объектов, зафиксированным предварительно в виде снимка состояния системы.

Kaspersky Endpoint Security позволяет обнаруживать зараженные объекты и обезвреживать обнаруженные в них угрозы. При этом приложение может использовать:

- Базы приложения для поиска и лечения зараженных файлов. Во время процесса проверки приложение анализирует каждый файл на наличие угрозы: сравнивает код файла с кодом конкретной угрозы и ищет возможные совпадения.

- Kaspersky Security Network. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложения Kaspersky Endpoint Security на различные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Перед лечением или удалением Kaspersky Endpoint Security сохраняет резервные копии файлов в резервном хранилище, расположенном на устройстве. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете восстановить файл из его копии.

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.

Приложение Kaspersky Endpoint Security может работать в информирующем режиме. *Информирующий режим* – это такой режим работы приложения, при котором в случае обнаружения угрозы компоненты и задачи приложения не пытаются лечить или удалять вредоносные объекты, запрещать доступ или блокировать активность приложений, а только информируют пользователя об обнаружении угрозы.

Kaspersky Endpoint Security поддерживает возможность интеграции с другими решениями "Лаборатории Касперского" для расширения возможностей использования приложения:

- Интеграция с Kaspersky Managed Detection and Response обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.

- Интеграция с Kaspersky Anti Targeted Attack Platform обеспечивает защиту ИТ-инфраструктуры организации и своевременное обнаружение таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats.

- Интеграция с Kaspersky Endpoint Detection and Response Optimum обеспечивает защиту 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.

- Интеграция с Kaspersky Unified Monitoring and Analysis Platform обеспечивает получение, обработку и хранение событий информационной безопасности; анализ и корреляцию данных; поиск по событиям и создание уведомлений о выявлении признаков угроз информационной безопасности.

- Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise) позволяет защититься от большинства киберрисков и покрыть основные сценарии распространения угроз.

Для поддержки приложения в актуальном состоянии предусмотрены дополнительные функции приложения:

- Активация приложения с помощью файла ключа или кода активации.

  Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент).

- Обновление баз и модулей приложения с серверов обновлений "Лаборатории Касперского", через Сервер администрирования или из указанного пользователем источника по расписанию и по требованию.

  Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, приложение получает обновление баз и программных модулей от Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент).

- Разграничение доступа пользователей к функциям приложения в соответствии с ролями пользователей.

- Уведомление администратора о событиях, произошедших во время работы приложения.

- Проверка целостности компонентов приложения с помощью утилиты проверки целостности.

Вы можете управлять приложением Kaspersky Endpoint Security следующими способами:

- С помощью Kaspersky Security Center через Kaspersky Security Center Web Console, Kaspersky Security Center Cloud Console или Консоль администрирования.

- С помощью команд управления из командной строки.

- С помощью графического пользовательского интерфейса.

  Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, для управления приложением требуется Kaspersky Security Center. Управление приложением с помощью Kaspersky Security Center Cloud Console и графического пользовательского интерфейса недоступно.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

О режимах использования приложения Kaspersky Endpoint Security

Вы можете использовать Kaspersky Endpoint Security в одном из следующих режимов:

- В стандартном режиме для защиты рабочих станций и серверов (далее также "Стандартный режим"). Kaspersky Endpoint Security используется как автономное приложение для защиты устройств под управлением операционных систем Linux.
- В режиме Легкого агента для защиты виртуальных сред в составе решения Kaspersky Security для виртуальных сред Легкий агент (далее также "режим Легкого агента"). Kaspersky Endpoint Security используется как компонент Легкий агент решения Kaspersky Security для виртуальных сред Легкий агент для защиты виртуальных машин с гостевыми операционными системами Linux.
- 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 (далее также "режим Агента Endpoint Detection and Response").

Приложение может одновременно использоваться только в одном режиме.

По умолчанию приложение используется в стандартном режиме.

Использование приложения в режиме Легкого агента

Если вы хотите использовать приложение в режиме Легкого агента, вам нужно выполнить следующие действия:

1. Выполнить установку приложения Kaspersky Endpoint Security в режиме Легкого агента на каждой виртуальной машине, которую требуется защищать с помощью решения Kaspersky Security для виртуальных сред Легкий агент. Вы также можете установить приложение на шаблоне виртуальных машин.

   Перед началом установки приложения требуется установить Агент администрирования Kaspersky Security Center на виртуальные машины и шаблоны виртуальных машин.

   В ходе установки вам нужно указать, что приложение будет использоваться в режиме Легкого агента, одним из следующих способов:

   - во время первоначальной настройки приложения в интерактивном или автоматическом режиме (в случае установки с помощью командной строки);
   - в свойствах инсталляционного пакета приложения или в конфигурационном файле autoinstall.ini, который включен в инсталляционный пакет (в случае установки с помощью Kaspersky Security Center).

   После установки Kaspersky Endpoint Security изменить режим использования приложения невозможно.

При выборе режима Легкого агента вы также можете настроить следующие параметры работы Kaspersky Endpoint Security в режиме Легкого агента:

- Роль виртуальной машины, которую вы хотите защищать, в виртуальной инфраструктуре: сервер или рабочая станция. Роль виртуальной машины определяет, по какой лицензии будет использоваться приложение на этой виртуальной машине, и объем доступной функциональности.

- Режим защиты инфраструктуры VDI. Рекомендуется включить этот режим, если вы устанавливаете приложение на шаблон виртуальных машин, из которого будут создаваться временные виртуальные машины. Режим защиты инфраструктуры VDI позволяет оптимизировать работу Kaspersky Endpoint Security на временных виртуальных машинах.

2. Настроить параметры подключения Легкого агента к SVM и параметры подключения Легкого агента к Серверу интеграции.

   Kaspersky Endpoint Security в режиме Легкого агента взаимодействует с другими компонентами решения Kaspersky Security для виртуальных сред Легкий агент: Сервером интеграции и Сервером защиты, установленным на SVM (см. подробнее в справке решения Kaspersky Security для виртуальных сред Легкий агент). Для взаимодействия с Сервером защиты Kaspersky Endpoint Security устанавливает и поддерживает подключение к SVM, на которой установлен этот Сервер защиты.

   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.

   Вы можете настроить параметры подключения в свойствах политики Kaspersky Endpoint Security с помощью Консоли администрирования Kaspersky Security Center или с помощью Kaspersky Security Center Web Console.

Информацию о параметрах работы приложения в режиме Легкого агента, о подключении к Серверу интеграции и к SVM вы можете получить с помощью команд приложения:

- `kesl-control --ksvla-info`

- `kesl-control --viis-info`

- `kesl-control --svm-info`

Информация о режиме использования приложения отображается в Kaspersky Security Center в свойствах приложения Kaspersky Endpoint Security на управляемом устройстве в разделе **Компоненты**. Информация отображается в строке **Режим Легкого агента для защиты виртуальных сред** следующим образом:

- статус *выполняется* означает, что приложение используется в режиме Легкого агента;

- статус *не установлено* означает, что приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response.

Об активации приложения в режиме Легкого агента

Если Kaspersky Endpoint Security используется в режиме Легкого агента, отдельно активировать приложение не требуется. Вы активируете одновременно все компоненты решения Kaspersky Security для виртуальных сред Легкий агент. Активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионного ключа на SVM. См. подробнее в справке Kaspersky Security для виртуальных сред Легкий агент.

Основная лицензия Kaspersky Security для виртуальных сред Легкий агент может не включать в себя дополнительную функциональность приложения Kaspersky Endpoint Security (например, функциональность интеграции с решениями Detection and Response от "Лаборатории Касперского"). В этом случае на SVM также требуется добавить лицензионный ключ для активации нужной дополнительной функциональности.

После активации решения и подключения Легкого агента к SVM компонент Сервер защиты передает информацию о лицензии Легкому агенту. При выборе SVM для подключения Легкий агент учитывает среди прочих параметров тип лицензионного ключа, добавленного на SVM. Легкий агент не подключается к SVM, если тип ключа, добавленного на SVM, не соответствует роли защищенной виртуальной машины в виртуальной инфраструктуре (сервер или рабочая станция). Подробнее об особенностях подключения Легкого агента к SVM см. в справке Kaspersky Security для виртуальных сред Легкий агент.

Информацию о лицензии, по которой используется Легкий агент для Linux, вы можете посмотреть удаленно с помощью Kaspersky Security Center или на защищенной виртуальной машине с Легким агентом с помощью командной строки.

Не поддерживается управление лицензионными ключами с помощью задачи Kaspersky Endpoint Security *Добавление ключа* и с помощью команд Kaspersky Endpoint Security для добавления и удаления лицензионных ключей.

Об обновлении баз и модулей приложения в режиме Легкого агента

Kaspersky Endpoint Security в режиме Легкого агента использует специальные базы вредоносного ПО, необходимые для работы приложения в составе решения Kaspersky Security для виртуальных сред Легкий агент. Kaspersky Endpoint Security получает от Сервера защиты обновления баз и программных модулей. См. подробнее в справке Kaspersky Security для виртуальных сред Легкий агент.

Обновление баз и программных модулей на защищенных виртуальных машинах выполняется с помощью специальной локальной задачи приложения Kaspersky Endpoint Security *Обновление*, в которой в качестве источника обновлений указана папка на SVM. Задача обновления запускается автоматически. Вы не можете удалять эту задачу и изменять ее параметры.

Не поддерживается обновление из источников, отличных от папки на SVM, и использование групповых задач обновления.

Откат последнего обновления баз вредоносного ПО также выполняется на стороне Сервера защиты. После отката обновления баз и программных модулей на SVM на защищенной виртуальной машине автоматически запускается специальная локальная задача *Обновление*. В результате выполнения задачи Легкий агент возвращается к использованию предыдущего набора баз вредоносного ПО.

Не поддерживается использование локальной и групповой задачи приложения Kaspersky Endpoint Security *Откат обновления баз*.

Другие 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.

Использование приложения в режиме Агента Endpoint Detection and Response

Приложение Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response позволяет использовать функциональность решений Detection and Response от "Лаборатории Касперского" для защиты устройств, на которых установлены антивирусные приложения от стороннего поставщика.

В режиме Агента Endpoint Detection and Response стандартные компоненты защиты и контроля Kaspersky Endpoint Security не используются для защиты устройства. Стандартную защиту устройства обеспечивает стороннее антивирусное приложение. Приложение Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response осуществляет постоянное наблюдение за процессами, запущенными на устройстве, открытыми сетевыми соединениями и изменяемыми файлами и обеспечивает интеграцию со следующими решениями Detection and Response:

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

Приложение Kaspersky Endpoint Security для Linux версии 12.4 может работать совместно с антивирусным приложением Dr. Web. Вы можете установить Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response на устройстве, где установлено приложение Dr. Web.

Приложения следует устанавливать в следующем порядке: сначала установите стороннее антивирусное приложение, затем Агент администрирования Kaspersky Security Center, затем приложение Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response. Это связано с тем, что установщик стороннего приложения может определить приложения "Лаборатории Касперского" как несовместимое ПО и удалить их. После обновления стороннего приложения на устройстве рекомендуется проверять работоспособность Kaspersky Endpoint Security и Агента администрирования, так как установщик стороннего приложения повторно проверяет устройство на несовместимое ПО и может удалить приложения "Лаборатории Касперского".

Настройка приложения в режиме Агента Endpoint Detection and Response

Если вы хотите использовать приложение Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response, вам нужно выполнить следующие действия:

1. Выполнить установку приложения Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response на каждой виртуальной машине, которую требуется защищать.

   Вы можете посмотреть информацию о режиме использования приложения с помощью командной строки, выполнив команду `kesl-control --app-info`.

2. Активировать приложение. Вам нужно добавить в приложение отдельный лицензионный ключ "Kaspersky Endpoint Detection and Response Expert (on-premise) Add-on" (далее также "ключ EDR Expert (on-premise)").

   > Для активации приложения в режиме Агента Endpoint Detection and Response нужен только ключ для дополнительной функциональности. Основной лицензионный ключ добавлять в приложение не нужно.

3. Включить интеграцию с решениями Detection and Response, которые вы хотите использовать для защиты устройства:

   - Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) на платформе OSMP вам нужно включить компонент EDR Expert (on-premise) и настроить параметры интеграции в Kaspersky Security Center Web Console или в командной строке.
   - Для интеграции с Kaspersky Endpoint Detection and Response на платформе Kaspersky Anti Targeted Attack Platform вам нужно включить компонент EDR Expert (on-premise) и настроить параметры интеграции в Kaspersky Security Center Web Console, в Консоли администрирования или в командной строке.
   - Для интеграции с Kaspersky Network Detection and Response на платформе Kaspersky Anti Targeted Attack Platform вам нужно включить компонент NDR (KATA) и настроить параметры интеграции в Kaspersky Security Center Web Console, в Консоли администрирования или в командной строке.

   Вы можете проверить статус работы компонентов EDR Expert (on-premise) и NDR (KATA):

   - В свойствах устройства в Web Console (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → **Общие** → **Компоненты**).
   - С помощью командной строки, выполнив команду `kesl-control --app-info`.

Особенности работы приложения в режиме Агента Endpoint Detection and Response

Если приложение Kaspersky Endpoint Security используется в режиме Агента Endpoint Detection and Response, набор доступных компонентов и задач приложения ограничен. После установки параметры приложения настроены следующим образом:

- Полностью доступны для управления компоненты, обеспечивающие интеграцию с решениями Detection and Response:
  - EDR Expert (on-premise).
  - NDR (KATA).

  Компоненты выключены по умолчанию, вам нужно их включить для работы приложения в режиме Агента Endpoint Detection and Response. 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 недоступен для изменения.
- 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 недоступны для изменения:
  - 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-premise) 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.

Комплект поставки

На веб-сайте "Лаборатории Касперского" вы можете скачать файлы, которые входят в комплект поставки приложения Kaspersky Endpoint Security, а также файлы, используемые в процедуре удаленной установки приложения с помощью Kaspersky Security Center.

В комплект поставки приложения Kaspersky Endpoint Security входят следующие файлы:

- kesl-12.4.0-<номер сборки>.i386.rpm, kesl_12.4.0-<номер сборки>_i386.deb

  Содержат основные файлы приложения. Пакеты могут быть установлены на 32-битные операционные системы в соответствии с типом менеджера пакетов.

- kesl-12.4.0-<номер сборки>.x86_64.rpm, kesl_12.4.0-<номер сборки>_amd64.deb

  Содержат основные файлы приложения. Пакеты могут быть установлены на 64-битные операционные системы в соответствии с типом менеджера пакетов.

- kesl-12.4.0-<номер сборки>.aarch64.rpm, kesl_12.4.0-<номер сборки>_arm64.deb

  Содержат основные файлы приложения. Пакеты могут быть установлены на 64-битные операционные системы для архитектуры Arm® в соответствии с типом менеджера пакетов.

- kesl-gui-12.4.0-<номер сборки>.i386.rpm, kesl-gui_12.4.0-<номер сборки>_i386.deb

  Содержат файлы графического интерфейса приложения. Пакеты могут быть установлены на 32-битные операционные системы в соответствии с типом менеджера пакетов.

- kesl-gui-12.4.0-<номер сборки>.x86_64.rpm, kesl-gui_12.4.0-<номер сборки>_amd64.deb

  Содержат файлы графического интерфейса приложения. Пакеты могут быть установлены на 64-битные операционные системы в соответствии с типом менеджера пакетов.

- kesl-gui-12.4.0-<номер сборки>.aarch64.rpm, kesl-gui_12.4.0-<номер сборки>_arm64.deb

  Содержат файлы графического интерфейса приложения. Пакеты могут быть установлены на 64-битные операционные системы для архитектуры Arm в соответствии с типом менеджера пакетов.

- kesl-12.4.0.<номер сборки>.zip

  Содержит файлы, используемые в процедуре удаленной установки приложения с помощью Kaspersky Security Center, включая файлы license.<идентификатор языка> и ksn_license.<идентификатор языка>.

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

- ksn_license.<идентификатор языка>

  Содержит текст Положения о Kaspersky Security Network.

- license.<идентификатор языка>

  Содержит текст Лицензионного соглашения. В Лицензионном соглашении указано, на каких условиях вы можете пользоваться приложением.

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.

Аппаратные и программные требования

Этот раздел содержит аппаратные и программные требования приложения Kaspersky Endpoint Security.

Аппаратные требования

Приложение Kaspersky Endpoint Security имеет следующие аппаратные требования:

Минимальные аппаратные требования

- Процессор с архитектурой AMD64, частотой 2 ГГц или выше, имеющий два или более ядер, поддерживающий инструкции SSE2.
- Раздел подкачки не менее 1 ГБ.
- 2 ГБ оперативной памяти, доступной для приложения, для 64-битных операционных систем (1 ГБ оперативной памяти, доступной для приложения, для 32-битных операционных систем).
- 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.

- При использовании графического интерфейса монитор должен обеспечивать отображение окон шириной 1000 пикселей и высотой 600 пикселей (если применяется масштабирование экрана, то эти размеры также масштабируются).

- Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, требуется виртуализированный сетевой интерфейс с полосой пропускания 100 Мбит/сек.

Минимальные аппаратные требования для архитектуры Arm

- 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.

- При использовании графического интерфейса монитор должен обеспечивать отображение окон шириной 1000 пикселей и высотой 600 пикселей (если применяется масштабирование экрана, то эти размеры также масштабируются).

Использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред не поддерживается на операционных системах для архитектуры Arm.

Программные требования

Для установки Kaspersky Endpoint Security на устройстве должна быть установлена одна из следующих операционных систем:

- 32-битные операционные системы:

  - Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12.

- 64-битные операционные системы:
  - 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).
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 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).

    На устройствах с операционными системами Astra Linux в режимах мандатного разграничения доступа и замкнутой программной среды не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

Работа операционной системы Astra на планшетном компьютере (планшете) в режиме "Мобильный" поддерживается только в десктопном виде.

- CentOS 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- CentOS Stream 8.
- CentOS Stream 9.
- CentOS Stream 10.
- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12.
- Debian GNU/Linux 13.0, 13.1, 13.2.
- 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.
- 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.
- SberOS 3.4.0, 3.5.0.
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7.
- SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7.
- Ubuntu® 22.04 LTS.
- Ubuntu 24.04 LTS.
- Альт Образование 10.
- Альт Образование 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.

- М ОС 12 Сервер release 2021.1.
- Мос ОС 15.5 Arbat.
- МСВСфера 9.4 АРМ.
- МСВСфера 9.4 Сервер.
- ОС МЭШ 12 Для всех пользователей (без телеметрии и без поддержки ДИТ) release 2021.1.
- ОС МЭШ 12 Для московских школ для интерактивных панелей (с телеметрией и поддержкой ДИТ) release 2021.1.
- ОС МЭШ 12 Для московских школ для компьютеров и ноутбуков (с телеметрией и поддержкой ДИТ) release 2021.1.
- ОСнова 2.14.
- ОСнова 3.0.5.
- 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.

- 64-битные операционные системы для архитектуры Arm:
  - 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 22.04 LTS.
  - Альт СП Рабочая Станция релиз 10.
  - Альт СП Сервер релиз 10.
  - РЕД ОС 8.0.

На устройствах с операционными системами для архитектуры Arm не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

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

Дополнительные программные 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 6.4. Вы можете посмотреть требования к виртуальным инфраструктурам для работы приложения в режиме Легкого агента в справке Kaspersky Security для виртуальных сред Легкий агент.

К виртуальным машинам, на которых устанавливается Kaspersky Endpoint Security в режиме Легкого агента, применяются программные и аппаратные требования приложения Kaspersky Endpoint Security с указанными ограничениями.

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

На виртуальных машинах, которые вы хотите защищать, должны быть установлены следующие пакеты, в зависимости от виртуальной инфраструктуры, в которой развернуто решение Kaspersky Security для виртуальных сред Легкий агент:

- В инфраструктуре Microsoft Hyper-V на виртуальных машинах должен быть установлен пакет служб интеграции (Integration Services).
- В инфраструктуре VMware vSphere на виртуальных машинах должен быть установлен пакет VMware Tools.
- В инфраструктуре XenServer на виртуальных машинах должна быть установлена программа XenTools.
- В инфраструктуре HUAWEI FusionSphere на виртуальных машинах должен быть установлен пакет HUAWEI Tools.
- В инфраструктуре KVM, OpenStack, Private Cloud от VK, Облачная платформа ТИОНИКС, Astra Linux, Альт Сервер Виртуализации, Базис.DynamiX и Базис Dynamix Standard на виртуальных машинах должен быть установлен QEMU Guest Agent.

Поддерживаемые версии Kaspersky Security Center

Приложение Kaspersky Endpoint Security совместимо с приложением Kaspersky Security Center следующих версий:

- Kaspersky Security Center Windows 14, 14.2, 15.1. Поддерживается управление приложением Kaspersky Endpoint Security 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. Поддерживается управление приложением Kaspersky Endpoint Security через Kaspersky Security Center Web Console с помощью веб-плагина управления.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент), для управления приложением рекомендуется использовать Kaspersky Security Center следующих версий:

- Kaspersky Security Center Windows 14.2, 15.1.
- Kaspersky Security Center 15.4, 16.0, 16.1, 16.2.

Для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center требуется Агент администрирования Kaspersky Security Center.

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

Если вы используете интеграцию приложения с компонентом Kaspersky Endpoint Detection and Response платформы Kaspersky Anti Targeted Attack Platform, для управления приложением рекомендуется использовать Kaspersky Security Center следующих версий:

- Kaspersky Security Center Windows 14.2, 15.1.
- Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.

Если вы используете интеграцию приложения с компонентом Kaspersky Endpoint Detection and Response Optimum, для управления приложением рекомендуется использовать Kaspersky Security Center следующих версий:

- Kaspersky Security Center Windows 15.1.
- Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.

Поддерживаемые версии решений на платформах KATA и OSMP

Приложение Kaspersky Endpoint Security совместимо с решениями на платформе Kaspersky Anti Targeted Attack Platform следующих версий:

- Kaspersky Anti Targeted Attack Platform 6.0 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA) и Sandbox).
- Kaspersky Anti Targeted Attack Platform 6.1 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA) и Sandbox).
- Kaspersky Anti Targeted Attack Platform 7.0 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA) и Sandbox).
- Kaspersky Anti Targeted Attack Platform 7.1 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA) и Sandbox).
- Kaspersky Anti Targeted Attack Platform 8.0 (Kaspersky Network Detection and Response (KATA) и Sandbox).

Подробнее о решении Kaspersky Anti Targeted Attack Platform см. в справке Kaspersky Anti Targeted Attack Platform.

Приложение Kaspersky Endpoint Security совместимо с решением Kaspersky Endpoint Detection and Response Expert (on-premise) 8.0 на платформе Open Single Management Platform (далее также OSMP).

Подробнее о решении Kaspersky Endpoint Detection and Response Expert (on-premise) 8.0 см. в справке Kaspersky Endpoint Detection and Response Expert (on-premise).

Что нового

В приложении Kaspersky Endpoint Security 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 (OSMP). Компонент также обеспечивает интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premise). Задача интеграции переименована в *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise)* (KATAEDR, ID:24).

- Реализована возможность интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) – решением для кибербезопасности бизнеса, позволяющим защититься от большинства киберрисков и покрыть основные сценарии распространения угроз. Компоненты Kaspersky Endpoint Detection and Response Expert (on-premise) развертываются на единой платформе управления Open Single Management Platform (OSMP). Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise) 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 (OSMP), обеспечивающего интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise)* 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.

Исправленные ошибки

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

Список ошибок, исправленных в веб-плагине 12.4.0.8289

Идентификатор	Описание
10724878	При применении политики к устройству для настройки `InterceptorApplyStrategy` использовалось значение `RestartServiceManually` вместо значения по умолчанию `RestartServiceAutomatically`.
10779263	В политике или профиле политики, созданных в Консоли администрирования, невозможно сохранить изменения, внесенные через Web Console.

Подготовка к установке приложения Kaspersky Endpoint Security

Общие действия

Перед началом установки приложения Kaspersky Endpoint Security вам нужно выполнить следующие действия:

- Проверить соответствие вашего устройства аппаратным и программным требованиям приложения.
- Убедиться в том, что на вашем устройстве не установлено стороннее антивирусное программное обеспечение.
- Убедиться в том, что на вашем устройстве не установлено приложение Kaspersky Endpoint Agent для Linux. Если приложение Kaspersky Endpoint Agent для Linux установлено, во время установки отобразится сообщение о необходимости удалить его вручную.
- Если вы планируете управлять приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, выполнить подготовительные действия для установки Агента администрирования Kaspersky Security Center на устройстве (подробнее см. в справке Kaspersky Security Center).

  Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, для управления приложением требуется Kaspersky Security Center.

- Если вы хотите использовать систему контроля доступа SELinux, вам нужно убедиться в том, что в операционной системе установлена утилита semanage. Если утилита не установлена, установите пакет policycoreutils-python или policycoreutils-python-utils в зависимости от типа менеджера пакетов.
- Если вы хотите использовать графический пользовательский интерфейс, вам нужно убедиться в том, что на вашем устройстве доступны необходимые зависимости для установки пакета графического интерфейса. Если устройство находится в закрытом сетевом контуре и не имеет доступа к репозиториям пакетного менеджера, рекомендуется проверить перечень зависимостей на эталонном устройстве (libice6, libsm6, libx11-6, libx11-xcb1, libxcb-icccm4, libxcb-image0, libxcb-keysyms1, libxcb-randr0, libxcb-render-util0, libxcb-render0, libxcb-shape0, libxcb-shm0, libxcb-sync1, libxcb-xfixes0, libxcb-xinerama0, libxcb-xkb1, libxcb1, libxi6, libxml2, zlib1g), затем скачать и распространить пакеты на все устройства перед установкой графического интерфейса.
- Если вы хотите использовать графический пользовательский интерфейс, вам нужно убедиться в том, что в операционной системе установлена утилита Zenity.
- На устройствах с операционными системами, не поддерживающими технологию fanotify, убедиться в том, что 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.
- На устройстве с операционной системой SUSE Linux Enterprise Server 15 установить пакет insserv-compat.

- 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 отключить 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**).

  Вы можете включить запрет трассировки ptrace, указав значение параметра ядра `kernel.yama.ptrace_scope=3`. Тогда в работе приложения произойдет следующее:

  - Невозможно будет создавать файлы дампа процесса kesl при падении приложения.
  - Компонент Анализ поведения не сможет получать параметры окружения процессов.
  - На операционных системах с версией ядра выше 5.7 компонент Контроль приложений не сможет 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 сможет нормально работать.
  - Не будет работать проверка памяти процессов и памяти ядра в задачах проверки, так как запрещено чтение /proc/pid/mem.
  - Не гарантируется YARA-проверка памяти процессов в режиме мандатного разграничения доступа, так как запрещено чтение /proc/pid/mem.

- Для работы компонентов Управление сетевым экраном, Защита от веб-угроз и Защита от сетевых угроз требуется установить на вашем устройстве пакет утилит iptables.
- Для работы MMC-плагина управления Kaspersky Endpoint Security на устройстве, где установлен Сервер администрирования Kaspersky Security Center, требуется установить Microsoft® Visual C++® 2015 Redistributable Update 3 RC (см. https://www.microsoft.com/ru-ru/download/details.aspx?id=52685).
- Для запуска и корректной работы приложения требуется убедиться, что учетная запись root является владельцем следующих директорий и только владелец имеет право на запись в них: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.
- Убедиться, что в операционной системе настроены ограничения на файловые дескрипторы, рекомендованные производителем операционной системы. Для проверки ограничения запустите команду `cat /proc/sys/fs/file-max`. При работе приложения потребление дескрипторов в операционной системе может существенно увеличиться. В общем случае рекомендуется выключить ограничение на количество файлов, указав в файле /etc/sysctl.conf значение параметра `fs.file-max=9223372036854775807`. После изменения значения этого параметра требуется перезагрузить операционную систему.

Дополнительные действия перед установкой Kaspersky Endpoint Security в режиме Легкого агента

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент), вам нужно дополнительно выполнить следующие действия перед началом установки приложения Kaspersky Endpoint Security:

- Убедиться в том, что виртуальные машины, которые вы хотите защищать, соответствуют общим требованиям для режима Легкого агента.

- Убедиться 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.

Установка и первоначальная настройка приложения Kaspersky Endpoint Security

Перед началом установки приложения Kaspersky Endpoint Security требуется выполнить подготовку к установке.

Сценарии ниже описывают установку и первоначальную настройку приложения Kaspersky Endpoint Security, а также установку Агента администрирования Kaspersky Security Center и плагинов управления Kaspersky Endpoint Security. Сценарий установки зависит от режима, в котором вы планируете использовать приложение Kaspersky Endpoint Security.

После установки Kaspersky Endpoint Security изменить режим использования приложения невозможно.

Стандартный режим

Если вы планируете использовать приложение Kaspersky Endpoint Security в стандартном режиме, процедура установки приложения состоит из следующих этапов:

1. **Установка и первоначальная настройка Агента администрирования**

   Если вы планируете управлять приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, установите на защищаемом устройстве Агент администрирования Kaspersky Security Center и настройте его параметры.

2. **Установка плагина управления Kaspersky Endpoint Security**

   Если вы планируете управлять приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, установите плагин управления Kaspersky Endpoint Security. В зависимости от консоли управления Kaspersky Security Center используются следующие плагины управления:

   - Веб-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console. Веб-плагин устанавливается на устройстве с установленным приложением Kaspersky Security Center Web Console.
   - 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.

3. **Установка пакетов приложения и графического пользовательского интерфейса**

   Приложение Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM. Предусмотрены отдельные пакеты для приложения и графического интерфейса приложения. Установите Kaspersky Endpoint Security и, если требуется, графический интерфейс из пакетов нужного формата.

   Вы можете выполнить установку одним из следующих способов:

   - С помощью Kaspersky Security Center.
   - С помощью командной строки.

4. **Первоначальная настройка Kaspersky Endpoint Security**

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

Если вы установили приложение Kaspersky Endpoint Security с помощью Kaspersky Security Center, первоначальная настройка была выполнена автоматически во время установки в соответствии с параметрами, указанными в инсталляционном пакете. После завершения установки выполните подготовку приложения к работе.

Если вы установили приложение Kaspersky Endpoint Security с помощью командной строки, после завершения установки запустите мастер первоначальной настройки и выполните первоначальную настройку приложения в интерактивном режиме или в автоматическом режиме.

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

Режим Легкого агента

Не поддерживается использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред на операционных системах для архитектуры Arm.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, процедура установки приложения состоит из следующих этапов:

1. **Установка и первоначальная настройка Агента администрирования**

   Установите на виртуальные машины и шаблоны виртуальных машин Агент администрирования Kaspersky Security Center и настройте его параметры.

   Если вы устанавливаете Агент администрирования на шаблон, из которого будут создаваться временные виртуальные машины, рекомендуется настроить параметры, которые позволяют оптимизировать работу на временных виртуальных машинах. Подробнее об установке на шаблон виртуальных машин см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

2. **Установка плагина управления Kaspersky Endpoint Security**

   Установите плагин управления Kaspersky Endpoint Security. В зависимости от консоли управления Kaspersky Security Center используются следующие плагины управления:

   - Веб-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console. Веб-плагин устанавливается на устройство с установленным приложением Kaspersky Security Center Web Console.
   - 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.

3. **Установка пакетов приложения и первоначальная настройка Kaspersky Endpoint Security**

   Приложение Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM. Установите Kaspersky Endpoint Security из пакета нужного формата. Предусмотрены отдельные пакеты для приложения и графического интерфейса приложения.

Графический интерфейс приложения не поддерживается, если Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Вы можете выполнить установку приложения одним из следующих способов:

- С помощью Kaspersky Security Center.

  Перед началом установки вам нужно указать параметры первоначальной настройки приложения в параметрах инсталляционного пакета или в конфигурационном файле, который включен в инсталляционный пакет.

  Вам нужно выбрать режим Легкого агента (в конфигурационном файле – параметр `KSVLA_MODE=Yes`). Если вы устанавливаете Kaspersky Endpoint Security на шаблон, из которого будут создаваться временные виртуальные машины, рекомендуется также включить режим защиты инфраструктуры VDI для оптимизации работы приложения на временных виртуальных машинах (в конфигурационном файле – параметр `VDI_MODE=Yes`).

  Значения параметров чувствительны к регистру.

- С помощью командной строки. В случае установки с помощью командной строки выбор режима использования приложения выполняется во время первоначальной настройки приложения в интерактивном или автоматическом режиме.

4. **Первоначальная настройка Kaspersky Endpoint Security**

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

Если вы установили приложение Kaspersky Endpoint Security с помощью Kaspersky Security Center, первоначальная настройка была выполнена автоматически во время установки в соответствии с параметрами, указанными в инсталляционном пакете. После завершения установки выполните подготовку приложения к работе.

Если вы установили приложение Kaspersky Endpoint Security с помощью командной строки, после завершения установки запустите мастер первоначальной настройки и выполните первоначальную настройку приложения в интерактивном режиме или в автоматическом режиме. Во время первоначальной настройки вам нужно выбрать режим Легкого агента одним из следующих способов:

- Ввести `yes` на шаге "Использование приложения в режиме Легкого агента" в мастере первоначальной настройки.

- Задать в конфигурационном файле первоначальной настройки параметр `KSVLA_MODE=Yes`.

  Значение параметра чувствительно к регистру.

Если вы устанавливаете приложение Kaspersky Endpoint Security на шаблон, из которого будут создаваться временные виртуальные машины, рекомендуется также настроить параметр, который позволяет оптимизировать работу на временных виртуальных машинах. Подробнее об установке на шаблон виртуальных машин см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

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

Режим Агента Endpoint Detection and Response

Рекомендуется выполнять установку после установки на устройстве сторонних антивирусных приложений.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response, процедура установки приложения состоит из следующих этапов:

1. **Установка и первоначальная настройка Агента администрирования**

   Если вы планируете управлять приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, установите на защищаемом устройстве Агент администрирования Kaspersky Security Center и настройте его параметры.

2. **Установка плагина управления Kaspersky Endpoint Security**

   Если вы планируете управлять приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, установите плагин управления Kaspersky Endpoint Security. В зависимости от консоли управления Kaspersky Security Center используются следующие плагины управления:

   - Веб-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console. Веб-плагин устанавливается на устройство с установленным приложением Kaspersky Security Center Web Console.
   - 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.

3. **Установка пакетов приложения и первоначальная настройка Kaspersky Endpoint Security**

   Приложение Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM. Установите Kaspersky Endpoint Security из пакета нужного формата. Предусмотрены отдельные пакеты для приложения и графического интерфейса приложения.

   Вы можете выполнить установку приложения одним из следующих способов:

   - С помощью Kaspersky Security Center.

     Перед началом установки вам нужно указать параметры первоначальной настройки приложения в параметрах инсталляционного пакета или в конфигурационном файле, который включен в инсталляционный пакет.

     Вам нужно выбрать режим Агента Endpoint Detection and Response (в конфигурационном файле – параметр `ENDPOINT_AGENT_MODE=Yes`).

     Значение параметра чувствительно к регистру.

   - С помощью командной строки. В случае установки с помощью командной строки выбор режима использования приложения выполняется во время первоначальной настройки приложения в интерактивном или автоматическом режиме.

4. **Первоначальная настройка Kaspersky Endpoint Security**

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

Если вы установили приложение Kaspersky Endpoint Security с помощью Kaspersky Security Center, первоначальная настройка была выполнена автоматически во время установки в соответствии с параметрами, указанными в инсталляционном пакете. После завершения установки выполните подготовку приложения к работе.

Если вы установили приложение Kaspersky Endpoint Security с помощью командной строки, после завершения установки запустите мастер первоначальной настройки и выполните первоначальную настройку приложения в интерактивном режиме или в автоматическом режиме. Во время первоначальной настройки вам нужно выбрать режим Агента Endpoint Detection and Response одним из следующих способов:

- Ввести `yes` на шаге "Использование приложения в режиме Агента Endpoint Detection and Response" в мастере первоначальной настройки.
- Задать в конфигурационном файле первоначальной настройки параметр `ENDPOINT_AGENT_MODE=Yes`.

  Значение параметра чувствительно к регистру.

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

Установка и первоначальная настройка Агента администрирования Kaspersky Security Center

Агент администрирования обеспечивает связь клиентского устройства с Сервером администрирования Kaspersky Security Center. Поэтому его требуется установить на каждое клиентское устройство, которое будет подключено к системе удаленного централизованного управления Kaspersky Security Center.

Перед началом установки Агента администрирования на устройства с операционными системами Linux требуется выполнить подготовительные действия. Описание подготовки устройств к установке Агента администрирования см. в справке Kaspersky Security Center. Набор необходимых действий зависит от операционной системы.

Вы можете выполнить установку и первоначальную настройку Агента администрирования:

- Удаленно с рабочего места администратора с помощью Kaspersky Security Center Web Console или Консоли администрирования. Для удаленной установки используется инсталляционный пакет Агента администрирования.
- С помощью командной строки:
  - В тихом режиме с файлом ответов. Файл ответов – это текстовый файл, который содержит пользовательский набор параметров установки и первоначальной настройки Агента администрирования. Описание параметров установки и первоначальной настройки Агента администрирования см. в справке Kaspersky Security Center (раздел "Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)").
  - В интерактивном режиме из пакета формата RPM или DEB в соответствии с типом менеджера пакетов. В этом случае после установки вам нужно выполнить первоначальную настройку Агента администрирования с помощью скрипта.

Подробнее об установке Агента администрирования см. в справке Kaspersky Security Center.

Установка плагинов управления Kaspersky Endpoint Security

Для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center используются следующие плагины управления Kaspersky Endpoint Security:

- веб-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console;
- MMC-плагин управления Kaspersky Endpoint Security позволяет управлять работой приложения через Консоль администрирования Kaspersky Security Center.

Вы можете одновременно 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.

Если для управления приложением вы используете Консоль администрирования Kaspersky Security Center, вы можете также конвертировать политики и задачи, созданные с помощью предыдущих версий плагина управления, в новые версии.

Установка веб-плагина Kaspersky Endpoint Security

Веб-плагин управления Kaspersky Endpoint Security требуется установить на устройство с установленным приложением Kaspersky Security Center Web Console. При этом функции веб-плагина доступны всем администраторам, у которых есть доступ к Kaspersky Security Center Web Console в браузере.

Вы можете установить веб-плагин следующими способами:

- 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 загрузит необходимые обновления для них. Дополнительная информация о мастере первоначальной настройки Kaspersky Security Center Web Console приведена в справке Kaspersky Security Center.

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

Чтобы установить веб-плагин Kaspersky Endpoint Security вручную:

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

   Откроется список установленных веб-плагинов.

2. Запустите установку веб-плагина Kaspersky Endpoint Security одним из следующих способов:

- Установка из списка веб-плагинов "Лаборатории Касперского":

  a. Нажмите на кнопку **Добавить**.

  Откроется список всех доступных веб-плагинов "Лаборатории Касперского". Список обновляется автоматически после выпуска новых версий веб-плагинов.

  b. Найдите в списке веб-плагин **Kaspersky Endpoint Security <номер версии> для Linux** и нажмите на его название.

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

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

  e. Откроется окно **Настройка веб-плагина**.

  > В версии Kaspersky Security Center Web Console 14.2 требуется обновить страницу браузера, чтобы открылось окно **Настройка веб-плагина**.

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

- Установка веб-плагина из стороннего источника (архивы, необходимые для установки веб-плагинов, входят в комплект поставки, вы также можете скачать их на веб-сайте "Лаборатории Касперского"):

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

  b. В открывшемся окне укажите путь к ZIP-архиву с дистрибутивом веб-плагина и путь к файлу с подписью в формате TXT. Этот файл находится в архиве с веб-плагином.

  c. Нажмите на кнопку **Добавить**.

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

  e. Откроется окно **Настройка веб-плагина**.

  > В версии Kaspersky Security Center Web Console 14.2 требуется обновить страницу браузера, чтобы открылось окно **Настройка веб-плагина**.

  f. 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.

Установка MMC-плагина Kaspersky Endpoint Security

MMC-плагин управления Kaspersky Endpoint Security требуется установить на том же устройстве, на котором установлена Консоль администрирования Kaspersky Security Center.

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

Чтобы установить MMC-плагин,

на устройстве, где установлена Консоль администрирования Kaspersky Security Center, запустите исполняемый файл klcfginst.msi.

Файл входит в комплект поставки приложения Kaspersky Endpoint Security.

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:
   - с помощью пункта **Свойства** контекстного меню узла **Сервер администрирования <имя сервера>**;
   - 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 приложениями**.

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

Установка и первоначальная настройка приложения с помощью Kaspersky Security Center

Вы можете установить приложение Kaspersky Endpoint Security на клиентское устройство удаленно с рабочего места администратора с помощью Kaspersky Security Center Web Console или с помощью Консоли администрирования.

Установка с помощью Kaspersky Security Center состоит из следующих этапов:

1. Создание инсталляционного пакета.

Для удаленной установки используется инсталляционный пакет приложения Kaspersky Endpoint Security. Инсталляционный пакет Kaspersky Endpoint Security является общим для всех поддерживаемых операционных систем и типов архитектуры процессора. Вы можете создать инсталляционный пакет с помощью Kaspersky Security Center Web Console или с помощью Консоли администрирования.

Вы можете указать параметры первоначальной настройки приложения в свойствах инсталляционного пакета или в конфигурационном файле autoinstall.ini, который включен в инсталляционный пакет.

Вам нужно настроить параметры первоначальной настройки приложения, если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент) или в режиме Агента Endpoint Detection and Response. По умолчанию приложение используется в стандартном режиме.

Если вы планируете использовать приложение Kaspersky Endpoint Security в стандартном режиме или в режиме Агента Endpoint Detection and Response, во время создания инсталляционного пакета вы можете добавить в пакет:

- лицензионный ключ для автоматической активации приложения во время установки;
- предварительно скачанные базы приложения, чтобы дополнительно не обновлять базы после установки.

Вы также можете активировать приложение и обновить базы позже, во время подготовки приложения к работе.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, не поддерживается активация приложения во время установки и автоматическое распространение лицензионных ключей. Kaspersky Endpoint Security получает информацию о лицензии от Сервера защиты после подключения к SVM, отдельно активировать Kaspersky Endpoint Security не требуется.

2. Развертывание приложения Kaspersky Endpoint Security на устройствах в сети организации.

   Kaspersky Security Center Web Console поддерживает следующие основные способы развертывания:

   - Установка приложения с помощью мастера развертывания защиты.
   - Установка приложения с помощью задачи удаленной установки приложений.

   Консоль администрирования Kaspersky Security Center поддерживает следующие основные способы развертывания:

   - Установка приложения с помощью мастера удаленной установки.
   - Установка приложения с помощью задачи удаленной установки приложений.

   Описание процедур развертывания см. в справке Kaspersky Security Center.

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

3. Подготовка приложения к работе.

   Перед началом использования приложения вам нужно завершить первоначальную настройку приложения и подготовить приложение к работе.

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

Чтобы управлять с помощью Kaspersky Security Center работой приложения Kaspersky Endpoint Security, установленного на клиентских устройствах, вам нужно поместить эти устройства в группы администрирования. Перед началом установки приложения Kaspersky Endpoint Security вы можете создать в Kaspersky Security Center группы администрирования, в которые вы хотите поместить устройства с установленным приложением, и настроить правила автоматического перемещения устройств в группы администрирования. Если правила перемещения устройств в группы администрирования не настроены, Kaspersky Security Center помещает все устройства с установленным Агентом администрирования, подключенным к Серверу администрирования, в список **Нераспределенные устройства**. В этом случае вам нужно вручную переместить устройства в группы администрирования (см. подробнее в справке Kaspersky Security Center).

Создание инсталляционного пакета в Web Console

В Kaspersky Security Center Web Console вы можете создать инсталляционный пакет одним из следующих способов:

- Из архивного файла, который вы подготовили предварительно.
- Из дистрибутива, размещенного на серверах "Лаборатории Касперского".

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред или в режиме Агента Endpoint Detection and Response, вам нужно указать режим использования приложения в параметрах первоначальной настройки. Вы можете указать параметры первоначальной настройки приложения в свойствах созданного инсталляционного пакета на закладке **Параметры** или в конфигурационном файле, который включен в инсталляционный пакет.

Чтобы подготовить архивный файл для создания инсталляционного пакета:

1. Скачайте архив kesl.zip на странице загрузки приложений в разделе **Kaspersky Endpoint Security для Linux** (**Дополнительный дистрибутив** → **Files for Product remote installation**).
2. Распакуйте архив kesl.zip в папку, доступную для Сервера администрирования Kaspersky Security Center. В ту же папку поместите файлы дистрибутива, соответствующие типу операционной системы, на которую вы хотите установить приложение, и типу менеджера пакетов на ней:
   - для установки Kaspersky Endpoint Security:
     - kesl-12.4.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
     - kesl_12.4.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
     - kesl-12.4.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
     - kesl_12.4.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)

- kesl-12.4.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
- kesl_12.4.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)

- для установки графического интерфейса приложения:
  - kesl-gui-12.4.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
  - kesl-gui_12.4.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
  - kesl-gui-12.4.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
  - kesl-gui_12.4.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)
  - kesl-gui-12.4.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
  - kesl-gui_12.4.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)

  Если вы не хотите устанавливать графический интерфейс, не помещайте в папку эти файлы, тогда размер инсталляционного пакета будет меньше.

  Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, графический интерфейс не поддерживается.

Если вы не планируете устанавливать графический интерфейс, вам нужно отказаться от его использования, настроив соответствующий параметр в свойствах созданного инсталляционного пакета или в конфигурационном файле autoinstall.ini (`USE_GUI=No`). В противном случае установка завершается с ошибкой.

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

3. Если вы планируете использовать приложение Kaspersky Endpoint Security в стандартном режиме и хотите использовать предварительно скачанные базы приложения:
   a. Поместите в папку подготовленные архивы с базами для всех необходимых типов операционных систем.
   b. В параметрах первоначальной настройки приложения выключите запуск задачи обновления баз после установки приложения. Вы можете настроить соответствующий параметр в свойствах созданного инсталляционного пакета или в конфигурационном файле autoinstall.ini (`UPDATE_EXECUTE=No`). Файл autoinstall.ini находится в папке, в которую вы распаковали архив kesl.zip.
4. Если вы хотите настроить параметры первоначальной настройки приложения с помощью конфигурационного файла, откройте конфигурационный файл autoinstall.ini и внесите необходимые изменения.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, в конфигурационном файле autoinstall.ini вам нужно установить значение параметра `KSVLA_MODE=Yes`.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response, в конфигурационном файле autoinstall.ini вам нужно установить значение параметра `ENDPOINT_AGENT_MODE=Yes`.

Значения параметров в файле autoinstall.ini чувствительны к регистру.

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

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

Чтобы создать инсталляционный пакет Kaspersky Endpoint Security в Kaspersky Security Center 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. Выберите способ создания инсталляционного пакета:

   - **Создать инсталляционный пакет из файла**. Инсталляционный пакет будет создан из архивного файла, который вы подготовили предварительно. Вам нужно выбрать этот вариант, если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.
   - **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**. Инсталляционный пакет будет создан из дистрибутива, размещенного на серверах "Лаборатории Касперского".

   Kaspersky Security Center Cloud Console не поддерживает создание инсталляционных пакетов из файла.

4. В зависимости от выбранного 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 **Загрузить 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. С помощью инсталляционного пакета вы можете установить приложение на устройства сети организации или обновить версию приложения.

7. Если требуется, настройте параметры первоначальной настройки приложения. Для этого откройте свойства инсталляционного пакета и перейдите на закладку **Параметры**.

> В версии Kaspersky Security Center Web Console ниже 14.2 не поддерживается настройка параметров первоначальной настройки приложения в свойствах инсталляционного пакета Kaspersky Endpoint Security. Для настройки параметров используйте конфигурационный файл autoinstall.ini.

Параметры первоначальной настройки в Web Console

В Kaspersky Security Center Web Console вы можете указать параметры первоначальной настройки приложения Kaspersky Endpoint Security в свойствах инсталляционного пакета на закладке **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**.

Вы также можете указать параметры первоначальной настройки приложения в конфигурационном файле, который включен в инсталляционный пакет.

Параметры первоначальной настройки приложения

Параметр	Описание
Язык событий в KSC	Выберите 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. Приложение использует кодировку UTF-8. 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. Вы также можете активировать приложение после установки. Параметр применяется, только если приложение используется в стандартном режиме.
Источник обновлений	Выберите 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 Агента Endpoint Detection and Response.
Запустить задачу обновления баз после установки	Если флажок установлен, после установки приложения запускается задача обновления баз и модулей приложения. По умолчанию флажок установлен. Параметр применяется, только если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response.
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>://]<IP address of the proxy server>:<port>`, если для подключения к прокси-серверу не требуется аутентификация; • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>`, если для подключения к прокси-серверу требуется аутентификация. Подключение к прокси-серверу по протоколу HTTPS не поддерживается. Параметр применяется, только если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response.
Установить исходный код ядра	Если флажок установлен, для операционных систем, не поддерживающих технологию fanotify, при запуске защиты от файловых угроз автоматически запускается компиляция модуля ядра. По умолчанию флажок установлен.
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 Агента Endpoint Detection and Response.
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, выполняется автоматическая настройка SELinux для работы с Kaspersky Endpoint Security. По умолчанию флажок установлен.

Параметр	Описание
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.
Режим использования приложения	Выберите 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 для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент).
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.
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.
Механизм перехвата	Выберите механизм перехвата системных событий, который приложение будет использовать 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	Описание
Если обновляемый модуль ядра не запускается	Выберите 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.

Создание инсталляционного пакета в Консоли администрирования

Перед тем, как создать инсталляционный пакет приложения Kaspersky Endpoint Security, вам нужно подготовить файлы, которые будут включены в пакет.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред или в режиме Агента Endpoint Detection and Response, вам нужно указать режим использования приложения в параметрах первоначальной настройки. Вы можете указать параметры первоначальной настройки приложения при создании инсталляционного пакета или после его создания в свойствах инсталляционного пакета в разделе **Параметры**, а также в конфигурационном файле, который включен в инсталляционный пакет.

Чтобы подготовить файлы для создания инсталляционного пакета:

1. Скачайте архив kesl.zip на странице загрузки приложений в разделе **Kaspersky Endpoint Security для Linux** (**Дополнительный дистрибутив → Files for Product remote installation**).

2. Распакуйте архив kesl.zip в папку, доступную для Сервера администрирования Kaspersky Security Center. В ту же папку поместите файлы дистрибутива, соответствующие типу операционной системы, на которую вы хотите установить приложение, и типу менеджера пакетов на ней:

   - для установки Kaspersky Endpoint Security:
     - kesl-12.4.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
     - kesl_12.4.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
     - kesl-12.4.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
     - kesl_12.4.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)
     - kesl-12.4.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
     - kesl_12.4.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)

- для установки графического интерфейса приложения:
  - kesl-gui-12.4.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
  - kesl-gui_12.4.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
  - kesl-gui-12.4.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
  - kesl-gui_12.4.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)
  - kesl-gui-12.4.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
  - kesl-gui_12.4.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)

Если вы не хотите устанавливать графический интерфейс, не помещайте в папку эти файлы, тогда размер инсталляционного пакета будет меньше.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, графический интерфейс не поддерживается.

Если вы не планируете устанавливать графический интерфейс, вам нужно отказаться от его использования, настроив соответствующий параметр при создании инсталляционного пакета, в свойствах созданного инсталляционного пакета или в конфигурационном файле autoinstall.ini (`USE_GUI=No`). В противном случае установка завершается с ошибкой.

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

3. Если вы планируете использовать приложение Kaspersky Endpoint Security в стандартном режиме и хотите использовать предварительно скачанные базы приложения:
   a. Поместите в папку подготовленные архивы с базами для всех необходимых типов операционных систем.
   b. В параметрах первоначальной настройки приложения выключите запуск задачи обновления баз после установки приложения. Вы можете настроить соответствующий параметр при создании инсталляционного пакета, в свойствах созданного инсталляционного пакета или в конфигурационном файле autoinstall.ini (`UPDATE_EXECUTE=No`) Файл autoinstall.ini находится в папке, в которую вы распаковали архив kesl.zip.
4. Если вы хотите настроить параметры первоначальной настройки приложения с помощью конфигурационного файла, откройте конфигурационный файл autoinstall.ini и внесите необходимые изменения.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, в конфигурационном файле autoinstall.ini вам нужно установить значение параметра `KSVLA_MODE=Yes`.

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response, в конфигурационном файле autoinstall.ini вам нужно установить значение параметра `ENDPOINT_AGENT_MODE=Yes`.

Значения параметров в файле autoinstall.ini чувствительны к регистру.

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

Чтобы создать инсталляционный пакет Kaspersky Endpoint Security в Консоли администрирования Kaspersky Security Center:

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 приложения "Лаборатории Касперского"**.
4. Введите имя нового инсталляционного пакета и перейдите к следующему шагу мастера.
5. Выберите дистрибутив приложения Kaspersky Endpoint Security. Для этого откройте стандартное окно Windows с помощью кнопки **Обзор** и укажите путь к файлу kesl.kud. Файл находится в папке, в которую вы распаковали архив kesl.zip.

   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.

   Для продолжения создания инсталляционного пакета требуется подтвердить, 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. Если требуется, настройте параметры первоначальной настройки приложения.

   Вы также можете настроить параметры первоначальной настройки приложения позже, в свойствах созданного инсталляционного пакета в разделе **Параметры**.
8. Мастер загружает файлы, необходимые для установки приложения, на Сервер администрирования Kaspersky Security Center. Дождитесь окончания загрузки.
9. Завершите работу мастера.

Созданный инсталляционный пакет размещается в дереве Консоли администрирования Kaspersky Security Center в папке **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**. Вы можете использовать один и тот же инсталляционный пакет многократно.

Параметры первоначальной настройки в Консоли администрирования

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**.

Вы также можете указать параметры первоначальной настройки приложения в конфигурационном файле, который включен в инсталляционный пакет.

Параметры первоначальной настройки приложения

Параметр	Описание
Язык событий в KSC	Выберите 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, по умолчанию используется английский язык. • Один из национальных языков. Приложение использует кодировку UTF-8. 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. Вы также можете активировать приложение после установки. 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**. • **Другие источники 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 Агента Endpoint Detection and Response.
Запустить задачу обновления баз после установки	Если флажок установлен, после установки приложения запускается задача обновления баз и модулей приложения. По умолчанию флажок установлен. Параметр применяется, только если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response.

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>://]<IP address of the proxy server>:<port>`, если для подключения к прокси-серверу не требуется аутентификация; • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>`, если для подключения к прокси-серверу требуется аутентификация. Подключение к прокси-серверу по протоколу HTTPS не поддерживается. Параметр применяется, только если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response.
Установить исходный код ядра	Если флажок установлен, для операционных систем, не поддерживающих технологию fanotify, при запуске защиты от файловых угроз автоматически запускается компиляция модуля ядра. По умолчанию флажок установлен.
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 Агента Endpoint Detection and Response.
Пользователь с ролью администратора (admin)	Введите 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, 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.
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 для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент).

Параметр	Описание
Защищаемая виртуальная машина используется как сервер (окно **Режим использования приложения**)	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.
Включить режим защиты инфраструктуры VDI (окно **Режим использования приложения**)	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.
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 будет использовать 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.
Если обновляемый модуль ядра не запускается (окно **Параметры перехвата системных событий**)	Выберите 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.

Подготовка архива с базами приложения для создания инсталляционного пакета с интегрированными базами

Вы можете создать инсталляционный пакет для удаленной установки, в который добавлены предварительно скачанные базы приложения. Это может потребоваться например, если вы устанавливаете приложение на устройство с операционной системой Astra Linux Special Edition. Если для установки используется инсталляционный пакет с интегрированными базами, приложение устанавливается с рабочими базами, обновлять базы сразу после установки не требуется.

Чтобы создать архив с базами для установки приложения:

1. Выполните установку и первоначальную настройку приложения Kaspersky Endpoint Security на устройстве с помощью командной строки или с помощью Kaspersky Security Center.

2. Выполните обновление баз приложения. Вы можете обновить базы в ходе первоначальной настройки приложения или после установки, запустив задачу типа Update в командной строке или задачу *Обновление* в Консоли администрирования Kaspersky Security Center или в Kaspersky Security Center Web Console.

3. Скопируйте содержимое директории /var/opt/kaspersky/kesl/private/updates/ в одну из следующих поддиректорий в зависимости от архитектуры операционной системы, для которой вы создаете инсталляционный пакет с интегрированными базами: /i386/, /x86_64/ или /arm64/.

4. Поместите директории с базами в архив kesl-bases.tgz, сохраняя структуру вложенных директорий. Вы можете поместить в архив только одну поддиректорию с базами для нужной архитектуры операционной системы или все поддиректории с базами (/i386/, /x86_64/ или /arm64/) в один архив под разные архитектуры, если вы планируете создать инсталляционный пакет для установки на несколько операционных систем с разной архитектурой.

Созданный архив с базами приложения вы можете использовать при создании инсталляционного пакета в Консоли администрирования Kaspersky Security Center или в Kaspersky Security Center Web Console.

Параметры конфигурационного файла autoinstall.ini

В конфигурационном файле autoinstall.ini вы можете задавать параметры, приведенные в таблице ниже. Набор применимых параметров зависит от режима использования приложения.

Значения параметров чувствительны к регистру.

Параметры конфигурационного файла autoinstall.ini

Параметр	Описание	Значения
KSVLA_MODE	Использование Kaspersky Endpoint Security в режиме Легкого агента.	`Yes` – Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент). `No` (значение по умолчанию) – Kaspersky Endpoint Security используется в стандартном режиме или в режиме Агента Endpoint Detection and Response (см. параметр ENDPOINT_AGENT_MODE).
SERVER_MODE	Роль защищаемой виртуальной машины (сервер или рабочая станция). Параметр применяется, только если приложение используется в режиме Легкого агента.	`Yes` (значение по умолчанию) – защищаемая виртуальная машина используется как сервер. `No` – защищаемая виртуальная машина используется как рабочая станция.

Параметр	Описание	Значения
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.	`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` (значение по умолчанию) – не включать режим защиты инфраструктуры VDI.
ENDPOINT_AGENT_MODE	Использование Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response.	`Yes` – Kaspersky Endpoint Security используется в режиме Агента Endpoint Detection and Response 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).
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.
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.
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` – не удалять пользователей из привилегированных групп.

Параметр	Описание	Значения
LOCALE	Дополнительный параметр. 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; • `fr_FR.UTF-8` – французский; • `ja_JP.UTF-8` – японский; • `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).
INSTALL_LICENSE	Код активации для добавления лицензионного ключа в приложение. Параметр применяется, только если приложение используется в стандартном режиме.	`<код активации>` – если требуется активировать приложение во время установки; `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 Агента Endpoint Detection and Response.	`SCServer` – использовать в качестве источника обновлений Сервер администрирования Kaspersky Security Center. `KLServers` – использовать в качестве источника обновлений серверы "Лаборатории Касперского". Это значение используется по умолчанию. `<адрес источника обновлений>`.
PROXY_SERVER	Адрес прокси-сервера, используемого для подключения к интернету. Параметр применяется, только если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response.	Адрес прокси-сервера в одном из следующих форматов: • `[<connection protocol>://]<IP address of the proxy server>:<port>`, если для подключения к прокси-серверу не требуется аутентификация; • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>`, если для подключения к прокси-серверу требуется аутентификация. 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 Агента Endpoint Detection and Response.	`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 (для операционных систем, 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 Агента Endpoint Detection and Response.	`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.
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.
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.
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.	`UseFanotify` (значение по умолчанию) – использовать технологию fanotify для перехвата системных событий. `UseUpdatableKernelModule` – использовать обновляемый модуль ядра для перехвата системных событий.
INTERCEPTOR_FALLBACK_STRATEGY	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) – 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.

Параметр	Описание	Значения
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 на устройствах, где операционная система поддерживает технологию fanotify.	`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` – не создавать файл трассировки при первом запуске приложения.

Если вы хотите изменить параметры в конфигурационном файле autoinstall.ini, укажите значения параметров в формате <имя параметра>=<значение параметра> без пробелов между именем параметра и его значением.

Подготовка приложения к работе с помощью Kaspersky Security Center

После развертывания приложения Kaspersky Endpoint Security через Kaspersky Security Center требуется подготовить приложение к работе. Действия, которые необходимо выполнить, зависят от режима, в котором вы планируете использовать приложение Kaspersky Endpoint Security.

Стандартный режим

Если вы планируете использовать приложение Kaspersky Endpoint Security в стандартном режиме, после развертывания приложения вам нужно выполнить следующие действия:

1. Активировать приложение, если активация не была выполнена с помощью ключа, добавленного в инсталляционный пакет приложения.

   Вы можете создать и выполнить задачу активации через Консоль администрирования или через Kaspersky Security Center Web Console, а также распространить на устройства лицензионный ключ из хранилища ключей Kaspersky Security Center.

2. Обновить базы и модули приложения, если в инсталляционный пакет приложения не были добавлены предварительно скачанные базы приложения. Вы можете использовать задачу *Обновление*, которая создана автоматически мастером первоначальной настройки Kaspersky Security Center после установки MMC-плагина управления или веб-плагина управления Kaspersky Endpoint Security.

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

3. Настроить политику для централизованного управления работой приложения с помощью Консоли администрирования Kaspersky Security Center (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) или Web Console. Вы можете использовать политику, которая создана автоматически мастером первоначальной настройки Kaspersky Security Center после установки MMC-плагина управления или веб-плагина управления Kaspersky Endpoint Security.

   Также вы можете настроить задачи управления приложением с помощью Консоли администрирования или Web Console.

Режим Легкого агента

Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, после развертывания приложения вам нужно выполнить следующие действия:

1. Настроить параметры обнаружения SVM Легкими агентами. Для этого вам нужно создать и настроить политику для централизованного управления работой приложения на клиентских устройствах. Для работы с политиками вы можете использовать Консоль администрирования (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) или Web Console.

   В свойствах политики вам нужно настроить следующие параметры:

   - Параметры подключения Легких агентов к Серверу интеграции.
   - Параметры подключения Легких агентов к SVM.

2. Убедиться в том, что установлено подключение Легких агентов к SVM и к Серверу интеграции.

   Вы можете получить информацию о подключении с помощью команд Kaspersky Endpoint Security на защищенной виртуальной машине:

   - Информацию о подключении к SVM вы можете посмотреть с помощью команды `kesl-control [-V] --svm-info`.
   - Информацию о подключении к Серверу интеграции вы можете посмотреть с помощью команды `kesl-control [-V] --viis-info`.

3. Убедиться в том, что приложение Kaspersky Endpoint Security, используемое в качестве Легкого агента, получает информацию о лицензии, по которой активировано решение Kaspersky Security для виртуальных сред Легкий агент.

   После активации решения на SVM и подключения Легких агентов к SVM компонент Сервер защиты передает информацию о лицензии Легким агентам. Информацию о лицензии, которую использует приложение Kaspersky Endpoint Security в составе решения, вы можете посмотреть удаленно с помощью Kaspersky Security Center или на защищенной виртуальной машине с помощью командной строки.

4. Убедиться в том, что на защищенных виртуальных машинах установлены обновления баз, необходимых для работы Легкого агента.

   Обновление баз на защищенных виртуальных машинах выполняется с помощью специальной задачи *Обновление*, в которой в качестве источника обновлений указана папка на SVM. Задача обновления запускается автоматически.

   Вы можете проверить актуальность баз на защищенной виртуальной машине с Легким агентом с помощью команды `kesl-control --app-info`.

Также вы можете настроить параметры работы приложения с помощью политики и задач управления приложением в Консоли администрирования или в Web Console.

Установка и первоначальная настройка приложения с помощью командной строки

Вы можете установить приложение Kaspersky Endpoint Security на клиентское устройство с помощью командной строки.

Установка с помощью командной строки состоит из следующих этапов:

1. Установка приложения и графического интерфейса приложения. В зависимости от режима, в котором вы планируете использовать приложение Kaspersky Endpoint Security, вы можете использовать следующие варианты установки приложения:

   - Если вы планируете использовать приложение Kaspersky Endpoint Security в стандартном режиме, вы можете:
     - установить приложение с графическим интерфейсом;
     - установить приложение без графического интерфейса;
     - установить графический интерфейс на устройстве, где установлено приложение.

       Невозможно установить графический интерфейс на устройстве, где приложение не установлено.

   - Если вы планируете использовать приложение Kaspersky Endpoint Security в режиме Легкого агента, вам нужно установить приложение без графического интерфейса приложения. Графический интерфейс не поддерживается.

   Если версия менеджера пакетов apt ниже 1.1.X, требуется использовать для установки менеджер пакетов dpkg (в зависимости от операционной системы).

2. Первоначальная настройка приложения.

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

   Если на устройстве не выполнена первоначальная настройка приложения, 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 приложения в интерактивном режиме или в автоматическом режиме.

Установка приложения с помощью командной строки

Установка приложения без графического интерфейса приложения

Чтобы установить Kaspersky Endpoint Security из пакета формата RPM на 32-битную операционную систему, выполните следующую команду:

```
# rpm -i kesl-12.4.0-<номер сборки>.i386.rpm
```

Чтобы установить Kaspersky Endpoint Security из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:

```
# rpm -i kesl-12.4.0-<номер сборки>.x86_64.rpm
```

Чтобы установить Kaspersky Endpoint Security из пакета формата RPM на 64-битную операционную систему из линейки Альт, выполните следующую команду:

```
# apt-get install kesl-12.4.0-<номер сборки>.x86_64.rpm
```

Чтобы установить Kaspersky Endpoint Security из пакета формата RPM на 64-битную операционную систему для архитектуры Arm, выполните следующую команду:

```
# rpm -i kesl-12.4.0-<номер сборки>.aarch64.rpm
```

Чтобы установить Kaspersky Endpoint Security из пакета формата RPM на 64-битную операционную систему из линейки Альт для архитектуры Arm, выполните следующую команду:

```
# apt-get install kesl-12.4.0-<номер сборки>.aarch64.rpm
```

Чтобы установить Kaspersky Endpoint Security из пакета формата DEB на 32-битную операционную систему, выполните следующую команду:

```
# apt-get install ./kesl_12.4.0-<номер сборки>_i386.deb
```

Чтобы установить Kaspersky Endpoint Security из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:

```
# apt-get install ./kesl_12.4.0-<номер сборки>_amd64.deb
```

Чтобы установить Kaspersky Endpoint Security из пакета формата DEB на 64-битную операционную систему для архитектуры Arm, выполните следующую команду:

```
# apt-get install ./kesl_12.4.0-<номер сборки>_arm64.deb
```

Установка графического интерфейса приложения

Чтобы установить графический интерфейс из пакета формата RPM на 32-битную операционную систему, выполните следующую команду:

```
# rpm -i kesl-gui-12.4.0-<номер сборки>.i386.rpm
```

Чтобы установить графический интерфейс из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:

```
# rpm -i kesl-gui-12.4.0-<номер сборки>.x86_64.rpm
```

Чтобы установить графический интерфейс из пакета формата RPM на 64-битную операционную систему из линейки Альт, выполните следующую команду:

```
# apt-get install kesl-gui-12.4.0-<номер сборки>.x86_64.rpm
```

Чтобы установить графический интерфейс из пакета формата RPM на 64-битную операционную систему для архитектуры Arm, выполните следующую команду:

```
# rpm -i kesl-gui-12.4.0-<номер сборки>.aarch64.rpm
```

Чтобы установить графический интерфейс из пакета формата RPM на 64-битную операционную систему из линейки Альт для архитектуры Arm, выполните следующую команду:

```
# apt-get install kesl-gui-12.4.0-<номер сборки>.aarch64.rpm
```

Чтобы установить графический интерфейс из пакета формата DEB на 32-битную операционную систему, выполните следующую команду:

```
# apt-get install ./kesl-gui_12.4.0-<номер сборки>_i386.deb
```

Чтобы установить графический интерфейс из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:

```
# apt-get install ./kesl-gui_12.4.0-<номер сборки>_amd64.deb
```

Чтобы установить графический интерфейс из пакета формата DEB на 64-битную операционную систему для архитектуры Arm, выполните следующую команду:

```
# apt-get install ./kesl-gui_12.4.0-<номер сборки>_arm64.deb
```

Первоначальная настройка приложения в интерактивном режиме

Для выполнения первоначальной настройки приложения в интерактивном режиме вам нужно запустить мастер первоначальной настройки приложения Kaspersky Endpoint Security.

Мастер первоначальной настройки требуется запускать с root-правами.

Чтобы запустить мастер первоначальной настройки, выполните следующую команду:

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

Мастер пошагово запрашивает значения параметров приложения Kaspersky Endpoint Security. Завершение работы мастера и освобождение консоли означает, что процесс первоначальной настройки приложения завершен.

Чтобы проверить код возврата, выполните следующую команду:

```
echo $?
```

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

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

Выбор режима использования: стандартный или Легкий агент

На этом шаге укажите, планируете ли вы использовать приложение Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред, как компонент решения Kaspersky Security для виртуальных сред Легкий агент:

- Введите `yes`, если вы хотите использовать Kaspersky Endpoint Security в режиме Легкого агента.
- Введите `no`, если вы хотите использовать Kaspersky Endpoint Security в стандартном режиме, как автономное приложение для защиты рабочих станций и серверов.

  Если вы планируете использовать приложение в режиме Агента Endpoint Detection and Response, на этом шаге вам также нужно ввести `no`. Вы сможете выбрать режим Агента Endpoint Detection and Response на следующем шаге.

После завершения первоначальной настройки изменить режим использования приложения невозможно.

Определение роли виртуальной машины

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

На этом шаге 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

Включение режима защиты инфраструктуры VDI

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в режиме Легкого агента для защиты виртуальных сред.

На этом шаге вы можете включить режим защиты инфраструктуры VDI. Этот режим 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.

Выбор режима использования: стандартный или Агент Endpoint Detection and Response

Этот шаг отображается, только если на первом шаге вы выбрали использование Kaspersky Endpoint Security в стандартном режиме. Приложение не может одновременно использоваться в режиме Легкого агента и в режиме Агента Endpoint Detection and Response.

На этом шаге укажите, планируете ли вы использовать приложение Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response:

- Введите `yes`, если вы хотите использовать Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response, как приложение, обеспечивающее совместную работу на защищаемых устройствах решений Detection and Response от "Лаборатории Касперского" и антивирусных решений от сторонних поставщиков.

- Введите `no`, если вы хотите использовать Kaspersky Endpoint Security в стандартном режиме, как автономное приложение для защиты рабочих станций и серверов.

После завершения первоначальной настройки изменить режим использования приложения невозможно.

Выбор языкового стандарта

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

Вам нужно указать 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.

Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге вам нужно ознакомиться с текстом Лицензионного соглашения, которое заключается между вами и "Лабораторией Касперского" и Политики конфиденциальности, которая описывает обработку и передачу данных.

Принятие Лицензионного соглашения

На этом шаге вам нужно принять или отклонить условия 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, процесс настройки приложения Kaspersky Endpoint Security прерывается.

Принятие Политики конфиденциальности

На этом шаге вам нужно принять или отклонить условия 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, процесс настройки приложения Kaspersky Endpoint Security прерывается.

Использование Kaspersky Security Network

На этом шаге вам нужно принять или отклонить условия использования Kaspersky Security Network. Файл ksn_license.<ID языка> с текстом Положения о Kaspersky Security Network находится в директории /opt/kaspersky/kesl/doc/.

Введите одно из следующих значений:

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

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 приложение Kaspersky Endpoint Security используется в стандартном режиме и вы включили использование Kaspersky Security Network, автоматически включается облачный режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО. В режиме Легкого агента для защиты виртуальных сред работа с облегченными базами вредоносного ПО не поддерживается.

Удаление пользователей из привилегированных групп

Этот шаг отображается, только если обнаружены пользователи в группе kesladmin и/или в группе keslaudit.

На этом шаге 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.

Назначение пользователю роли администратора

На этом шаге вы можете назначить пользователю 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.

Настройка механизма перехвата системных событий

На этом шаге определяется возможность использования в работе приложения различных механизмов перехвата системных событий. Если операционная система на устройстве поддерживает технологию fanotify, вы можете выбрать механизм перехвата системных событий, который приложение будет использовать в своей работе:

- 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.

Приложение может использовать механизм перехвата на основе обновляемого модуля ядра, если операционная система соответствует требованиям для установки обновляемого модуля ядра. Если операционная система на устройстве поддерживает технологию fanotify, но не соответствует требованиям для установки обновляемого модуля ядра, для перехвата системных событий приложение будет использовать технологию 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.

Если операционная система на устройстве не поддерживает технологию fanotify, для перехвата системных событий приложение будет использовать модуль ядра для защиты от файловых угроз. При наличии всех необходимых пакетов компиляция модуля ядра будет запущена 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.

Включение автоматической настройки SELinux

Этот шаг отображается, только если в вашей операционной системе установлена система SELinux.

На этом шаге вы можете включить автоматическую настройку системы контроля доступа SELinux для работы с приложением Kaspersky Endpoint Security.

Введите `yes`, чтобы включить автоматическую настройку системы SELinux. Если не удалось настроить систему SELinux автоматически (например, в случае отсутствия утилиты semanage), приложение выводит сообщение об ошибке и предлагает пользователю настроить систему SELinux вручную.

Введите `no`, если вы не хотите, чтобы приложение автоматически настроило систему SELinux.

По умолчанию приложение предлагает значение `yes`.

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

Настройка источника обновлений

Этот шаг отображается, только если на первых шагах мастера вы выбрали использование Kaspersky Endpoint Security в стандартном режиме или в режиме Агента Endpoint Detection and Response. Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает обновления баз и программных модулей Легкого агента от Сервера защиты.

На этом шаге вам нужно указать 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 локальной сети или в интернете.

Настройка параметров прокси-сервера

Этот шаг отображается, только если на первых шагах мастера вы выбрали использование Kaspersky Endpoint Security в стандартном режиме или в режиме Агента Endpoint Detection and Response.

На этом шаге вам нужно указать параметры прокси-сервера, если вы используете прокси-сервер для доступа в интернет. Для загрузки баз приложения с серверов обновлений требуется подключение к интернету.

Чтобы настроить параметры прокси-сервера, выполните одно из следующих действий:

- Если при подключении к интернету вы используете прокси-сервер, укажите адрес прокси-сервера в одном из следующих форматов:
  - `<протокол подключения>://<IP-адрес прокси-сервера>:<номер порта>`, если для подключения к прокси-серверу не требуется аутентификация;
  - `<протокол подключения>://<имя пользователя>:<пароль>@<IP-адрес прокси-сервера>:<номер порта>`, если для подключения к прокси-серверу требуется аутентификация.

    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 для подключения к интернету не используется прокси-сервер, введите значение `no`.

По умолчанию приложение предлагает значение `no`.

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

Запуск обновления баз приложения

Этот шаг отображается, только если на первых шагах мастера вы выбрали использование Kaspersky Endpoint Security в стандартном режиме или в режиме Агента Endpoint Detection and Response. Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает обновления баз и программных модулей Легкого агента от Сервера защиты.

На этом шаге вы можете запустить задачу обновления баз приложения на клиентском устройстве.

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

Если вы хотите запустить задачу обновления баз на устройстве, введите `yes`.

По умолчанию приложение 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.

Включение автоматического обновления баз приложения

Этот шаг отображается, только если на первых шагах мастера вы выбрали использование Kaspersky Endpoint Security в стандартном режиме или в режиме Агента Endpoint Detection and Response. Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает обновления баз и программных модулей Легкого агента от Сервера защиты.

На этом шаге вы можете включить автоматическое обновление баз приложения.

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.

Активация приложения

Этот шаг отображается, только если на первых шагах мастера вы выбрали использование Kaspersky Endpoint Security в стандартном режиме. Если Kaspersky Endpoint Security используется в режиме Агента Endpoint Detection and Response, после завершения первоначальной настройки приложения вам нужно добавить лицензионный ключ, предназначенный для активации функциональности Kaspersky Endpoint Detection and Response Expert (on-premise). Если Kaspersky Endpoint Security используется в режиме Легкого агента, Kaspersky Endpoint Security получает информацию о лицензии от Сервера защиты, отдельно активировать Kaspersky Endpoint Security не требуется.

На этом шаге вы можете активировать приложение с помощью кода активации или файла ключа.

Чтобы активировать приложение с помощью кода активации, требуется ввести код активации.

Чтобы активировать приложение с помощью файла ключа, требуется указать 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.

Первоначальная настройка приложения в автоматическом режиме

Для выполнения первоначальной настройки приложения в автоматическом режиме вам нужно:

1. Подготовить конфигурационный файл, который содержит параметры первоначальной настройки. Вы можете создать этот файл или скопировать структуру для него из конфигурационного файла autoinstall.ini, который используется для удаленной установки приложения с помощью Kaspersky Security Center.

2. Запустить мастер первоначальной настройки приложения Kaspersky Endpoint Security, указав путь к конфигурационному файлу.

   Мастер первоначальной настройки требуется запускать с root-правами.

Чтобы запустить первоначальную настройку приложения в автоматическом режиме, выполните следующую команду:

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=< конфигурационный файл первоначальной настройки >
```

где < конфигурационный файл первоначальной настройки > – путь к конфигурационному файлу, который содержит параметры первоначальной настройки.

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

Чтобы проверить код возврата, выполните следующую команду:

```
echo $?
```

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

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

Для корректного обновления модулей приложения после завершения работы мастера может потребоваться перезапуск приложения. Проверьте состояние обновлений для приложения с помощью команды `kesl-control --app-info`.

Параметры конфигурационного файла первоначальной настройки

В конфигурационном файле первоначальной настройки вы можете задавать параметры, приведенные в таблице ниже. Набор применимых параметров зависит от режима использования приложения.

Значения параметров чувствительны к регистру.

Параметры конфигурационного файла первоначальной настройки

Параметр	Описание	Значения
KSVLA_MODE	Использование Kaspersky Endpoint Security в режиме Легкого агента.	`Yes` – Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент). `No` – Kaspersky Endpoint Security используется в стандартном режиме или в режиме Агента Endpoint Detection and Response (см. параметр ENDPOINT_AGENT_MODE).
SERVER_MODE	Роль защищаемой виртуальной машины (сервер или рабочая станция). Параметр применяется, только если приложение используется в режиме Легкого агента.	`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.	`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.

Параметр	Описание	Значения
ENDPOINT_AGENT_MODE	Использование Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response.	`Yes` – Kaspersky Endpoint Security используется в режиме Агента Endpoint Detection and Response для обеспечения совместной работы на защищаемых устройствах решений Detection and Response от "Лаборатории Касперского" и антивирусных решений от сторонних поставщиков. `No` – Kaspersky Endpoint Security используется в стандартном режиме или в режиме Легкого агента (см. параметр KSVLA_MODE).
EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения.	`Yes` – принять условия Лицензионного соглашения. `No` – не принимать условия Лицензионного соглашения. Первоначальная настройка приложения будет прервана.
PRIVACY_POLICY_AGREED	Обязательный параметр. Согласие с условиями Политики конфиденциальности.	`Yes` – принять условия Политики конфиденциальности, чтобы продолжить процедуру установки приложения. `No` – не принимать условия Политики конфиденциальности. Первоначальная настройка 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` – не принимать условия Положения о Kaspersky Security Network. Отказ от использования KSN не прерывает процесс первоначальной настройки приложения.
GROUP_CLEAN	Обязательный параметр. 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` – не удалять пользователей из привилегированных групп.

Параметр	Описание	Значения
LOCALE	Дополнительный параметр. 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; • `fr_FR.UTF-8` – французский; • `ja_JP.UTF-8` – японский; • `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).
INSTALL_LICENSE	Код активации или путь к файлу ключа для добавления лицензионного ключа в приложение. Параметр применяется, только если приложение используется в стандартном режиме.	`<код активации>` – если требуется активировать приложение с использованием кода активации во время установки; `<полный путь к файлу ключа>` – если требуется активировать приложение с использованием файла ключа во время установки; `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 Агента Endpoint Detection and Response.	`SCServer` – использовать в качестве источника обновлений Сервер администрирования Kaspersky Security Center. `KLServers` – использовать в качестве источника обновлений серверы "Лаборатории Касперского". `<адрес источника обновлений>`.
PROXY_SERVER	Адрес прокси-сервера, используемого для подключения к интернету. Параметр применяется, только если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response.	Адрес прокси-сервера в одном из следующих форматов: • `[<connection protocol>://]<IP address of the proxy server>:<port>`, если для подключения к прокси-серверу не требуется аутентификация; • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>`, если для подключения к прокси-серверу требуется аутентификация. Подключение к прокси-серверу по протоколу HTTPS не поддерживается.

Параметр	Описание	Значения
UPDATE_EXECUTE	Запуск задачи обновления баз приложения во время первоначальной настройки. Параметр применяется, только если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response.	`Yes` – запускать задачу обновления. `No` – не запускать задачу обновления.
KERNEL_SRCS_INSTALL	Автоматический запуск компиляции модуля ядра при запуске защиты от файловых угроз (для операционных систем, не поддерживающих технологию fanotify).	`Yes` – компилировать модуль ядра при запуске защиты от файловых угроз. `No` – не компилировать модуль ядра.
ADMIN_USER	Пользователь, которому назначается роль администратора (admin).	
CONFIGURE_SELINUX	Автоматическая настройка SELinux для работы с приложением Kaspersky Endpoint Security.	`Yes` – выполнить автоматическую настройку SELinux для работы с Kaspersky Endpoint Security. `No` – не выполнять автоматическую настройку SELinux.
DISABLE_PROTECTION	Выключение компонентов защиты и задач проверки приложения после его установки. Установка с выключенными компонентами защиты 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 и задачи, то после перезапуска приложения включенные компоненты и задачи 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.
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.	`UseFanotify` – использовать технологию fanotify для перехвата системных событий. `UseUpdatableKernelModule` – использовать обновляемый модуль ядра для перехвата системных событий.
INTERCEPTOR_FALLBACK_STRATEGY	Действие, которое приложение выполняет, если обновляемый модуль ядра не запускается. Параметр применяется только на устройствах, где операционная система поддерживает технологию fanotify.	`FallbackToFanotify` – 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.
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 приложения при первом запуске после установки. `No` – не создавать файл трассировки при первом запуске приложения.

Указывайте значения параметров в формате <имя параметра>=<значение параметра> без пробелов

между именем параметра и его значением.

Настройка разрешающих правил в системе SELinux

Настройка SELinux для работы с приложением вручную

Если во время первоначальной настройки приложению Kaspersky Endpoint Security не удалось настроить систему SELinux автоматически или вы отказались от автоматической настройки, вы можете вручную настроить систему SELinux для работы с приложением Kaspersky Endpoint Security.

Чтобы вручную настроить систему SELinux для работы с приложением:

1. Переведите систему SELinux в неблокирующий режим:

   - Если SELinux был активирован, выполните следующую команду:

     ```
     # setenforce Permissive
     ```

   - Если SELinux был 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, выполнив следующие команды:

   ```
   # semanage fcontext -a -t bin_t < исполняемый файл >
   # restorecon -v < исполняемый файл >
   ```

   где `< исполняемый файл >`:

   - /var/opt/kaspersky/kesl/12.4.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/12.4.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/12.4.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/12.4.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kesl/shared/kesl

4. Запустите следующие задачи:

   - задачу Защита от файловых угроз:

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

- задачу Проверка важных областей:

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

Рекомендуется запустить все задачи, которые вы планируете запускать 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:

   ```
   # 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, и снова запустите задачи, которые вы планируете запускать при использовании приложения Kaspersky Endpoint Security, выполнив следующие команды:

   ```
   # 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 запуска задачи Запуск процесса

Если в вашей операционной системе установлена система SELinux в режиме `Enforcing`, то для запуска задачи Запуск процесса вам нужно дополнительно настроить систему SELinux.

Чтобы настроить систему SELinux для запуска задачи Запуск процесса:

1. Переведите систему SELinux в неблокирующий режим:

   - Если SELinux был активирован, выполните следующую команду:

     ```
     # setenforce Permissive
     ```

   - Если SELinux был 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 задачу Запуск процесса.

4. Убедитесь, что в файле audit.log нет ошибок:

   ```
   # 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 задачу Запуск процесса.

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

6. Переведите систему SELinux в блокирующий режим:

   ```
   # setenforce Enforcing
   ```

Запуск приложения в ОС Astra Linux в режиме замкнутой программной среды

В этом разделе описаны действия, которые требуется выполнить, чтобы запустить приложение в операционной системе Astra Linux Special Edition в режиме замкнутой программной среды.

Для Astra Linux Special Edition (очередные обновления 1.6, 1.7 и 1.8)

Чтобы запустить приложение в операционной системе Astra Linux Special Edition (очередные обновления 1.6, 1.7 или 1.8):

1. Укажите следующие параметры в файле /etc/digsig/digsig_initramfs.conf:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Установите пакет совместимости:

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

3. Создайте директорию для ключа приложения:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Разместите ключ приложения (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) в директории, созданной на предыдущем шаге:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. Обновите образ initramfs:

   ```
   update-initramfs -u -k all
   ```

6. Перезагрузите операционную систему.

Для Astra Linux Special Edition (очередное обновление 1.5)

Чтобы запустить приложение в операционной системе Astra Linux Special Edition (очередное обновление 1.5):

1. Укажите следующие параметры в файле /etc/digsig/digsig_initramfs.conf:

   ```
   DIGSIG_LOAD_KEYS=1
   DIGSIG_ENFORCE=1
   ```

2. Создайте директорию для ключа приложения:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

3. Разместите ключ приложения (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) в директории, созданной на предыдущем шаге:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

4. Обновите образ initramfs:

   ```
   sudo update-initramfs -u -k all
   ```

5. Перезагрузите операционную систему.

Работа с графическим пользовательским интерфейсом приложения поддерживается для сессий с мандатным разграничением доступа.

Запуск приложения в ОС Альт СП в режиме замкнутой программной среды

В этом разделе описаны действия, которые требуется выполнить в командной строке, чтобы запустить приложение в операционной системе Альт СП в режиме замкнутой программной среды.

Чтобы запустить приложение в операционной системе Альт СП:

1. Выключите режим замкнутой программной среды, если он включен, выполнив команду:

   ```
   integrity-remover
   ```

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

   ```
   groupadd kesl
   ```

3. Узнайте уникальный идентификатор (GUID) созданной группы, выполнив команду:

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

4. Внесите изменения в политику IMA, чтобы исключить группу kesl. Для этого выполните следующие действия:

   a. Скопируйте файл /usr/share/integrity/policy, выполнив команду:

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

b. Отредактируйте файл /etc/integrity/policy с помощью текстового редактора (например, vim), выполнив команду:

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

c. После строки `dont_measure fsmagic=0xf97cff8c` (обычно это последняя строка блока `dont_measure`) добавьте строку `dont_measure fgroup=<GUID>`, где `<GUID>` – это 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=<GUID>`, где `<GUID>` – это 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 для включения приложения Kaspersky Endpoint Security в список разрешенных для запуска в режиме замкнутой программной среды. Для этого выполните следующие действия:

a. Отредактируйте файл /usr/sbin/integrity-sign с помощью текстового редактора (например, vim), выполнив команду:

```
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.

6. Установите приложение Kaspersky Endpoint Security. Чтобы убедиться в корректности работы обновления баз приложения после его установки, на этапе первоначальной настройки приложения откажитесь от запуска обновления баз приложения (для этого введите no на шаге запуска обновления баз приложения).

7. Назначьте наследование группы kesl и права на директории для обновляемых компонентов приложения Kaspersky Endpoint Security, выполнив следующие команды:

```
cd /var/opt/kaspersky/kesl/< номер сборки _*>/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 {} \;
```

8. Назначьте наследование группы kesl и права на директории для обновляемых компонентов Агента администрирования, выполнив следующие команды:

```
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 {} \;
```

9. Включите режим замкнутой программной среды, выполнив запуск подписания системы с помощью команды:

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

10. Убедитесь, что подсистема IMA активирована, выполнив команду:

    ```
    cat /proc/cmdline
    ```

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

11. Запустите задачу обновления баз, выполнив команду:

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

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

12. Перезапустите приложение, выполнив команду:

    ```
    systemctl restart kesl
    ```

Настройка ОС ОСнова для работы приложения

Для ОСнова версии 2.4

Чтобы подготовить устройство с операционной системой ОСнова 2.4 к удаленной установке Агента администрирования:

1. Откройте файл /etc/systemd/logind.conf и в секции `[Login]` закомментируйте строку `#KillUserProcesses=yes`.

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

Чтобы запустить приложение в операционной системе ОСнова 2.4:

1. Откройте файл /etc/NESS/systemd/kesl.service.config и задайте значение параметра `NESSCTX_MODIFY=t+ADDEQUSOCK,OMIT,70,SSUID_SAVE_CTX_PERMANENT"`.

2. Обновите параметры служб, выполнив команду `systemctl daemon-reload`.

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

4. Перезагрузите операционную систему.

После установки графического интерфейса (пакета kesl-gui) выполните следующие команды в терминале командной строки от имени пользователя root:

```
rm /etc/xdg/autostart/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/autostart.desktop /etc/xdg/autostart/kaspersky-
kesl.desktop

rm /usr/share/applications/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/app.desktop /usr/share/applications/kaspersky-
kesl.desktop

rm /usr/share/autostart/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/autostart.desktop /usr/share/autostart/kaspersky-
kesl.desktop

rm /usr/share/kde4/services/ServiceMenus/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/kde.desktop
/usr/share/kde4/services/ServiceMenus/kaspersky-kesl.desktop

rm /usr/share/kservices5/ServiceMenus/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/kde.desktop /usr/share/kservices5/ServiceMenus/kaspersky-
kesl.desktop

rm /usr/share/Thunar/sendto/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/sendto.desktop /usr/share/Thunar/sendto/kaspersky-
kesl.desktop
```

Для ОСнова версии 2.5.1 и выше

Чтобы подготовить устройство с операционной системой ОСнова 2.5.1 и выше к удаленной 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`.

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

Чтобы запустить приложение в операционной системе ОСнова 2.5.1 и выше:

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. Обновите параметры служб, выполнив команду `systemctl daemon-reload`.

3. Откройте файл /etc/sysctl.d/30-disable-ptrace.conf и задайте значение параметра `kernel.yama.ptrace_scope=0.`

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

5. Перезагрузите операционную систему.

При установке приложения Kaspersky Endpoint Security на устройство с операционной системой ОСнова версий 2.14 и выше может возникать ошибка `"dpkg: error processing package kesl (--install): installed kesl package post-installation script subprocess returned error exit status 1"` из-за наличия двух строк `SUPPORT_URL` в файле /etc/os-release. Для корректной установки приложения требуется удалить одну из двух строк `SUPPORT_URL` в файле /etc/os-release.

Оптимизация потребления ресурсов приложением

Этот раздел содержит рекомендации специалистов "Лаборатории Касперского" по настройке приложения Kaspersky Endpoint Security для оптимизации потребления ресурсов системы. 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. Чтобы избежать снижения производительности, рекомендуется после установки и первоначальной настройки приложения выполнить процедуры, описанные в этом разделе.

Рекомендуемый сценарий настройки приложения для оптимизации потребления ресурсов системы состоит из следующих этапов:

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 по 1-2 пилотных устройств 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 параметров 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.

   Вы также можете оптимизировать работу компонентов Защита от веб-угроз и Защита от сетевых угроз.

5. **Настройка параметров приложения на всех устройствах**

   Если указанные действия привели к приросту производительности на устройстве, выполните аналогичную настройку приложения на других устройствах того же типа.

Рекомендации для типовых серверных ролей

Веб-сервер

При работе по протоколу HTTPS и высокой клиентской нагрузке на сервер компоненты Защита от веб-угроз и Защита от сетевых угроз могут значительно увеличивать потребление системных ресурсов. Это происходит из-за того, что приложение расшифровывает и проверяет HTTPS-трафик.

Проанализируйте, как изменяется нагрузка на сервер во время работы этих компонентов. Обратитесь в техническую поддержку "Лаборатории Касперского", чтобы подобрать оптимальные параметры работы и устранить проблемы совместимости.

Прокси-сервер

Рекомендуется выключить компоненты Защита от веб-угроз и Защита от сетевых угроз на устройстве, выполняющем функции прокси-сервера или балансировщика нагрузки.

Сервер с контейнеризацией

Рекомендуется выключить компоненты Защита от веб-угроз и Защита от сетевых угроз на серверах, которые используются для сервисов контейнеризации. Для защиты контейнерных сред вы можете использовать приложение Kaspersky Container Security.

Анализ работы приложения на устройстве

При проверке объектов приложение Kaspersky Endpoint Security использует ресурсы процессора, ввод-вывод дисковой подсистемы и оперативную память.

Чтобы посмотреть информацию о потреблении ресурсов приложением, выполните следующую команду:

```
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%.

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 с помощью командной строки:

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.

2. Определите наиболее часто проверяемые объекты. Вы можете оптимизировать работу приложения, исключив из проверки неопасные объекты и файлы.

Анализ работы задач выполняется с помощью командной строки. Если устройство находится под управлением политики Kaspersky Security Center, требуется на время проведения исследования разрешить управление локальными задачами.

Анализ потребления ресурсов задачей Защита от файловых угроз

Чтобы 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, выполнив следующую команду:

   ```
   kesl-control --get-task-list
   ```

   b. Получите параметры расписания всех задач типов ODS и ContainerScan, выполнив следующую команду:

   ```
   kesl-control --get-schedule <идентификатор/имя задачи>
   ```

   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, выполнив следующую команду:

   ```
   kesl-control --set-schedule <идентификатор/имя задачи> RuleType=Manual
   ```

3. Включите создание файлов трассировки приложения с высоким уровнем детализации, выполнив следующую команду:

   ```
   kesl-control --set-app-settings TraceLevel=Detailed
   ```

4. Запустите задачу Защита от файловых угроз, если она не запущена, выполнив следующую команду:

   ```
   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). Требуется оптимизировать работу этих задач.

7. Выключите создание файлов трассировки приложения, выполнив следующую команду:

   ```
   kesl-control --set-app-settings TraceLevel=None
   ```

Определение наиболее часто проверяемых объектов

Вы можете получить список объектов, которые были проверены наибольшее количество раз, выполнив следующую команду:

```
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, где 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
```

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, выполнив следующую команду:

```
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
```

Рекомендуется определить, являются ли опасными объекты и файлы, которые были проверены наибольшее количество раз. Неопасные объекты и файлы можно добавить в исключения для оптимизации работы Защиты от файловых угроз и задач проверки. 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.

Рекомендации для Защиты от файловых угроз и задач проверки

Оптимизация Защиты от файловых угроз

Для оптимизации работы компонента Защита от файловых угроз вы можете выполнить следующие действия:

- Настроить исключения из проверки для объектов, которые проверяются наиболее часто, и не являются опасными.
- Настроить исключения из перехвата файловых операций.
- Изменить 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 с помощью команды:

    ```
    kesl-control --set-set 1 ScanByAccessType=Open
    ```

  Изменения, внесенные в файл после открытия, не будут проверяться до следующего обращения к файлу.
- Убедиться, 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`).
- Установить ограничение на использование оперативной памяти приложением.

Оптимизация задач проверки

Для оптимизации работы задач проверки (задач типов ODS и ContainerScan) вы можете выполнить следующие действия:

- Настроить 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.
- Запускать проверку во время наименьшей нагрузки на сервер.
- Убедиться, 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).
- Настроить исключения из проверки для объектов, которые проверяются наиболее часто, и не являются опасными.
- Настроить исключения из перехвата файловых операций.
- Установить ограничение на использование оперативной памяти приложением.

Настройка исключений из проверки

Исключения из проверки позволяют поддерживать баланс между защищенностью и производительностью системы. По мнению вирусных экспертов "Лаборатории Касперского" можно без опасения добавлять в исключения файлы данных и индексные файлы баз данных. Считается, что опасность проникновения вирусов через такие файлы отсутствует.

Вы можете исключить из проверки 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.

Вы можете настроить исключения для Защиты от файловых угроз в политике с помощью Web Console или Консоли администрирования или локально на устройстве с помощью командной строки.

Вы также можете настроить исключения для задач проверки с типами ODS и ContainerScan. Исключения задаются в параметрах задач в Kaspersky Security Center или локально на устройстве с помощью командной строки.

Параметры исключений из проверки для одной задачи проверки не распространяются на другие задачи проверки. Для каждой задачи проверки требуется настроить свои исключения.

Ниже показаны примеры настройки исключений для Защиты от файловых угроз с помощью командной строки.

Чтобы исключить директорию /tmp/logs и все поддиректории и файлы рекурсивно, выполните следующую команду:

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

Чтобы исключить конкретный файл или файлы по маске в директории /tmp/logs, выполните следующую команду:

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

Чтобы исключить по рекурсивной маске все файлы с расширением .log в директории /tmp/ и поддиректориях, выполните следующую команду:

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Настройка исключений 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.

Вы можете получать статистику по файлам, перехваченным приложением, с помощью команды:

```
kesl-control --get-statistic --files
```

Команда позволяет вывести статистические данные о файловых операциях, перехваченных за последние 24 часа.

Если требуется, вы можете выполнить более точный анализ с помощью файлов трассировки приложения. По умолчанию файлы трассировки не создаются. Вы можете включить создание файлов трассировки с помощью команды:

```
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.

Вы можете выключить создание файлов трассировки с помощью команды:

```
kesl-control --set-app-settings TraceLevel=None
```

Анализируя файлы трассировки, вы можете получить список файлов, перехваченных приложением, и определить пути, по которым происходит большое количество перехватов файловых операций. Вы можете получить список перехваченных файлов, выполнив следующую команду:

```
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
```

Чтобы исключить файлы определенной директории не только из проверки, но и из перехвата, нужно исключить точку монтирования целиком. Исключение точек монтирования (глобальное исключение) позволяет исключать из перехвата файловых операций локальные или удаленные директории, смонтированные на устройстве.

Для путей, которые не являются точками монтирования, глобальные исключения не действуют.

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.

Для защиты общих сетевых ресурсов используйте приложение Kaspersky Endpoint Security на том устройстве, где ресурсы хранятся физически.

Вы можете настраивать глобальные исключения в политике с помощью Web Console или Консоли администрирования или локально на устройстве с помощью командной строки.

Ниже показан пример настройки исключения из перехвата файловых операций с помощью командной строки.

Чтобы исключить из перехвата все файлы в директории /tmp:

1. Если директория не является точкой монтирования, нужно создать из нее точку монтирования. Например, чтобы создать точку монтирования из директории /tmp, выполните следующую команду:

   ```
   mount --bind /tmp/ /tmp
   ```

2. Чтобы точка монтирования сохранилась после перезагрузки сервера, добавьте в файл /etc/fstab следующую строку:

   ```
   /tmp /tmp none defaults,bind 0 0
   ```

3. Добавьте директорию /tmp в глобальные исключения, выполнив следующую команду:

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
   ```

4. Если требуется добавить несколько директорий, увеличивайте счетчик item_0000 на единицу (item_0001, item_0002 и так далее).

Установка ограничения на использование 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=<количество памяти в мегабайтах>` 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.

Рекомендации для Защиты от веб-угроз и Защиты от сетевых угроз

Чтобы снизить влияние компонентов Защита от веб-угроз и Защита от сетевых угроз на работу прикладных приложений, рекомендуется выполнить следующие действия.

- Настроить межсетевой экран операционной системы. Если в системе настроены свои (или firewalld) сетевые правила с Drop политиками, то для корректной работы приложения вам нужно добавить разрешающее правило для разрешения входящих соединений локального устройства (loopback).

  Пример команды для iptables:

```
iptables -A INPUT -i lo -j ACCEPT
```

- Чтобы обеспечить совместимость правила REDIRECT (например, перенаправление с 443 порта на 8443) с правилами перехвата компонента Защита от сетевых угроз:

  a. Удалить правило:

  ```
  iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
  ```

  b. Добавить 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
  ```

- Настроить политику 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, вам нужно выбрать локальный способ проверки сертификатов приложением (без использования интернета) или использовать прокси-сервер для доступа в интернет.

  Вы можете выбрать 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 команды:

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  Приложение не будет использовать интернет для проверки сертификатов.

  Вы можете включить использование прокси-сервера и настроить его параметры в политике с помощью Web Console, Консоли администрирования или локально с помощью командной строки.

- Ограничить 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`.

При использовании приложения совместно с балансировщиком HAProxy рекомендуется выполнить следующие действия:

1. Открыть конфигурационный файл /var/opt/kaspersky/kesl/common/kesl.ini, создать секцию `[Environment]` и добавить в нее параметр `TcpSynInterceptDisabled=1`.

2. Перезапустить приложение:

   ```
   systemctl restart kesl
   ```

Совместная работа компонентов Защита от веб-угроз и Защита от сетевых угроз и контейнеризации Kubernetes требует дополнительной тонкой и трудоемкой настройки межсетевого экрана операционной системы. Совместная работа невозможна при использовании Kubernetes с Cillium CNI.

Обновление предыдущей версии приложения

Вы можете обновить до версии Kaspersky Endpoint Security 12.4 для Linux только версию Kaspersky Endpoint Security 12.3 для Linux.

Обновление Kaspersky Endpoint Security более ранних версий до версии 12.4 не предусмотрено. Если у вас установлена более ранняя версия Kaspersky Endpoint Security, вам нужно сначала удалить ее, а затем установить Kaspersky Endpoint Security 12.4 для Linux.

Перед началом обновления приложения Kaspersky Endpoint Security требуется выполнить подготовку к установке.

Процедура обновления приложения состоит из следующих этапов:

1. **Обновление Агента администрирования Kaspersky Security Center**

   Если вы управляете приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, вам нужно обновить 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.

   Во время обновления Агента администрирования приложение продолжает корректно работать.

2. **Обновление плагина управления Kaspersky Endpoint Security**

   Если вы управляете приложением Kaspersky Endpoint Security с помощью Kaspersky Security Center, вам нужно обновить веб-плагин или MMC-плагин управления Kaspersky Endpoint Security, в зависимости от консоли управления Kaspersky Security Center, которую вы используете.

3. **Обновление приложения и графического интерфейса на защищаемых устройствах**

   Вам нужно обновить приложение, установленное на защищаемых устройствах. 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 Агента Endpoint Detection and Response и вы используете графический интерфейс приложения, вам также нужно обновить графический интерфейс.

Вы можете обновлять приложение и графический интерфейс приложения следующими способами:

- Удаленно с помощью Kaspersky Security Center.
- Локально из командной строки.

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).

Независимо от того, было ли приложение Kaspersky Endpoint Security запущено до начала процесса обновления, если обновление завершено успешно, то запустится новая версия приложения.

При обновлении версии приложения файлы дампов предыдущей версии удаляются.

При обновлении версии приложения файл базы данных 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 Агента Endpoint Detection and Response, 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.

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.

В Kaspersky Security Center Web Console процедура конвертации политик и задач 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.

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.

Обновление приложения с помощью Kaspersky Security Center

Обновление приложения и графического интерфейса выполняется путем удаленной установки новой версии пакетов приложения и графического интерфейса на защищаемом устройстве.

> Графический интерфейс не поддерживается, если Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Обновление с помощью Kaspersky Security Center состоит из следующих этапов:

1. Создание инсталляционного пакета.

   Для удаленной установки используется инсталляционный пакет приложения Kaspersky Endpoint Security. Вы можете создать инсталляционный пакет с помощью Kaspersky Security Center Web Console или с помощью Консоли администрирования.

2. Развертывание приложения Kaspersky Endpoint Security на устройствах в сети организации.

   Kaspersky Security Center Web Console поддерживает следующие основные способы развертывания:

   - Установка приложения с помощью мастера развертывания защиты.
   - Установка приложения с помощью задачи удаленной установки приложений.

   Консоль администрирования Kaspersky Security Center поддерживает следующие основные способы развертывания:

   - Установка приложения с помощью мастера удаленной установки.
   - Установка приложения с помощью задачи удаленной установки приложений.

   Описание процедур развертывания см. в справке Kaspersky Security Center.

Обновление приложения с помощью командной строки

Обновление приложения с помощью командной строки выполняется путем установки на устройство новой версии приложения из пакета формата RPM или DEB в соответствии с типом менеджера пакетов.

Графический интерфейс не поддерживается, если Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Если в новой версии приложения изменились условия Лицензионного соглашения и/или Политики конфиденциальности, вам нужно принять новые условия в ходе обновления приложения. Ознакомьтесь с новой версией Лицензионного соглашения и/или Политики конфиденциальности:

- новая версия Лицензионного соглашения расположена в директории ~/.kesl/<версия приложения>/license.<идентификатор языка>;
- новая версия Политики конфиденциальности расположена в директории ~/.kesl/<версия приложения>/license.<идентификатор языка>.

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. Ознакомьтесь с новой версией документа, расположенной в директории ~/.kesl/<версия приложения>/ksn_license.<ID языка>. Отказ от использования Kaspersky Security Network не прерывает процесс обновления приложения Kaspersky Endpoint Security. 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.

Чтобы принять условия новых соглашений в ходе обновления, используйте переменные `KESL_EULA_AGREED=yes`, `KESL_PRIVACY_POLICY_AGREED=yes` и `KESL_USE_KSN=yes/no`.

Чтобы обновить приложение:

1. Установите пакет приложения с помощью следующей команды в соответствии с типом менеджера пакетов. Если у вас установлен графический пользовательский интерфейс приложения предыдущей версии, вам также нужно установить пакет, содержащий файлы графического интерфейса приложения.

   - Для пакета в формате RPM:

     ```
     # [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] rpm -U --replacefiles --replacepkgs kesl-12.4.0-<номер сборки>.<arch>.rpm [kesl-gui-12.4.0-<номер сборки>.<arch>.rpm]
     ```

где <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.

Если на операционной системе с менеджером пакетов типа rpm установлены пакет приложения и пакет графического интерфейса, не рекомендуется обновлять только один из пакетов.

- Для пакета в формате DEB:

  ```
  # [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] apt-get install ./kesl_12.4.0-<номер сборки>_<arch>.deb [./kesl-gui_12.4.0-<номер сборки>_<arch>.deb]
  ```

  где <arch> – тип архитектуры:

  - i386 – для 32-битных операционных систем;
  - amd64 – для 64-битных операционных систем;
  - arm64 – для 64-битных операционных систем для архитектуры Arm.

  Если на операционной системе с менеджером пакетов типа dpkg установлены пакет приложения и пакет графического интерфейса, невозможно обновить только один из пакетов.

2. 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-12.4.0-<номер сборки>.x86_64.rpm kesl-gui-12.4.0-<номер сборки>.x86_64.rpm
```

Если для управления приложением вы используете командную строку, после обновления для большинства параметров приложения используются значения, настроенные для предыдущей версии приложения. Для некоторых параметров устанавливаются особые значения. Параметры, которые отсутствовали в предыдущей версии приложения, в новой версии приложения принимают значения по умолчанию.

Изменения параметров приложения, сделанные после завершения обновления и до перезапуска приложения, не сохраняются.

Особенности установки значений параметров при обновлении приложения

Если для управления приложением вы используете Консоль администрирования Kaspersky Security Center, вы можете выполнить конвертацию политик и задач, чтобы использовать значения параметров политик и задач, настроенных для предыдущей версии приложения (см. подробнее в справке Kaspersky Security Center). В Kaspersky Security Center Web Console процедура конвертации политик и задач 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.

Источники обновления баз

В новой версии приложения в задачах обновления баз произошли следующие изменения:

- Удален параметр **Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны** (`UseKLServersWhenUnavailable`). Вы можете настроить эту функциональность с помощью других параметров задачи.

- Вы можете указать сразу несколько источников обновления баз. Приложение будет использовать их в соответствии с порядком их расположения в списке источников.

После конвертации задач в MMC-плагине источники обновлений настроены следующим образом:

- Если в предыдущей версии был выбран вариант **Серверы обновлений "Лаборатории Касперского"**, то в списке источников будет установлен флажок **Серверы обновлений "Лаборатории Касперского"**.

- Если в предыдущей версии был выбран вариант **Kaspersky Security Center**, то в списке источников будет установлен флажок **Kaspersky Security Center**.

  При этом, если в предыдущей версии был установлен флажок **Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны**, то в списке источников также будет установлен флажок **Серверы обновлений "Лаборатории Касперского"**, а источник **Kaspersky Security Center** будет перемещен на первую строчку списка.

- Если в предыдущей версии был настроен пользовательский источник (вариант **Другие источники в локальной или глобальной сети**), то в список источников будет добавлен пользовательский источник с указанными параметрами (путь или веб-адрес источника), этот флажок будет установлен.

  При этом, если в предыдущей версии был установлен флажок **Использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны**, то в списке источников также будет установлен флажок **Серверы обновлений "Лаборатории Касперского"**, а пользовательский источник будет перемещен на первую строчку списка.

Конвертация политик в веб-плагине не поддерживается.

После обновления приложения с помощью командной строки источники обновлений настроены следующим образом:

- Если в предыдущей версии для параметра `SourceType` было выбрано значение `KLServers`, то в секции **[Sources]** создается источник обновления: `SourceType=KLServers`, `Enabled=Yes`.

- Если в предыдущей версии для параметра `SourceType` было выбрано значение `SCServer`, то в секции **[Sources]** создается источник обновления: `SourceType=SCServer`, `Enabled=Yes`.

  При этом, если в предыдущей версии было задано значение параметра `UseKLServersWhenUnavailable=Yes`, то в секции **[Sources]** создается второй источник обновления: `SourceType=KLServers`, `Enabled=Yes`.

- Если в предыдущей версии для параметра `SourceType` было выбрано значение `Custom` и настроены параметры пользовательского источника в секции **[CustomSources.item_#]**, то в секции **[Sources]** создается пользовательский источник обновления: `SourceType=Custom`, `URL=<путь или веб-адрес источника>`, `Enabled=Yes`.

  При этом, если в предыдущей версии было задано значение параметра `UseKLServersWhenUnavailable=Yes`, то в секции **[Sources]** создается второй источник обновления: `SourceType=KLServers`, `Enabled=Yes`.

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**.

Конвертация политик в веб-плагине не поддерживается.

После обновления приложения с помощью командной строки для параметра `UseKSN` устанавливается значение `No`, если при обновлении вы установили значение параметра `KESL_USE_KSN=No`, и устанавливается значение `UseKSN=Extended`, если вы установили значение параметра `KESL_USE_KSN=Yes`. 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.

Конвертация политик в веб-плагине не поддерживается.

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, требуется:

- при использовании MMC- или веб-плагина выбрать вариант **Расширенный режим KSN** и установить флажок **Включить облачный режим**;
- при использовании командной строки задать для параметра `UseKSN` значение `Basic` или `Extended` и для параметра `CloudMode` значение `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.

Конвертация политик в веб-плагине не поддерживается.

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.

Удаление приложения

Процедура удаления приложения Kaspersky Endpoint Security состоит из следующих этапов:

1. **Удаление приложения и графического интерфейса приложения**

   Вам нужно удалить с защищаемых устройств пакеты приложения и графического интерфейса приложения, если вы использовали графический интерфейс.

   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.

   > В процессе удаления приложения на устройстве будут остановлены все задачи Kaspersky Endpoint Security.

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.

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.

> После удаления приложения удаляется вся информация, сохраненная во время его работы, кроме базы данных лицензий. Удаляются в том числе установленные сертификаты приложения. База данных лицензий сохраняется, вы можете использовать ее для повторной установки приложения. Также сохраняется уникальный идентификатор установки приложения (SensorID).

Если приложение было установлено в systemd-системе, то после удаления приложения параметры systemd возвращаются в исходное состояние.

Об удалении приложения и Агента администрирования с помощью Kaspersky Security Center

Вы можете удаленно удалять с клиентских устройств приложение Kaspersky Endpoint Security и Агент администрирования.

Удаление выполняется с помощью задачи удаленной деинсталляции приложений в Kaspersky Security Center Web Console или в Консоли администрирования. См. подробнее в справке Kaspersky Security Center.

> Если вы хотите удалить только графический пользовательский интерфейс, не удаляя при этом приложение, вам нужно установить значение параметра `USE_GUI=No` в конфигурационном файле autoinstall.ini и запустить задачу удаленной установки приложений.

Удаление выполняется в фоновом режиме. После завершения удаления приложения отобразится запрос на перезагрузку клиентского устройства.

Удаление приложения с помощью командной строки

Удаление пакета приложения и пакета графического интерфейса

Чтобы удалить приложение и графический интерфейс приложения, установленные из пакетов формата RPM, выполните следующую команду:

```
# rpm -e kesl kesl-gui
```

Чтобы удалить приложение и графический пользовательский интерфейс, установленные из пакетов формата DEB, выполните следующую команду:

```
# apt-get purge kesl kesl-gui
```

Удаление пакета приложения без удаления пакета графического интерфейса

Чтобы удалить приложение, установленное из пакета формата RPM, без удаления графического интерфейса приложения, выполните следующую команду:

```
# rpm -e kesl
```

Чтобы удалить приложение, установленное из пакета формата DEB, без удаления графического интерфейса приложения, выполните следующую команду:

```
# apt-get purge kesl
```

Удаление пакета графического интерфейса

Чтобы удалить графический интерфейс приложения, установленный из пакета формата RPM, выполните следующую команду:

```
# rpm -e kesl-gui
```

Чтобы удалить графический интерфейс приложения, установленный из пакета формата DEB, выполните следующую команду:

```
# apt-get purge kesl-gui
```

После завершения процедуры удаления выводится сообщение о результатах удаления.

Удаление Агента администрирования с помощью командной строки

Чтобы удалить Агент администрирования, установленный на 32-битную операционную систему из пакета формата RPM, выполните следующую команду:

```
# rpm -e klnagent
```

Чтобы удалить Агент администрирования, установленный на 64-битную операционную систему из пакета формата RPM, выполните следующую команду:

```
# rpm -e klnagent64
```

Чтобы удалить Агент администрирования, установленный на 32-битную операционную систему из пакета формата DEB, выполните следующую команду:

```
# apt-get purge klnagent
```

Чтобы удалить Агент администрирования, установленный на 64-битную операционную систему из пакета формата DEB, выполните следующую команду:

```
# apt-get purge klnagent64
```

После завершения процедуры удаления выводится сообщение о результатах удаления.

Удаление плагинов управления Kaspersky Endpoint Security

Удаление веб-плагина управления Kaspersky Endpoint Security выполняется в Kaspersky Security Center Web Console в списке установленных плагинов (**Параметры** → **Веб-плагины**).

Чтобы 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**.

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложений "Лаборатории Касперского", а также информацию об особенностях активации приложения Kaspersky Endpoint Security.

После активации приложения рекомендуется следить за сроком действия лицензии, которую использует приложение, чтобы своевременно продлевать срок действия лицензии. Вы можете просматривать информацию о лицензионных ключах, которые использует приложение Kaspersky Endpoint Security с помощью Kaspersky Security Center или с помощью командной строки на защищенном устройстве.

О Лицензионном соглашении

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>.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Endpoint Security, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *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 использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая*

  Платная лицензия.

  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.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

Для активации приложения Kaspersky Endpoint Security требуется лицензия, которая включает в себя основную функциональность приложения. Основная лицензия также может включать в себя дополнительную функциональность приложения (например, функциональность интеграции с решениями Detection and Response от "Лаборатории Касперского"). Если основная лицензия, по которой вы используете приложение, не включает нужную вам дополнительную функциональность, вам нужно приобрести отдельную лицензию для активации дополнительной функциональности.

Объем функциональности, включенный в основную лицензию и в лицензию для дополнительной функциональности, уточняйте у партнера "Лаборатории Касперского", у которого вы приобретаете лицензию.

О Лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О лицензионном ключе

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".

Для активации приложения вам требуется основной лицензионный ключ. Если основная лицензия, по которой вы используете приложение, не включает в себя нужную вам дополнительную функциональность (например, функциональность Kaspersky Endpoint Detection and Response Optimum), вам также требуется лицензионный ключ для дополнительной функциональности.

Вы можете добавить лицензионный ключ на защищенное устройство одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его на защищенное устройство.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы приложения требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть добавлен как активный или как резервный.

- *Активный лицензионный ключ* – лицензионный ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен ключ для пробной лицензии, ключ для коммерческой лицензии (коммерческий ключ) или ключ по подписке. Вы можете добавить в качестве активного ключа только один основной лицензионный ключ. Активных лицензионных ключей для дополнительной функциональности может быть несколько.
- *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.

  Чтобы продлить срок действия основной лицензии приложения, вы можете добавить резервный ключ для основной функциональности. Если вы активировали дополнительную функциональность по отдельной лицензии, вы можете также добавить резервный ключ для дополнительной функциональности.

  Резервный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа того же типа.

  > Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве резервного лицензионного ключа.

О коде активации

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

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.

О файле ключа

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

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

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

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

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

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

О подписке

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

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

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

Набор возможных действий для управления подпиской может различаться в зависимости от поставщика услуг. Поставщик услуг может не предоставлять льготный период, в течение которого сохраняется функциональность приложения, для продления подписки.

Чтобы использовать приложение Kaspersky Endpoint Security по подписке, вам нужно применить код активации, предоставленный поставщиком услуг. После применения кода активации в приложение добавляется активный ключ, соответствующий лицензии на использование приложения по подписке. При этом резервный ключ может быть добавлен только с помощью кода активации и не может быть добавлен с помощью файла ключа или по подписке.

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

Сравнение функций приложения в зависимости от лицензии

Набор доступных функций приложения Kaspersky Endpoint Security зависит от вида основной лицензии.

Основная лицензия, по которой используется приложение, может включать в себя и основную, и дополнительную функциональность приложения. Например, лицензия "Kaspersky Optimum Security" позволяет активировать основные компоненты защиты и контроля, а также функциональность интеграции с Kaspersky Endpoint Detection and Response Optimum.

Для активации дополнительной функциональности приложения также могут использоваться отдельные лицензии, например лицензия для активации функциональности Kaspersky Unified Monitoring and Analysis Platform.

Объем функциональности, включенный в основную лицензию и в лицензию для дополнительной функциональности, уточняйте у партнера "Лаборатории Касперского", у которого вы приобретаете лицензию.

Открыть список функций решения, доступных по основным лицензиям приложения

Активация приложения и управление лицензионными ключами

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

Для активации приложения Kaspersky Endpoint Security на защищенном устройстве требуется добавить основной лицензионный ключ в приложение. Если основная лицензия, по которой вы используете приложение, не включает в себя нужную вам дополнительную функциональность приложения Kaspersky Endpoint Security, вам также требуется добавить в приложение лицензионный ключ для дополнительной функциональности:

- отдельный лицензионный ключ "Kaspersky Endpoint Detection and Response Optimum Add-on" (далее также "ключ EDR Optimum") – для активации компонента EDR Optimum;
- отдельный лицензионный ключ "Kaspersky Unified Monitoring and Analysis Platform Add-on" (далее также "ключ KUMA") – для активации функциональности Kaspersky Unified Monitoring and Analysis Platform;
- отдельный лицензионный ключ "Kaspersky Managed Detection and Response Optimum/Expert Add-on" (далее также "ключ MDR") – для активации компонента MDR;
- отдельный лицензионный ключ "Kaspersky Endpoint Detection and Response Expert (on-premise) Add-on" (далее также "ключ EDR Expert (on-premise)") – для активации компонента EDR Expert (on-premise).

Ключ EDR Expert (on-premise) также используется для активации приложения Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response. В этом режиме не требуется добавлять в приложение основной лицензионный ключ.

Вы можете добавлять лицензионные ключи в приложение одним из следующих способов:

- с помощью файла ключа;
- с помощью кода активации.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, активировать приложение не требуется. Вы активируете решение Kaspersky Security для виртуальных сред Легкий агент. Активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионного ключа на SVM. Лицензионный ключ для активации дополнительной функциональности тоже добавляется на SVM при необходимости.

Если вы не активировали приложение Kaspersky Endpoint Security во время установки (путем добавления ключа в инсталляционный пакет или при выполнении первоначальной настройки), вам нужно активировать установленное приложение одним из следующих способов:

- Удаленно через Kaspersky Security Center:
  - С помощью задачи добавления ключа в приложение.
  - Путем распространения на клиентские устройства лицензионного ключа, размещенного на Сервере администрирования.
- В командной строке с помощью команд управления.

Для добавления в приложение лицензионного ключа для дополнительной функциональности вы также можете использовать задачу добавления ключа, процедуру распространения ключа на клиентские устройства или команды управления лицензионными ключами. Добавление ключа для дополнительной функциональности ничем не отличается от добавления основного лицензионного ключа приложения.

Если приложение Kaspersky Endpoint Security используется в стандартном режиме, ключ для дополнительной функциональности может быть добавлен только после добавления основного лицензионного ключа приложения.

Вы также можете добавить в приложение резервный ключ для основной функциональности приложения и резервный ключ для дополнительной функциональности. Резервный ключ становится активным либо по истечении срока действия лицензии, связанной с активным ключом, либо при удалении активного ключа. Наличие резервного ключа позволяет избежать ограничения функциональности приложения в момент окончания срока действия лицензии.

Резервный ключ может быть добавлен только после добавления активного лицензионного ключа.

Вы можете посмотреть информацию о лицензионных ключах, добавленных в приложение, удаленно с помощью Kaspersky Security Center или с помощью командной строки на защищенном устройстве.

Вы также можете активировать приложение и управлять лицензионными ключами через графический пользовательский интерфейс.

Активация приложения с помощью Kaspersky Security Center

Вы можете добавлять лицензионные ключи в приложение через Kaspersky Security Center следующими способами:

- С помощью задачи добавления ключа в приложение.

  Этот способ позволяет добавить лицензионный ключ на конкретное устройство или устройства, входящие 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 активации.

- Путем распространения на клиентские устройства лицензионного ключа, размещенного на Сервере администрирования Kaspersky Security Center.

  Этот способ позволяет автоматически добавлять ключ на клиентские устройства, уже подключенные к Kaspersky Security Center, а также на новые клиентские устройства. Для использования этого способа требуется сначала добавить ключ в хранилище ключей Kaspersky Security Center.

Для создания задачи добавления ключа в приложение, задачи добавления ключа в хранилище ключей и задачи распространения ключа на клиентские устройства вы можете использовать Kaspersky Security Center Web Console или Консоль администрирования Kaspersky Security Center.

Добавление ключей с помощью Kaspersky Security Center Web Console

Чтобы 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.

Чтобы добавить ключ в приложение через Web Console с помощью задачи Добавление ключа:

1. В главном окне Web Console выберите **Активы (Устройства)** → **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 **Хранилище ключей Kaspersky Security Center**.
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, нажмите на кнопку **Добавить 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. Завершите работу мастера.

   В списке задач отобразится новая задача.

9. Установите флажок напротив задачи. Нажмите на кнопку **Запустить**.

В свойствах задачи *Добавление ключа* вы можете добавить в приложение *резервный ключ*. Резервный ключ становится активным либо по истечении срока действия лицензии, связанной с активным ключом, либо при удалении активного ключа. Наличие резервного ключа позволяет избежать ограничения функциональности приложения в момент окончания срока действия лицензии.

Если вы добавляете резервный ключ, но активный ключ еще не добавлен в приложение, задача завершается с ошибкой.

Чтобы добавить ключ через Web Console путем распространения на устройства ключа, размещенного на Сервере администрирования:

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 закладке **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.

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 закладке **Устройства**.

Особенности активации в Kaspersky Security Center Cloud Console

Для Kaspersky Security Center Cloud Console предусмотрена пробная версия. *Пробная версия* – это специальная версия Kaspersky Security Center Cloud Console, предназначенная для ознакомления пользователя с функциями Cloud Console. В этой версии 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. Дополнительная информация о Cloud Console приведена в документации Kaspersky Security Center Cloud Console.

Пробная версия Kaspersky Security Center Cloud Console не позволяет впоследствии перейти на коммерческую версию. Любое пробное рабочее пространство будет автоматически удалено со всем его содержимым по истечении тридцати дней.

Управление лицензионными ключами в командной строке

Для управления лицензионными ключами на устройстве вы можете использовать команды управления лицензионными ключами.

Команды управления лицензионными ключами могут быть выполнены, только если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, команды управления лицензионными ключами завершаются с ошибкой. Вы активируете приложение в составе решения Kaspersky Security для виртуальных сред Легкий агент, отдельно активировать приложение не требуется.

Чтобы добавить в приложение активный лицензионный ключ, выполните команду:

```
kesl-control [-L] --add-active-key <путь к файлу ключа / код активации>
```

где:

- `путь к файлу ключа` – путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.
- `код активации` – код активации.

Чтобы добавить в приложение резервный лицензионный ключ, выполните команду:

```
kesl-control [-L] --add-reserve-key <путь к файлу ключа / код активации>
```

Если активный ключ еще не добавлен в приложение на устройстве, команда завершается с ошибкой.

С помощью команды добавления ключа вы можете добавлять как основные лицензионные ключи приложения, так и лицензионные ключи для дополнительной функциональности. Указывать тип ключа в команде не требуется.

Для удаления основных лицензионных ключей и ключей для дополнительной функциональности предусмотрены разные команды.

Чтобы удалить основной активный ключ, выполните команду:

```
kesl-control [-L] --remove-active-key
```

Чтобы удалить основной резервный ключ, выполните команду:

```
kesl-control [-L] --remove-reserve-key
```

Чтобы удалить активный ключ EDR Optimum, выполните команду:

```
kesl-control [-L] --remove-active-key --edr-optimum
```

Чтобы удалить резервный ключ EDR Optimum, выполните команду:

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

Чтобы удалить активный ключ KUMA, выполните команду:

```
kesl-control [-L] --remove-active-key --kuma
```

Чтобы удалить резервный ключ KUMA, выполните команду:

```
kesl-control [-L] --remove-reserve-key --kuma
```

Чтобы удалить активный ключ MDR, выполните команду:

```
kesl-control [-L] --remove-active-key --mdr
```

Чтобы удалить резервный ключ MDR, выполните команду:

```
kesl-control [-L] --remove-reserve-key --mdr
```

Чтобы удалить активный ключ EDR Expert (on-premise), выполните команду:

```
kesl-control [-L] --remove-active-key --edr-kata
```

Чтобы удалить резервный ключ EDR Expert (on-premise), выполните команду:

```
kesl-control [-L] --remove-reserve-key --edr-kata
```

Просмотр информации об используемых лицензионных ключах

Вы можете просматривать информацию о лицензионных ключах, которые использует приложение Kaspersky Endpoint Security, следующими способами:

- В Kaspersky Security Center в свойствах задачи добавления ключа.

  В свойствах задачи *Добавление ключа* отображаются сведения о ключе, который добавляется в приложение в результате выполнения этой задачи.

- В Kaspersky Security Center в свойствах приложения "Лаборатории Касперского", установленного на клиентском устройстве.

  В свойствах приложения Kaspersky Endpoint Security на защищенном устройстве отображается информация об активном и резервном ключах, добавленных в приложение на этом устройстве. Вы можете просматривать свойства приложения с помощью Web Console, а также с помощью Консоли администрирования.

- В Kaspersky Security Center в отчете об использовании лицензионных ключей.

  Вы можете просматривать отчет об использовании ключей с помощью Web Console (**Мониторинг и отчеты** → **Отчеты**), а также с помощью Консоли администрирования (закладка **Отчеты**). Чтобы посмотреть отчет, вам нужно выбрать в списке отчетов шаблон "Отчет об использовании лицензионных ключей" и запустить формирование отчета.

- В Kaspersky Security Center в хранилище лицензионных ключей 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**). В хранилище отображаются сведения обо всех ключах, добавленных на Сервер администрирования Kaspersky Security Center.

- На устройстве с установленным приложением Kaspersky Endpoint Security. Вы можете посмотреть информацию о лицензии, которую использует приложение Kaspersky Endpoint Security, с помощью командной строки.

Вы также можете получать информацию об используемых лицензионных ключах и связанных и 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.

Если приложение Kaspersky Endpoint Security используется в стандартном режиме или в режиме Агента Endpoint Detection and Response 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.

Просмотр информации о ключах на устройстве через Web Console

Чтобы просмотреть в Web Console информацию о лицензионных ключах, добавленных на устройство:

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 выберите в открывшемся окне группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. В списке найдите устройство, информацию о котором вы хотите просмотреть, и нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.

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

6. В открывшемся окне свойств приложения откройте закладку **Общие**, раздел **Лицензии**.

   В разделе отображается информация о лицензионных ключах, добавленных в приложение, и связанных с этими ключами лицензиях:

   - **Статус лицензионного ключа** – статус 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.

Просмотр информации о ключах на устройстве через Консоль администрирования

Чтобы просмотреть в Консоли администрирования Kaspersky Security Center информацию о лицензионных ключах, добавленных на устройство:

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 закладку **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.

Просмотр информации о лицензии и ключе в командной строке

В командной строке с помощью команды `-L --query` вы можете просматривать информацию об активном и резервном лицензионных ключах, добавленных в приложение, и о лицензии, по которой активировано приложение. Если в приложение добавлен отдельный ключ для активации дополнительной функциональности, также отображается информация о добавленных активном и резервном лицензионных ключах для дополнительной функциональности.

Чтобы посмотреть информацию о лицензионных ключах и лицензии на устройстве, выполните следующую команду:

```
kesl-control -L --query [--json]
```

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

В результате выполнения команды в консоль будет выведена следующая информация:

- Информация об активном основном лицензионном ключе, если ключ добавлен:
  - Дата и время окончания срока действия лицензии, по которой используется приложение.
  - Количество дней до окончания срока действия лицензии.
  - Информация об ограничении функций защиты.
  - Информация об ограничении функции 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 основном лицензионном ключе. Отображается, если приложение используется в стандартном режиме и резервный ключ добавлен. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, информация о резервном ключе не отображается, резервный ключ добавляется на SVM.
  - Дата и время окончания срока действия лицензии, по которой используется приложение.
  - Информация об ограничении функций защиты.
  - Информация об ограничении функции 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.

- Информация об активном ключе для дополнительной функциональности, если добавлен отдельный ключ:
  - Дата и время окончания срока действия лицензии для активации дополнительной функциональности.
  - Количество дней до окончания срока действия лицензии.
  - Информация об ограничении функции 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 ключе для дополнительной функциональности. Отображается, если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response и добавлен резервный ключ для дополнительной функциональности. Если приложение используется в режиме Легкого агента для защиты виртуальных сред, информация о резервном ключе не отображается, резервный ключ добавляется на SVM.
  - Дата и время окончания срока действия лицензии для активации дополнительной функциональности.
  - Информация об ограничении функции 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 с помощью команды `kesl-control --app-info`.

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 Агента Endpoint Detection and Response 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 Агента Endpoint Detection and Response 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 для защиты виртуальных сред 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-premise)

Если вы используете Kaspersky Endpoint Security как часть решения Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise)

При интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise).
- Открытый ключ сертификата сервера, обеспечивающего интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise).
- Сертификат клиента для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise).
- Учетные данные для авторизации на прокси-сервере.
- Параметры частоты синхронизации с сервером, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise), и параметры передачи данных на сервер.
- Статус соединения с сервером, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise), и сведения об ошибках сертификата клиента и сертификата сервера.
- Параметры задач, поступающих от серверов, обеспечивающих интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise):
  - 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-premise) приложение сохраняет и может передавать серверу, обеспечивающему интеграцию, 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 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-premise).
    - 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 сетевого соединения:
  - Локальный IP-адрес.
  - Удаленный IP-адрес.
  - Направление соединения.
  - Протокол.
- 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.
  - Информация о процессе, осуществившем внедрение кода, и о его родительском процессе.
    - Идентификатор процесса и уникальный идентификатор процесса и родительского процесса.
    - Командная строка, 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.

- Информация 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.
- Информация о процессе, являющемся инициатором процесса.
  - Идентификатор процесса и уникальный идентификатор процесса, являющегося инициатором процесса.
  - Командная строка 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.

Концепция управления приложением

Для управления приложением Kaspersky Endpoint Security вы можете использовать:

- Kaspersky Security Center;
- командную строку;
- графический интерфейс приложения.

> 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.

Набор действий, которые вы можете выполнять с помощью графического интерфейса приложения Kaspersky Endpoint Security, ограничен.

В этом разделе описаны особенности управления приложением через Kaspersky Security Center и командную строку, а также основные приемы работы в консолях управления Kaspersky Security Center и в командной строке.

Управление приложением 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.

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 для Консоли администрирования на основе MMC (далее также "MMC-плагин").

- 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, которое имеет доступ к Серверу администрирования.

  Интерфейс для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center Web Console обеспечивает веб-плагин управления (далее также "веб-плагин").

- 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 для защиты виртуальных сред.

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.

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).

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.

Независимо от консоли управления Kaspersky Security Center, которую вы используете, 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 Kaspersky Endpoint Security (см. подробнее в документации Kaspersky Security Center).

О плагинах управления Kaspersky Endpoint Security

Для управления приложением Kaspersky Endpoint Security через Kaspersky Security Center требуются следующие плагины управления:

- Веб-плагин управления Kaspersky Endpoint Security (далее также *веб-плагин*) обеспечивает взаимодействие приложения Kaspersky Endpoint Security с приложением Kaspersky Security Center через Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console.

  Веб-плагин требуется установить на устройство с установленным приложением Kaspersky Security Center Web Console. Управление приложением Kaspersky Endpoint Security с помощью веб-плагина доступно всем администраторам, у которых есть доступ к Kaspersky Security Center Web Console в браузере.

- MMC-плагин управления Kaspersky Endpoint Security (далее также *MMC-плагин*) обеспечивает взаимодействие приложения Kaspersky Endpoint Security с Kaspersky Security Center через Консоль администрирования.

  MMC-плагин требуется установить на устройство с установленной Консолью администрирования Kaspersky Security Center.

Плагины управления Kaspersky Endpoint Security позволяют управлять приложением Kaspersky Endpoint Security с помощью политик и задач.

Дополнительная информация о плагинах управления приведена в документации Kaspersky Security Center.

Если в Kaspersky Security Center Web Console 16.0 или Kaspersky Security Center Web Console 16.1 установлены веб-плагины Kaspersky Endpoint Security для Windows (сборка 12.11.0.2004) и Kaspersky Endpoint Security для Linux (сборка 12.4.0.1354), то обновление версии веб-плагина Kaspersky Endpoint Security для Windows до версии 12.11.0.6004 может привести к сбоям в работе политик Kaspersky Endpoint Security для Linux. В этом случае перейдите в окно **Параметры** → **Веб-плагины** и удалите из списка веб-плагины Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux и Unified Protection and Management Plug-in. Далее установите сначала веб-плагин Kaspersky Endpoint Security для Linux, затем – веб-плагин Kaspersky Endpoint Security для Windows.

О политиках Kaspersky Security Center

Политика – это набор параметров приложения Kaspersky Endpoint Security, которые применяются для всех клиентских устройств, входящих в состав группы администрирования.

Для одного приложения вы можете настроить несколько политик с различными значениями параметров. Однако одновременно для приложения может быть активна только одна политика в пределах группы администрирования. При создании новой политики все остальные политики в группе администрирования становятся неактивными. Вы можете изменить статус политики позже.

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

Вы можете локально изменять значения параметров, заданные политикой, для отдельных устройств в группе администрирования, если изменение этих параметров не запрещено политикой.

Каждый параметр политики имеет атрибут "замок", который показывает, наложен ли запрет на изменение параметров в дочерних политиках и локально в параметрах приложения. Возможность изменять параметр приложения на клиентском устройстве определяется статусом "замка" у параметра в свойствах политики:

- Если параметр закрыт "замком" (🔒), это означает, что вы не можете изменить значение параметра локально или в политиках вложенного уровня иерархии. Для всех клиентских устройств группы администрирования и вложенных групп используется значение параметра, заданное этой политикой.

- Если параметр не закрыт "замком" (🔓), это означает, что вы можете изменить значение параметра локально или в политиках вложенного уровня иерархии. Если для клиентских устройств группы администрирования значения параметра заданы локально или в политиках вложенного уровня иерархии, то значение параметра, заданное в свойствах политики, не применяется.

В веб-плагине и MMC-плагине количество параметров с "замками" отличается. В веб-плагине присутствуют "замки", которых нет в MMC-плагине.

Для некоторых списков вы можете включить объединение элементов списка. Для объединения элементов списка требуется выполнить следующие действия:

- В свойствах дочерней политики на закладке **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.

Профиль политики может содержать параметры, 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. Вы можете создавать и настраивать профили в свойствах политики в разделе **Профили политики**.

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.

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.

Настройки ранее удаленной политики продолжают применяться на устройстве до тех пор, пока устройство не получит новую политику или пока на устройстве не изменят настройки локально.

Подробнее о политиках и профилях политик, а также о механизме наследования параметров см. в справке Kaspersky Security Center.

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 наборов устройств для выполнения на нескольких устройствах, независимо от их вхождения в группы администрирования.

  Задачи для наборов устройств выполняются только на устройствах, указанных в параметрах задачи. Если в выборку устройств, для которой сформирована задача, добавлены новые устройства, то для них эта задача не выполняется. В этом случае вам нужно создать новую задачу или изменить параметры уже существующей задачи.

Вы можете создавать любое количество групповых задач, задач для наборов устройств и локальных задач.

Задачи выполняются, только если на устройствах запущено приложение Kaspersky Endpoint Security.

Общая информация о задачах, созданных в Kaspersky Security Center, приведена в справке Kaspersky Security Center.

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.
- *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.

Набор параметров и значения по умолчанию для параметров задач зависят от типа лицензии. Задачи *Добавление ключа, Обновление* и *Откат обновления* баз неприменимы, 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 политиками в Web Console

Вы можете выполнять следующие действия с политиками в Web Console:

- Создавать политику.
- Изменять параметры политики. Вы можете настраивать параметры политики на закладке **Параметры приложения** окна свойств политики. Параметры политики в Web Console описаны в Приложении 5.

  Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Экспортировать и импортировать параметры политики.

  Экспорт и импорт параметров политики из версии Kaspersky Endpoint Security 12.3 для Linux в версию Kaspersky Endpoint Security 12.4 для Linux не поддерживается.

- Копировать и перемещать политику.
- Удалять политику.
- Изменять статус политики.
- Создавать профили политики.

Общую информацию о работе с политиками см. в справке Kaspersky Security Center.

Создание политики в Web Console

Чтобы создать политику в Web Console:

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

   Откроется список политик и профилей политик.

2. Выберите группу администрирования, содержащую устройства, на которых должна применяться политика. Для этого нажмите на ссылку в поле **Текущий путь**, расположенном над списком политик и профилей политик, и выберите группу администрирования в открывшемся окне.

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.

   - **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.

6. Если вы используете приложение в режиме Легкого агента для защиты виртуальных сред, 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 (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.

   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 **Подключение 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, в окне отображается 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 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. Откроется окно параметров созданной политики на закладке **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 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.

     - **Обеспечить принудительное наследование параметров для дочерних политик**. Если переключатель включен, значения параметров политики будут распространены на дочерние политики. В свойствах дочерней политики будет автоматически включен и недоступен для выключения переключатель **Наследовать параметры родительской политики**. Параметры дочерней политики наследуются из родительской политики, кроме параметров, для которых "замок" открыт (🔓). По умолчанию переключатель выключен.

   Общая информация о параметрах политик приведена в справке Kaspersky Security Center.

9. Если вы хотите настроить другие параметры политики, перейдите на закладку **Параметры приложения** и внесите необходимые изменения.

   Вы также можете изменить параметры политики позже.

10. Нажмите на кнопку **Сохранить**.

    Созданная политика появится в списке политик.

Общую информацию об управлении политиками см. в справке Kaspersky Security Center.

Изменение параметров политики в Web Console

Чтобы изменить параметры политики в Web Console:

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

   Откроется список политик.

2. Выберите группу администрирования, содержащую устройства, на которых применяется политика. Для этого нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите группу администрирования в открывшемся окне.

   В списке отобразятся политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.

   Откроется окно свойств политики.

4. Измените параметры политики на закладке **Параметры приложения**.

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

Политика будет сохранена с обновленными параметрами.

Параметры политики в Web Console

Набор параметров и значения по умолчанию для параметров политики зависят от лицензии, по которой активировано приложение. Некоторые параметры политики применяются или не применяются в работе приложения в зависимости от режима, в котором используется приложение.

Вы можете настраивать параметры политики на закладке **Параметры приложения** окна свойств политики.

Параметры политики в Web Console описаны в Приложении 5.

Параметры политики

Раздел	Подразделы
Защита устройств от угроз	**Защита от файловых угроз**. В этом подразделе вы можете управлять защитой от файловых угроз. **Защита от атак BadUSB**. В этом подразделе вы можете настраивать параметры защиты от атак BadUSB. **Проверка съемных дисков**. В этом подразделе вы можете настраивать параметры проверки съемных дисков при подключении их к защищаемому устройству. **Анализ поведения**. В этом подразделе вы можете настраивать параметры анализа поведения приложений. **Защита от шифрования**. В этом подразделе вы можете настраивать параметры защиты от удаленного вредоносного шифрования. **Защита от эксплойтов**. В этом подразделе вы можете настраивать параметры защиты от эксплойтов.
Защита сетевых соединений и средств коммуникации	**Защита от почтовых угроз**. В этом подразделе вы можете настраивать параметры защиты от почтовых угроз. **Защита от веб-угроз**. В этом подразделе вы можете настраивать параметры защиты от веб-угроз. **Защита от сетевых угроз**. В этом подразделе вы можете настраивать параметры защиты от сетевых угроз. **Сетевой экран**. В этом подразделе вы можете настраивать параметры управления сетевым экраном.

Раздел	Подразделы
Контроль безопасности	**Контроль устройств**. В этом подразделе вы можете настраивать параметры контроля устройств. **Веб-Контроль**. В этом подразделе вы можете настраивать параметры Веб-Контроля. **Контроль приложений**. В этом подразделе вы можете настраивать параметры контроля приложений. **Контроль целостности системы**. В этом подразделе вы можете настраивать параметры контроля целостности системы.
Доверенная зона	В этом разделе вы можете настраивать следующие параметры: • Исключения, которые применяются в работе компонента Защита от файловых угроз. • Исключения, которые применяются в работе компонента Защита от веб-угроз. • Исключения, которые применяются в работе компонента Защита от сетевых угроз. • Исключения из проверки сетевого трафика. • Исключение точек монтирования из перехвата файловых операций. • Доверенные устройства, которые применяются в работе компонента Контроль устройств.
Общие настройки	**Настройки обнаружения**. В этом подразделе вы можете настраивать следующие параметры: • Обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным. • Режим перехвата файловых операций. **Kaspersky Security Network**. В этом подразделе вы можете настраивать использование Kaspersky Security Network в работе приложения Kaspersky Endpoint Security. **Взаимодействие с пользователем**. В этом подразделе вы можете настраивать следующие параметры: • Параметры запуска приложения. • Разрешения для пользователей на управление задачами. **Производительность**. В этом подразделе вы можете настраивать следующие параметры: • Отмена запуска запланированных задач на устройстве, работающем от аккумулятора. • Исключение памяти процессов из проверки. • Ограничение на использование памяти и ресурсов процессора для задач проверки. • Ограничение на использование резидентной памяти приложением. • Отслеживание стабильности работы приложения. **Настройки сети**. В этом подразделе вы можете настраивать: • Параметры прокси-сервера, если доступ пользователей с клиентских устройств в интернет осуществляется через прокси-сервер. • Параметры проверки сетевого трафика. **Проверка контейнеров**. В этом подразделе вы можете настраивать работу компонента Мониторинг контейнеров. **Служба технической поддержки**. В этом подразделе вы можете настраивать параметры трассировки и записи дампов. **Отчеты и хранилище**. В этом подразделе вы можете настраивать параметры резервного хранилища и карантина. **Интеграция с KSC**. В этом подразделе вы можете настраивать параметры отправки информации в хранилище Kaspersky Security Center. **Настройки взаимодействия с ОС**. В этом подразделе вы можете: • Выбирать механизм, который приложение должно использовать для **перехвата системных событий**. В Web Console вы можете настраивать параметры перехвата системных событий в свойствах политики (**Параметры приложения → Общие настройки → Настройки взаимодействия с ОС**). Параметры применяются только на устройствах, где операционная система поддерживает технологию fanotify. • Настраивать дополнительные параметры сбора телеметрии. **Настройки уведомлений**. В этом подразделе вы можете настраивать параметры уведомлений о событиях.

Раздел	Подразделы
Встроенные агенты	**Managed Detection and Response**. В этом подразделе вы можете включать и выключать интеграцию с Kaspersky Managed Detection and Response и загружать файл MDR BLOB, необходимый для интеграции. **Network Detection and Response (KATA)**. В этом подразделе вы можете включать и выключать интеграцию с Kaspersky Network Detection and Response (KATA). **Endpoint Detection and Response**. В этом подразделе вы можете включать и выключать интеграцию с Kaspersky Detection and Response Optimum и настраивать параметры интеграции. **Endpoint Detection and Response Expert (on-premise)**. В этом подразделе вы можете включать и выключать интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise) или с Kaspersky Endpoint Detection and Response (KATA) и настраивать параметры интеграции. **Sandbox**. В этом подразделе вы можете включать и выключать интеграцию с Sandbox и настраивать параметры интеграции. **Интеграция с KUMA**. В этом подразделе вы можете включать и выключать интеграцию с Kaspersky Unified Monitoring and Analysis Platform и настраивать параметры интеграции.
Режим Легкого агента Параметры в этом разделе применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.	**Настройки обнаружения SVM**. В этом подразделе вы можете выбрать способ, который используют Легкие агенты для обнаружения доступных для подключения SVM. **Настройки подключения к Серверу интеграции**. В этом подразделе вы можете настроить подключение Легких агентов к Серверу интеграции, компоненту Kaspersky Security для виртуальных сред Легкий агент. **Тег для подключения к SVM**. В этом подразделе вы можете включить использование тегов Легким агентом и назначить тег, который Легкий агент будет использовать для подключения. **Алгоритм выбора SVM**. В этом подразделе вы можете указать, какой алгоритм выбора SVM должны использовать Легкие агенты. **Защита соединения**. В этом подразделе вы можете включить шифрование канала передачи данных между Легким агентом и Сервером защиты.

Управление политиками в Консоли администрирования

Вы можете выполнять следующие действия с политиками в Консоли администрирования Kaspersky Security Center:

- Создавать политику.
- Изменять параметры политики. Вы можете настраивать параметры политики в окне свойств политики.

  Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Экспортировать и импортировать параметры политики.
- Удалять политику.
- Изменять статус политики.
- Создавать профили политики.

Общую информацию о работе с политиками см. в справке Kaspersky Security Center.

Создание политики с помощью Консоли администрирования

Чтобы 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 закладке **Устройства** папки с названием группы администрирования вы можете просмотреть список устройств, которые входят в состав этой группы администрирования.

2. В рабочей области выберите закладку **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 для защиты виртуальных сред, 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 (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.

   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 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.

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, в окне отображается 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 закладке **Политики** и в папке **Политики** дерева консоли.

Вы можете изменить параметры политики позже. Общую информацию об управлении политиками см. в справке Kaspersky Security Center.

Изменение параметров политики в Консоли администрирования Kaspersky Security Center

Чтобы изменить параметры политики 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 закладку **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. Измените параметры политики.
5. В окне **Свойства: <Название политики>** нажмите на кнопку **OK**, чтобы сохранить изменения.

Параметры политики в Консоли администрирования

Набор параметров и значения по умолчанию для параметров политики зависят от лицензии, по которой активировано приложение. Некоторые параметры политики применяются или не применяются в работе приложения в зависимости от режима, в котором используется приложение.

Вы можете настраивать параметры политики в разделах и подразделах окна свойств политики. О настройке общих параметров политики и параметрах событий см. в справке Kaspersky Security Center.

Параметры политики

Раздел	Подразделы
Базовая защита	**Защита от файловых угроз**. В этом подразделе вы можете управлять защитой от файловых угроз. **Исключения Защиты от файловых угроз**. В этом подразделе вы можете настраивать исключения, которые применяются в работе компонента Защита от файловых угроз. **Управление сетевым экраном**. В этом подразделе вы можете настраивать параметры управления сетевым экраном. **Защита от веб-угроз**. В этом подразделе вы можете настраивать параметры защиты от веб-угроз. **Защита от почтовых угроз**. В этом подразделе вы можете настраивать параметры защиты от почтовых угроз. **Защита от сетевых угроз**. В этом подразделе вы можете настраивать параметры защиты от сетевых угроз. **Защита от атак BadUSB**. В этом подразделе вы можете настраивать параметры защиты от атак BadUSB.
Продвинутая защита	**Kaspersky Security Network**. В этом подразделе вы можете настраивать использование Kaspersky Security Network в работе приложения Kaspersky Endpoint Security. **Защита от шифрования**. В этом подразделе вы можете настраивать параметры защиты от удаленного вредоносного шифрования. **Анализ поведения**. В этом подразделе вы можете настраивать параметры анализа поведения приложений.
Detection and Response	**Managed Detection and Response**. В этом подразделе вы можете включать и выключать интеграцию с Kaspersky Managed Detection and Response и загружать файл MDR BLOB, необходимый для интеграции. **EDR Expert (on-premise)**. В этом подразделе вы можете включать и выключать интеграцию с Kaspersky Endpoint Detection and Response (KATA) и настраивать параметры интеграции. **Network Detection and Response (KATA)**. В этом подразделе вы можете включать и выключать интеграцию с Kaspersky Network Detection and Response (KATA).
Контроль безопасности	**Контроль приложений**. В этом подразделе вы можете настраивать параметры контроля приложений. **Контроль целостности системы**. В этом подразделе вы можете настраивать параметры контроля целостности системы. **Контроль устройств**. В этом подразделе вы можете настраивать параметры контроля устройств. **Веб-Контроль**. В этом подразделе вы можете настраивать параметры Веб-Контроля.
Локальные задачи	**Управление задачами**. В этом подразделе вы можете настраивать разрешения для пользователей на управление задачами. **Проверка съемных дисков**. В этом подразделе вы можете настраивать параметры проверки съемных дисков при подключении их к защищаемому устройству.

Раздел	Подразделы
Общие параметры	**Параметры прокси-сервера**. В этом подразделе вы можете настраивать параметры прокси-сервера, если доступ пользователей с клиентских устройств в интернет осуществляется через прокси-сервер. **Параметры приложения**. В этом подразделе вы можете настраивать следующие параметры: • Обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным. • Параметры уведомлений о событиях. • Ограничение на использование памяти и ресурсов процессора для задач проверки. • Ограничение на количество задач выборочной проверки, которые может одновременно запустить на устройстве непривилегированный пользователь. • Параметры запуска приложения. • Параметры трассировки и записи дампов. • Отслеживание стабильности работы приложения. • Ограничение на использование резидентной памяти приложением. • Режим перехвата файловых операций. **Параметры проверки контейнеров**. В этом подразделе вы можете управлять работой компонента Мониторинг контейнеров. **Параметры сети**. В этом подразделе вы можете настраивать параметры проверки сетевого трафика. **Глобальные исключения**. В этом подразделе вы можете настраивать: • Исключение точек монтирования из перехвата файловых операций. • Исключения для промышленного ПО – исключение процессов, файлов и директорий, связанных с ПО определенного типа. **Исключение памяти процессов**. В этом подразделе вы можете настраивать исключение памяти процессов из проверки. **Параметры хранилищ**. В этом подразделе вы можете настраивать: • Параметры резервного хранилища и карантина. • Параметры отправки информации в хранилище Kaspersky Security Center. **Параметры взаимодействия с ОС**. В этом подразделе вы можете: • Выбирать механизм, который приложение должно использовать для перехвата системных событий. • Настраивать дополнительные параметры сбора телеметрии.
Интеграция с KUMA	**Интеграция с KUMA**. В этом подразделе вы можете включать и выключать интеграцию Kaspersky Unified Monitoring and Analysis Platform и настраивать параметры интеграции.
Режим Легкого агента Параметры в этом разделе применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.	**Подключение к Серверу интеграции**. В этом подразделе вы можете настроить подключение Легких агентов к Серверу интеграции, компоненту Kaspersky Security для виртуальных сред Легкий агент. **Параметры обнаружения SVM**. В этом подразделе вы можете выбрать способ, который используют Легкие агенты для обнаружения доступных для подключения SVM. **Тег для подключения к SVM**. В этом подразделе вы можете включить использование тегов Легким агентом и назначить тег, который Легкий агент будет использовать для подключения. **Алгоритм выбора SVM**. В этом подразделе вы можете указать, какой алгоритм выбора SVM должны использовать Легкие агенты. **Защита соединения**. В этом подразделе вы можете включить шифрование канала передачи данных между Легким агентом и Сервером защиты.

Управление задачами в Web Console

Вы можете выполнять следующие действия над задачами для Kaspersky Endpoint Security в Web Console:

- Создавать новые задачи.
- Изменять параметры задач.

  Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Запускать, останавливать, приостанавливать и возобновлять выполнение задач.

  Задачу *Обновление* невозможно приостановить и возобновить, ее можно только запустить или остановить.

- Экспортировать и импортировать задачи.
- Удалять задачи.

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 (**Мониторинг и отчеты** → **Выборки событий**). Дополнительная информация о выборке событий приведена в документации Kaspersky Security Center.

Результаты выполнения задач также сохраняются локально на устройстве и в отчетах Kaspersky Security Center.

Общую информацию о работе с задачами см. в справке Kaspersky Security Center.

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.

Создание задач в Web Console

Чтобы создать задачу для группы или набора 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.

Чтобы 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 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 устройство, для которого вы хотите создать задачу, и нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на закладку **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.

Изменение параметров задач в Web Console

Чтобы изменить параметры задачи в Web Console:

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

   Откроется список задач.

2. Выполните одно из следующих действий:

   - Если вы хотите изменить параметры задачи, которая выполняется на всех устройствах, входящих в определенную группу администрирования, нажмите на ссылку в поле **Текущий путь** в верхней части окна и в открывшемся окне выберите группу администрирования.

     В списке отобразятся только задачи, настроенные для выбранной группы администрирования.

   - Если вы хотите изменить параметры задачи, которая выполняется на одном или нескольких устройствах (задачи для набора устройств), нажмите на ссылку в поле **Текущий путь** 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 выберите нужную задачу и откройте окно свойств задачи по ссылке в названии задачи.

4. Настройте параметры задачи:

   - На закладке **Общие** вы можете изменить название задачи.
   - На закладке **Параметры приложения** вы можете настроить специфические параметры задачи. Наличие настраиваемых параметров зависит от типа задачи.
   - На закладке **Расписание** вы можете настроить расписание запуска задачи и дополнительные параметры запуска и остановки задачи.

   Закладки **Общие**, **Результаты**, **Параметры**, **Расписание** и **История ревизий** окна свойств задачи стандартны для Kaspersky Security Center, см. подробнее в справке Kaspersky Security Center.

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

Запуск, остановка, приостановка и возобновление задач в Web Console

Чтобы 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 ссылку в поле **Текущий путь** 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 ссылку в поле **Текущий путь** 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.

Управление задачами в Консоли администрирования

Вы можете выполнять следующие действия над задачами для Kaspersky Endpoint Security в Консоли администрирования:

- Создавать новые задачи.
- Изменять параметры задач.

> Если учетная запись пользователя, под которой осуществляется доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Запускать, останавливать, приостанавливать и возобновлять выполнение задач.

  Задачу *Обновление* невозможно приостановить и возобновить, ее можно только запустить или остановить.

- Экспортировать и импортировать задачи.
- Удалять задачи.

В списке задач вы можете следить за выполнением задачи: просматривать статус задачи и статистику выполнения задачи на устройствах.

Информацию о ходе и результатах выполнения задач вы можете посмотреть в списке событий, которые приложение Kaspersky Endpoint Security отправляет на Сервер администрирования Kaspersky Security Center (на закладке **События** в рабочей области узла **Сервер администрирования <имя сервера>**). Также вы можете создать выборку событий для контроля за выполнением задач. Дополнительная информация о выборке событий приведена в документации Kaspersky Security Center.

Результаты выполнения задач также сохраняются локально на устройстве и в отчетах Kaspersky Security Center.

Общую информацию о работе с задачами см. в справке Kaspersky Security Center.

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.

Создание задач в Консоли администрирования

Чтобы создать задачу для группы или набора 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 закладку **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 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.

Чтобы 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 закладку **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.

Изменение параметров задач в Консоли администрирования

Чтобы изменить параметры задачи 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 закладку **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 и откройте окно **Свойства: <Название задачи>** двойным щелчком мыши.

   Вы также можете открыть окно свойств задачи с помощью пункта **Свойства** контекстного меню задачи.

3. Измените параметры задачи. Наличие настраиваемых параметров зависит от типа задачи.

   Закладки **Общие**, **Уведомление**, **Расписание** и **История ревизий** окна свойств задачи стандартны для Kaspersky Security Center, см. подробнее в справке Kaspersky Security Center.

4. Нажмите на кнопку **Применить** или на кнопку **ОК** в окне **Свойства: <Название задачи>**, чтобы сохранить внесенные изменения.

Запуск, остановка, приостановка и возобновление задач в Консоли администрирования

Чтобы 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 закладку **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 задачи, созданных на Сервере администрирования.

2. В списке задач выберите нужную задачу, откройте контекстное меню задачи и выберите действие, которое вы хотите выполнить.

Управление приложением 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.

Работу функциональных компонентов приложения обеспечивают *локальные задачи Kaspersky Endpoint Security*, которые выполняются в операционной системе. Вы можете включать и выключать функциональные компоненты приложения на устройстве путем запуска и остановки задач Kaspersky Endpoint Security в командной строке. Однократные проверки устройства также выполняются путем запуска задач Kaspersky Endpoint Security. Вы можете задавать параметры работы функциональных компонентов на устройстве и параметры проверки устройства, настраивая *параметры задач* Kaspersky Endpoint Security.

Помимо параметров задач для настройки работы приложения предусмотрены следующие параметры:

- Общие параметры проверки контейнеров.
- Параметры проверки сетевого трафика.
- Общие параметры приложения, которые определяют работу приложения в целом и работу отдельных функций.

Управление приложением Kaspersky Endpoint Security в командной строке выполняется с помощью *команд управления Kaspersky Endpoint Security*.

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.

Включение автоматического дополнения команды kesl-control (bash completion)

Для оболочки bash есть возможность включить автоматическое дополнение команды kesl-control.

Чтобы включить автоматическое дополнение команды kesl-control в текущей сессии оболочки bash, выполните следующую команду:

```
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

Чтобы включить автоматическое дополнение для всех новых сессий оболочки bash, выполните следующую команду:

```
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~/.bashrc
```

Управление задачами в командной строке

Для управления приложением Kaspersky Endpoint Security с помощью командной строки предусмотрены следующие задачи приложения:

- *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. Задача запускается автоматически при запуске приложения.

- *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.

- *Проверка важных областей*. Эта задача позволяет выполнять проверку важных областей операционной системы по требованию и определяет параметры проверки.

- *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.

- *Проверка контейнеров*. Эта задача позволяет выполнять проверку контейнеров и образов по требованию и определяет параметры проверки.

- *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.

- *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.

- *Защита от веб-угроз*. Эта задача позволяет включать и выключать защиту от веб-угроз и определяет параметры работы компонента Защита от веб-угроз.

- *Защита от сетевых угроз*. Эта задача позволяет включать и выключать защиту от сетевых угроз и определяет параметры работы компонента Защита от сетевых угроз.

- *Защита от шифрования*. Эта задача позволяет включать и выключать защиту файлов от удаленного вредоносного шифрования и определяет параметры компонента Защита от шифрования.

- *Управление сетевым экраном*. Эта задача позволяет включать и выключать управление сетевым экраном и определяет параметры контроля сетевых соединений на устройстве.

- *Контроль приложений*. Эта задача позволяет включать и выключать Контроль приложений и определяет параметры компонента Контроль приложений.

- *Инвентаризация*. Эта задача позволяет получать информацию обо всех исполняемых файлах приложений, хранящихся на устройстве.

- *Контроль устройств*. Эта задача позволяет включать и выключать Контроль устройств и определяет параметры компонента Контроль устройств. Задача запускается автоматически при запуске приложения Kaspersky Endpoint Security.

- *Веб-Контроль*. Эта задача позволяет включать и выключать Веб-Контроль и определяет параметры компонента Веб-Контроль.

- *Анализ поведения*. Эта задача позволяет контролировать вредоносную активность приложений в операционной системе. Задача запускается автоматически при запуске приложения Kaspersky Endpoint Security.

- *Контроль целостности системы*. Эта задача позволяет в реальном времени отслеживать действия, выполняемые с объектами из области мониторинга, указанной в параметрах компонента Контроль целостности системы.

- *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.

- *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.

- *Обновление*. С помощью этой задачи вы можете выполнять обновление баз и модулей приложения по расписанию и по требованию и настраивать параметры обновления.

- *Откат обновления баз*. С помощью этой задачи вы можете выполнять откат последнего обновления баз и модулей приложения.

- *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise)*. Эта задача позволяет включать и выключать интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise) или с Kaspersky Endpoint Detection and Response (KATA) и определяет параметры интеграции.

- *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.

- *Интеграция с Sandbox*. Эта задача позволяет включать и выключать интеграцию с Sandbox и определяет параметры интеграции.

- *Интеграция с KUMA*. Эта задача позволяет включать и выключать интеграцию с Kaspersky Unified Monitoring and Analysis Platform и определяет параметры интеграции.

- *Запрет запуска объектов (EDR Expert (on-premise))*. Эта задача позволяет включать и выключать использование правил запрета запуска объектов компонента Endpoint Detection and Response Expert (on-premise) и просматривать список этих правил.

- *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.

Каждая задача приложения имеет имя, используемое в командной строке, идентификатор и тип (см. таблицу ниже).

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	Имя задачи в командной строке	ID задачи	Тип задачи
Защита от файловых угроз	File_Threat_Protection	1	OAS
Поиск вредоносного ПО	Scan_My_Computer	2	ODS
Поиск вредоносного ПО (пользовательская)	задается пользователем	от 100	ODS
Выборочная проверка файлов	Scan_File	3	ODS
Проверка важных областей	Critical_Areas_Scan	4	ODS
Обновление	Update	6	Update
Обновление (пользовательская)	задается пользователем	от 100	Update
Откат обновления баз	Rollback	7	Rollback
Откат обновления баз (пользовательская)	задается пользователем	от 100	Rollback
Лицензирование	License	9	License
Контроль целостности системы	System_Integrity_Monitoring	11	OAFIM
Контроль целостности системы (пользовательская)	задается пользователем	от 100	ODFIM
Управление сетевым экраном	Firewall_Management	12	Firewall
Защита от шифрования	Anti_Cryptor	13	AntiCryptor
Защита от веб-угроз	Web_Threat_Protection	14	WTP
Контроль устройств	Device_Control	15	DeviceControl
Проверка съемных дисков	Removable_Drives_Scan	16	RDS
Защита от сетевых угроз	Network_Threat_Protection	17	NTP
Проверка контейнеров	Container_Scan	18	ContainerScan
Проверка контейнеров (пользовательская)	задается пользователем	от 100	ContainerScan
Выборочная проверка контейнеров	Custom_Container_Scan	19	ContainerScan
Анализ поведения	Behavior_Detection	20	BehaviorDetection
Контроль приложений	Application_Control	21	AppControl
Инвентаризация	Inventory_Scan	22	InventoryScan
Инвентаризация (пользовательская)	задается пользователем	от 100	InventoryScan
Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise)	KATAEDR	24	KATAEDR
Веб-Контроль	Web_Control	26	WebControl

Задача	Имя задачи в командной строке	ID задачи	Тип задачи
Интеграция с Sandbox	Standalone_Sandbox	29	StandaloneSandbox
Запрет запуска объектов (EDR Expert (on-premise))	KATAEDR_Prevention	30	KATAEDRPrevention
Интеграция с Kaspersky Network Detection and Response (KATA)	KATANDR	31	KATANDR
Запрет запуска объектов (EDR Optimum)	EDRO_Prevention	32	Prevention
Интеграция с KUMA	KUMA	33	KUMA
Защита от почтовых угроз	Mail_Monitoring	35	MailMonitoring
Защита от атак BadUSB	Bad_USB	37	BadUSB

Вы можете выполнять следующие действия над задачами:

- Запускать и останавливать все предустановленные и пользовательские задачи, кроме задачи *License*.
- Приостанавливать и возобновлять задачи типов *ODS*, *ODFIM* и *InventoryScan*.
- Создавать и удалять пользовательские задачи. В зависимости от режима использования приложения вы можете создавать задачи следующих типов:
  - стандартный режим: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* и *InventoryScan*;
  - режим Легкого агента для защиты виртуальных сред: *ODS*, *ODFIM*, *ContainerScan* и *InventoryScan*.
- Изменять параметры всех пользовательских задач и всех предустановленных задач, кроме задач типов *Rollback* и *License*.

  Если приложение используется в режиме Легкого агента для защиты виртуальных сред, параметры предустановленной задачи *Update* также недоступны для изменения.

- Настраивать расписание запуска задач.

Просмотр списка задач в командной строке

Чтобы просмотреть список задач приложения, выполните следующую команду:

```
kesl-control --get-task-list [--json]
```

где:

`--json` – формат вывода списка задач приложения. Если вы не укажете формат, вывод будет выполнен в формате INI.

Отобразится список задач приложения Kaspersky Endpoint Security.

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 (в стандартном режиме) и Rollback (в стандартном режиме) недоступна.

Просмотр состояния задачи в командной строке

Чтобы посмотреть состояние задачи, выполните следующую команду:

```
kesl-control --get-task-state <идентификатор/имя задачи> [--json]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--json` – выводить параметры в формате JSON.

Для задач приложения предусмотрены следующие основные 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.

Создание задачи в командной строке

Если приложение используется в стандартном режиме, вы можете создавать задачи следующих типов: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* и *InventoryScan*.

Если приложение используется в режиме Легкого агента для защиты виртуальных сред, вы можете создавать задачи следующих типов: *ODS*, *ODFIM*, *ContainerScan* и *InventoryScan*.

Вы можете создавать задачи с параметрами по умолчанию или с параметрами, указанными в конфигурационном файле.

Чтобы создать задачу с параметрами по умолчанию, выполните следующую команду:

```
kesl-control --create-task <имя задачи> --type <тип задачи>
```

где:

- `<имя задачи>` – имя, которое вы задаете для новой задачи;
- `<тип задачи>` – обозначение типа создаваемой задачи.

Чтобы создать задачу с параметрами, указанными в конфигурационном файле, выполните следующую команду:

```
kesl-control --create-task <имя задачи> --type <тип задачи> --file <путь к конфигурационному файлу> [--json]
```

где:

- `<имя задачи>` – имя, которое вы задаете для новой задачи;
- `<тип задачи>` – обозначение типа создаваемой задачи;
- `<путь к файлу>` – 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.

Запуск, остановка, приостановка и возобновление задачи в командной строке

Вы можете запускать и останавливать предустановленные и пользовательские задачи, кроме задачи License.

Вы можете приостанавливать и возобновлять задачи типов ODS, ODFIM и InventoryScan.

Запустить задачу

```
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.

Пример запуска задачи с идентификатором 1 с включенным выводом 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.

Остановить задачу

```
kesl-control --stop-task <task ID|name> [-W]
```

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.

Приостановить задачу

```
kesl-control --suspend-task <task ID|name>
```

Возобновить задачу

```
kesl-control --resume-task <task ID|name>
```

Удаление задачи в командной строке

Вы можете удалять только пользовательские задачи. Предустановленные задачи недоступны для удаления.

Чтобы удалить задачу, выполните следующую команду:

```
kesl-control --delete-task <идентификатор/имя задачи>
```

где `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Вывод параметров задачи в командной строке

Вы можете выводить текущие значения параметров всех пользовательских задач и всех предустановленных задач, кроме задач *Rollback* и *License* (эти задачи не имеют параметров).

Вы можете выводить текущие значения параметров задачи в консоль или в конфигурационный файл, который вы можете использовать для изменения параметров задачи.

Чтобы вывести в консоль текущие значения параметров задачи, выполните следующую команду:

```
kesl-control --get-settings <идентификатор/имя задачи> [--json]
```

где:

- `<идентификатор/имя задачи>` – 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.

Чтобы вывести в конфигурационный файл текущие значения параметров задачи, выполните следующую команду:

```
kesl-control --get-settings <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--file <путь к конфигурационному файлу>` – 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 формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Изменение параметров задачи в командной строке

Вы можете изменять параметры всех пользовательских задач и всех предустановленных задач, кроме задач *Rollback* и *License*.

Если приложение используется в режиме Легкого агента для защиты виртуальных сред, параметры предустановленной задачи *Update* также недоступны для изменения.

В командной строке вы можете изменять параметры задач с помощью команды `kesl-control --set-settings`:

- Вы можете изменять все параметры задачи, используя конфигурационный файл, который содержит параметры задачи. Конфигурационный файл вы можете получить с помощью команды вывода параметров задачи.
- Вы можете изменять отдельные параметры задачи, используя ключи командной строки в формате `< имя параметра >=< значение параметра >`. Текущие значения параметров задачи вы можете получить с помощью команды вывода параметров задачи.
- Вы можете восстанавливать заданные по умолчанию параметры задачи.

Вы можете добавлять и удалять области проверки и области исключения используя конфигурационный файл, который содержит параметры задачи, или ключи командной строки. Настройка областей проверки и областей исключения доступна для задач с типами *OAS*, *ODS*, *OAFIM*, *ODFIM* и *AntiCryptor*.

> 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/`.

Для некоторых задач также предусмотрены отдельные команды управления, которые позволяют изменять параметры задач.

Изменение параметров задачи с помощью конфигурационного файла

Чтобы изменить значения параметров задачи с помощью конфигурационного файла:

1. Выведите параметры задачи в конфигурационный файл с помощью команды `kesl-control --get-settings`.
2. Откройте конфигурационный файл и измените значения нужных параметров.

   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. Сохраните конфигурационный файл.
4. Выполните команду:

   `kesl-control --set-settings <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]`

   где:

   - `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
   - `--file <путь к конфигурационному файлу>` – 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`.

Изменение параметров задачи с помощью ключей командной строки

С помощью ключей команды `kesl-control --set-settings` вы можете изменять отдельные значения параметров задачи, а также добавлять или удалять области проверки и области исключения для задач типа *OAS*, *ODS*, *OAFIM*, *ODFIM* и *AntiCryptor*.

Настройка отдельных параметров задач

Чтобы изменить отдельные значения параметров задачи с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-settings <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `<имя параметра>=<значение параметра>` – 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`.

Добавление и удаление области проверки

Чтобы добавить область проверки с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-settings <идентификатор/имя задачи> --add-path <путь>
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--add-path <путь>` – добавить путь к директории с проверяемыми объектами.

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:
Добавление области проверки для задачи с ID=100:

```
kesl-control --set-settings 100 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

В задачу будут добавлены следующие параметры области проверки:

```
[ScanScope.item_0001]

AreaDesc=

UseScanArea=Yes

Path=/home

AreaMask.item_0000=*
```

Чтобы удалить область проверки с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-settings <идентификатор/имя задачи> --del-path <путь>
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--del-path <путь>` – удалить путь к директории с проверяемыми объектами.

  Секция `[ScanScope.item_#]`, содержащая указанный путь, будет удалена из параметров задачи. Приложение не будет проверять объекты в указанной директории.

Добавление и удаление области исключения

Чтобы добавить область исключения с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-settings <идентификатор/имя задачи> --add-exclusion <путь>
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--add-exclusion <путь>` – 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.

Чтобы удалить область исключения с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-settings <идентификатор/имя задачи> --del-exclusion <путь>
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--del-exclusion <путь>` – 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.

Восстановление параметров задачи по умолчанию в командной строке

Вы можете восстанавливать заданные по умолчанию параметры для всех пользовательских задач и всех предустановленных задач, кроме задач типов *Rollback* и *License* (эти задачи не имеют параметров).

Чтобы восстановить заданные по умолчанию параметры задачи, выполните следующую команду:

```
kesl-control --set-settings <идентификатор/имя задачи> --set-to-default
```

где `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Приложение изменит значения параметров на заданные по умолчанию.

Настройка расписания задачи в командной строке

Если приложение используется в стандартном режиме, вы можете настраивать расписание запуска для задач следующих типов: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* и *InventoryScan*.

Если приложение используется в режиме Легкого агента для защиты виртуальных сред, вы можете настраивать расписание запуска для задач следующих типов: *ODS*, *ODFIM*, *ContainerScan* и *InventoryScan*.

Вы можете выводить текущие значения параметров расписания запуска задачи в консоль или в конфигурационный файл.

Чтобы вывести в консоль текущие параметры расписания запуска задачи, выполните следующую команду:

```
kesl-control --get-schedule <идентификатор/имя задачи> [--json]
```

где:

- `< идентификатор/имя задачи >` – 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.

Чтобы вывести в конфигурационный файл текущие параметры расписания запуска задачи, выполните следующую команду:

```
kesl-control --get-schedule < идентификатор/имя задачи > --file < путь к конфигурационному файлу > [--json]
```

где:

- `< идентификатор/имя задачи >` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--file < путь к конфигурационному файлу >` – 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.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

  Примеры:

  Сохранить параметры задачи обновления в файле с именем update_schedule.ini и сохранить созданный файл в текущей директории:

  ```
  kesl-control --get-schedule 6 --file update_schedule.ini
  ```

  Вывести в консоль расписание задачи обновления:

  ```
  kesl-control --get-schedule 6
  ```

Вы можете изменять параметры расписания запуска задачи следующими способами:

- Импортировать параметры из конфигурационного файла, который содержит все параметры расписания.
- Задавать с помощью командной строки отдельные параметры расписания запуска задачи в формате `< имя параметра >=< значение параметра >`.

Чтобы изменить значения параметров расписания запуска задачи с помощью конфигурационного файла, выполните следующие действия:

1. Выведите параметры задачи в конфигурационный файл с помощью команды `kesl-control --get-schedule`.
2. Измените в файле значения нужных параметров и сохраните изменения.
3. Выполните команду:

   ```
   kesl-control --set-schedule < идентификатор/имя задачи > --file < путь к конфигурационному файлу > [--json]
   ```

где:

- `< идентификатор/имя задачи >` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `--file < путь к конфигурационному файлу >` – 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.

Все значения параметров расписания запуска задачи, заданные в файле, будут импортированы в приложение.

Пример:
Импортировать в задачу с ID=2 параметры расписания из конфигурационного файла с именем /home/test/on_demand_schedule.ini:

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

Чтобы изменить отдельные значения параметров расписания запуска задачи с помощью командной строки, выполните следующую команду:

```
kesl-control --set-schedule < идентификатор/имя задачи > < имя параметра >=< значение параметра > [< имя параметра >=< значение параметра >]
```

где:

- `< идентификатор/имя задачи >` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `< имя параметра >=< значение параметра >` – имя и значение одного из параметров расписания задач.

Значения указанных параметров расписания запуска задачи будут изменены.

Примеры:

Чтобы настроить запуск задачи каждые 10 часов, укажите следующие параметры:

```
RuleType=Hourly

RunMissedStartRules=No

StartTime=2021/May/30 23:05:00;10

RandomInterval=0
```

Чтобы настроить запуск задачи каждые 10 минут, укажите следующие параметры:

```
RuleType=Minutely

RunMissedStartRules=No

StartTime=23:10:00;10

RandomInterval=0
```

Чтобы настроить запуск задачи 15-го числа каждого месяца, укажите следующие параметры:

```
RuleType=Monthly

RunMissedStartRules=No

StartTime=23:25:00;15

RandomInterval=0
```

Чтобы настроить запуск задачи каждый вторник, укажите следующие параметры:

```
RuleType=Weekly

StartTime=18:01:30;Tue

RandomInterval=99

RunMissedStartRules=No
```

Чтобы настроить запуск задачи через каждые 11 дней, укажите следующие параметры:

```
RuleType=Daily

RunMissedStartRules=No

StartTime=23:15:00;11

RandomInterval=0
```

Управление общими параметрами приложения в командной строке

Общие параметры приложения определяют работу приложения в целом и работу отдельных функций.

Вы можете управлять общими параметрами приложения с помощью специальных команд управления:

- Выводить текущие значения общих параметров приложения в консоль или в конфигурационный файл.
- Изменять общие параметры приложения, используя конфигурационный файл, содержащий все общие параметры, или ключи командной строки в формате `< имя параметра >=< значение параметра >`.

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 проверку 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.

Вывод общих параметров приложения

Вы можете выводить текущие значения общих параметров приложения в консоль или в конфигурационный файл, который вы можете использовать для изменения параметров приложения.

Чтобы вывести в консоль текущие значения общих параметров приложения, выполните следующую команду:

```
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.

Чтобы вывести в конфигурационный файл текущие значения общих параметров приложения, выполните следующую команду:

```
kesl-control --get-app-settings --file < путь к конфигурационному файлу > [--json]
```

где:

- `--file <путь к конфигурационному файлу>` – 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.

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

Пример:
Вывести общие параметры приложения в файл с именем kesl_config.ini. Сохранить созданный файл в текущей директории:

```
kesl-control --get-app-settings --file kesl_config.ini
```

Изменение общих параметров приложения

В командной строке вы можете изменять общие параметры приложения с помощью команды `kesl-control --set-app-settings`:

- Вы можете изменять все общие параметры, используя конфигурационный файл, который содержит общие параметры приложения. Конфигурационный файл вы можете получить с помощью команды вывода общих параметров.

- Вы можете изменять отдельные параметры, используя ключи командной строки в формате `<имя параметра>=<значение параметра>`. Текущие значения общих параметров приложения вы можете получить с помощью команды вывода общих параметров.

Чтобы изменить значения общих параметров приложения с помощью конфигурационного файла:

1. Выведите общие параметры приложения в конфигурационный файл.

2. Измените значения нужных параметров в файле и сохраните изменения.

3. Выполните команду:

   `kesl-control --set-app-settings --file <путь к конфигурационному файлу> [--json]`

   где:

   - `--file <путь к конфигурационному файлу>` – 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.

Чтобы изменить значения общих параметров приложения с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-app-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

где < имя параметра >=< значение параметра > – имя и значение одного из общих параметров приложения.

Значения указанных общих параметров будут изменены.

Примеры:

Импортировать в приложение общие параметры из конфигурационного файла /home/test/kesl_config.ini:

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

Установить низкий уровень детализации файла трассировки:

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

Добавить точку монтирования, которую требуется исключить 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:

```
"< поле > < операция сравнения > '< значение >'"
```

```
"< поле > < операция сравнения > '< значение >' and < поле > < операция сравнения >
'< значение >'"
```

где:

- < поле > – название поля базы данных.
- < операция сравнения > – 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.

- < значение > – 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.

Вы можете использовать фильтр в следующих командах управления приложением:

- Вывод информации об определенных текущих событиях приложения (Просмотр событий в командной строке, Просмотр событий в Kaspersky Security Center):

  ```
  kesl-control -W --query "< условия фильтра >"
  ```

- Вывод информации об определенных событиях приложения (Просмотр событий в командной строке, Просмотр событий в Kaspersky Security Center) в журнале событий:

  ```
  kesl-control -E --query "< условия фильтра >"
  ```

- Вывод информации об определенных объектах в резервном хранилище:

  ```
  kesl-control -B --query "< условия фильтра >"
  ```

- Удаление определенных объектов из резервного хранилища:

  ```
  kesl-control -B --mass-remove --query "< условия фильтра >"
  ```

  Примеры:

  Вывести информацию о событиях, которые содержат текст "etc" в поле FileName:

  ```
  kesl-control -E --query "FileName like '%etc%'"
  ```

  Вывести информацию о событиях с типом ThreatDetected (обнаружена угроза):

  ```
  kesl-control -E --query "EventType == 'ThreatDetected'"
  ```

  Вывести информацию о событиях с типом ThreatDetected, сформированных задачами типа ODS:

  ```
  kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
  ```

  Вывести информацию 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'"
  ```

  Вывести информацию 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'"
  ```

  Вывести информацию о файлах в резервном хранилище, имеющих высокий (High) уровень важности:

  ```
  kesl-control -B --query "DangerLevel == 'High'"
  ```

Экспорт и импорт параметров приложения

Если вы управляете приложением Kaspersky Endpoint Security через Kaspersky Security Center, импорт параметров недоступен.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, параметры предустановленной задачи типа *Update* недоступны для экспорта и импорта.

Kaspersky Endpoint Security позволяет импортировать и экспортировать все параметры приложения для диагностики сбоев, проверки параметров или для упрощения настройки приложения на устройствах пользователей. 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 импортировать параметры в приложение.

Во время импорта или экспорта параметров приложение должно быть запущено. После импорта параметров требуется перезапустить приложение.

При импорте или экспорте параметров из более старой версии приложения для новых параметров устанавливаются значения по умолчанию. Импорт параметров в более старую версию приложения недоступен.

Чтобы экспортировать параметры приложения, выполните следующую команду:

```
kesl-control --export-settings --file <путь к конфигурационному файлу> [--json]
```

где:

- `--file <путь к конфигурационному файлу>` – 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.

Чтобы импортировать параметры приложения из файла, выполните следующую команду:

```
kesl-control --import-settings --file <путь к конфигурационному файлу> [--json]
```

где:

- `--file <путь к конфигурационному файлу>` – 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.

При импорте параметров из файла для параметров `UseKSN` и `CloudMode` устанавливается значение `No`, а также выключается интеграция с MDR. Чтобы начать или возобновить использование Kaspersky Security Network, требуется задать для параметра `UseKSN` значение `Basic` или `Extended`. Чтобы включить облачный режим, требуется задать для параметра `CloudMode` значение `Yes`. Облачный режим доступен, если включено использование KSN. Чтобы включить интеграцию с MDR, вам надо сначала включить использование Kaspersky Security Network в расширенном режиме, а потом задать для параметра `UseMDR` значение `Yes`.

После импорта параметров приложения внутренние идентификаторы задач могут измениться. Для управления задачами рекомендуется использовать имена задач.

Невозможно импортировать следующие параметры политики из веб-плагина приложения версий 12.3 в приложение версии 12.4:

- область защиты и область исключений Защиты от файловых угроз, Защиты от шифрования;
- исключение из проверки процессов для Анализ 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).

Управление ролями пользователей с помощью командной строки

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* и *nokesl*. Когда роль в приложении назначается пользователю системы, этот пользователь добавляется в соответствующую группу (см. таблицу *Роли* ниже). При отзыве роли у пользователя пользователь удаляется из соответствующей группы.

Если пользователю системы не назначено ни одной роли в приложении, этот пользователь относится к отдельной группе *пользователи без прав*.

Таким образом, роли соответствуют четырем группам пользователей операционной системы:

- kesladmin соответствует роли Администратор;
- kesluser соответствует роли Пользователь;
- keslaudit соответствует роли Аудитор;
- nokesl назначается пользователю, если не назначена ни одна из ролей. В этом случае пользователь относится к отдельной группе *пользователи без прав*.

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.

Роли 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. Просмотр отчетов для созданных пользователем задач. Просмотр особых событий, общих для всех пользователей приложения.
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.

Просмотр списка пользователей и ролей

Чтобы просмотреть список пользователей и их ролей, выполните следующую команду:

```
kesl-control [-U] --get-user-list
```

Назначение роли пользователю

Чтобы назначить роль определенному пользователю, выполните следующую команду:

```
kesl-control [-U] --grant-role <роль> <пользователь>
```

Пример:
Назначить роль audit пользователю test15:

```
kesl-control --grant-role audit test15
```

Отзыв роли у пользователя

Чтобы отозвать роль у определенного пользователя, выполните следующую команду:

```
kesl-control [-U] --revoke-role <роль> <пользователь>
```

Пример:
Отозвать роль audit у пользователя test15:

```
kesl-control --revoke-role audit test15
```

Запуск и остановка приложения

После установки приложения Kaspersky Endpoint Security на устройство запуск приложения выполняется автоматически. Далее по умолчанию приложение запускается автоматически при запуске операционной системы (на уровнях выполнения по умолчанию, принятых для каждой операционной системы).

По умолчанию при запуске приложения Kaspersky Endpoint Security автоматически запускаются следующие функциональные компоненты приложения:

- 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, все выполняющиеся на устройстве задачи будут прерваны. Прерванные пользовательские задачи после повторного запуска приложения автоматически не возобновляются.

Запуск и остановка приложения с помощью Web Console

Чтобы запустить или остановить приложение дистанционно:

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 закладку **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**.

Запуск и остановка приложения с помощью Консоли администрирования

Чтобы запустить или остановить приложение на клиентском устройстве:

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

   - Если вы хотите запустить приложение, нажмите на кнопку справа от списка приложений "Лаборатории Касперского" или в контекстном меню приложения выберите пункт **Запустить**.
   - Если вы хотите остановить работу приложения, нажмите на кнопку справа от списка приложений "Лаборатории Касперского" или в контекстном меню приложения выберите пункт **Остановить**.

Запуск и остановка приложения 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.

Запуск, перезапуск и остановка приложения Kaspersky Endpoint Security

Чтобы запустить приложение, выполните следующую команду:

```
systemctl start kesl
```

Чтобы остановить приложение, выполните следующую команду:

```
systemctl stop kesl
```

Чтобы перезапустить приложение, выполните следующую команду:

```
systemctl restart kesl
```

Мониторинг статуса приложения 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.

Чтобы вывести статус приложения, выполните следующую команду:

```
systemctl status kesl
```

Просмотр состояния защиты устройства и информации о работе приложения

Вы можете просматривать информацию о состоянии защиты устройства и о статусе работы приложения Kaspersky Endpoint Security и его компонентов на устройстве.

Вы можете получать информацию о состоянии защиты устройства следующими способами:

- В Web Console или в Консоли администрирования с помощью статусов клиентских устройств (*OK*, *Критический*, *Предупреждение*). Устройство, на котором установлен Агент администрирования Kaspersky Security Center, является клиентским устройством для Kaspersky Security Center. Статус клиентского устройства может изменяться на *Критический* или *Предупреждение* по следующим причинам:

  - В соответствии с правилами, определенными в Kaspersky Security Center. Например, статус изменяется, если на устройстве не установлено приложение защиты, давно не выполнялся поиск вирусов, устарели базы приложения, истек срок действия лицензии или приложение работает нестабильно. Подробнее о причинах изменения статусов и настройке условий присвоения статусов см. в справке Kaspersky Security Center.

  - Kaspersky Security Center получает статус устройства от управляемого приложения, то есть от Kaspersky Endpoint Security.

    > Получение статуса устройства от управляемого приложения должно быть включено в Kaspersky Security Center в списках условий назначения статусов *Критический* и *Предупреждение*. Условия назначения статусов устройства настраиваются в окне свойств группы администрирования.

  Подробнее о статусах клиентского устройства см. в справке Kaspersky Security Center.

- В Web Console или в Консоли администрирования с помощью статусов функциональных компонентов приложения Kaspersky Endpoint Security на устройстве. В свойствах приложения Kaspersky Endpoint Security, установленного на устройстве, отображается список функциональных компонентов приложения. Для каждого компонента отображается его статус.

- В командной строке с помощью следующих команд управления приложением:

  - команды `kesl-control --app-info`, которая выводит информацию о работе приложения и состоянии функциональных компонентов и задач приложения;

  - команды `kesl-control --supported-tech-info`, которая выводит список функций приложения, информацию об их статусах (используется или не используется) и технологиях Linux, с помощью которых реализованы эти функции приложения;

  - команды `kesl-control --get-statistic`, которая выводит статистику о работе приложения и список точек монтирования;

  - команды `kesl-control --export-metrics`, которая выводит метрики о состоянии операционной системы.

Просмотр состояния защиты устройства в Web Console

Чтобы просмотреть состояние защиты устройства 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 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 устройство, информацию о котором вы хотите просмотреть, и нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства на закладке **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.
- **Обнаружено вирусов** – 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.

Просмотр состояния защиты устройства в Консоли администрирования

Чтобы просмотреть 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 закладку **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.

Просмотр информации о работе приложения в Web Console

Чтобы просмотреть в Web Console информацию о работе приложения:

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 выберите в открывшемся окне группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. В списке найдите устройство, информацию о котором вы хотите просмотреть, и нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.

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

   Откроется окно свойств приложения.

В окне отображается следующая информация о приложении Kaspersky Endpoint Security:

- На закладке **Общие** в разделе **Информация** содержится общая информация об установленном приложении:
  - **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 защиты от файловых угроз на устройстве, например: *Выполняется* или *Приостановлена*.
  - 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.
- На закладке **Общие** в разделе **Лицензии** приведена информация о лицензионных ключах, добавленных в приложение, и связанных с этими ключами лицензиях.
- На закладке **Общие** в разделе **Компоненты** содержится список функциональных компонентов приложения. Для каждого компонента отображается его статус (например, *Остановлен, Приостановлен, Не установлен*) и версия.

  В строке **Режим Легкого агента для защиты виртуальных сред** вы можете посмотреть информацию о режиме использования приложения:
  - статус *выполняется* означает, что приложение используется в режиме Легкого агента;
  - статус *не установлено* означает, что приложение используется в стандартном режиме.
- На закладке **События** отображается список событий приложения на устройстве.

- На закладке **Настройка событий** отображаются типы событий, которые приложение сохраняет в хранилище событий, и время их хранения.
- На закладке **Параметры приложения** вы можете выполнить следующие действия:
  - в разделе **Detection and Response** вы можете управлять сетевой изоляцией устройства;
  - в разделе **Контроль приложений** вы можете экспортировать настроенные параметры компонента и категории приложений в файл, и импортировать их из файла;
  - в разделе **Статистика** вы можете просмотреть статистику работы приложения, а также список точек монтирования.

Просмотр информации о работе приложения в Консоли администрирования

Чтобы просмотреть в Консоли администрирования Kaspersky Security Center информацию о работе приложения:

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 закладку **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.

В окне отображается следующая информация о Kaspersky Endpoint Security:

- В разделе **Общие** содержится общая информация об установленном приложении:
  - **Номер версии** – номер версии приложения.
  - **Установлено** – дата и время установки приложения на устройстве.
  - **Текущее состояние** – состояние защиты от файловых угроз на устройстве, 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.

- В разделе **Контроль приложений** вы можете экспортировать настроенные параметры компонента и категории приложений в файл, и импортировать их из файла.
- В разделе **Статистика** отображается статистика работы приложения, а также информация о точках монтирования.
- В разделе **Компоненты** содержится список стандартных компонентов приложения. Для каждого компонента отображается его статус (например, *Остановлен, Приостановлен, Не установлен*) и версия.

  В строке **Режим Легкого агента для защиты виртуальных сред** вы можете посмотреть информацию о режиме использования приложения:

  - статус *выполняется* означает, что приложение используется в режиме Легкого агента;
  - статус *не установлено* означает, что приложение используется в стандартном режиме.
- В разделе **Лицензионные ключи** приведена информация об активном и резервном лицензионных ключах.
- В разделе **Настройка событий** отображаются типы событий, которые приложение сохраняет в хранилище событий, и время их хранения.
- В разделе **Дополнительно** содержится информация о плагине управления приложением.

Просмотр информации о работе приложения в командной строке

Чтобы посмотреть информацию о приложении, выполните команду:

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

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

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 об основной 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 дополнительной функциональности приложения. Поля отображаются, если на защищенное устройство добавлены ключи для дополнительной функциональности:
  - **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-premise)**. Информация о лицензии, по которой активирован компонент Endpoint Detection and Response Expert (on-premise), или статус лицензионного ключа EDR Expert (on-premise).
  - **Дата окончания срока действия лицензии EDR Expert (on-premise)**. 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 для защиты виртуальных сред**. Информация о том, что приложение используется в режиме Легкого агента для защиты виртуальных сред. 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 Агента Endpoint Detection and Response. 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: `Включена`, `Выключена`.
- **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 (Проверка контейнеров, Мониторинг контейнеров).
- **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-premise)**. Статус интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) или с Kaspersky Endpoint Detection and Response (KATA).
- **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 сбое в работе приложения и создании файла дампа. Это поле отображается, если при предыдущем запуске приложения произошел сбой.

Просмотр статистики работы приложения

Для улучшения производительности вы можете добавить в исключения из проверки файлы, которые наиболее часто проверяет компонент Защита от файловых угроз, и пути к процессам, которые наиболее часто проверяет компонент Анализ поведения, а также обнаруженные на устройстве точки монтирования.

> На устройствах с операционными системами, поддерживающими технологию fanotify, наиболее эффективным способом улучшить производительность является добавление точек монтирования в исключения.

Вы можете просматривать статистику о наиболее часто проверяемых файлах и запускаемых процессах, а также список обнаруженных точек монтирования следующими способами:

- в Web Console;
- в Консоли администрирования;
- в командной строке.

Параметры подсчета и вывода статистики приложением вы можете настроить в конфигурационном файле kesl.ini в секции `[ScannerImpactStats]`.

Просмотр статистики работы приложения в Web Console

Чтобы просмотреть в Web Console статистику о работе приложения:

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 выберите в открывшемся окне группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. В списке найдите устройство, информацию о котором вы хотите просмотреть, и нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.

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

6. В открывшемся окне свойств приложения на закладке **Параметры приложения** выберите раздел **Статистика** → **Статистика проверки**.

   Откроется окно **Статистика проверки**.

   В окне **Статистика проверки** отображается следующая статистика 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 в верхней части каждого блока, вы можете экспортировать статистику, отображающуюся в этом блоке, в файл, имеющий текстовый формат.

Просмотр статистики работы приложения в Консоли администрирования

Чтобы просмотреть в Консоли администрирования статистику о работе приложения:

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 закладку **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 **Приложения**.

   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**.

   Справа в окне отображается следующая статистика 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, отображающуюся в этом блоке, в файл, имеющий текстовый формат.

Просмотр списка точек монтирования в Web Console

Чтобы просмотреть в Web Console список точек монтирования:

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 выберите в открывшемся окне группу администрирования.

   В списке отобразятся только управляемые устройства выбранной группы администрирования.

3. В списке найдите устройство, информацию о котором вы хотите просмотреть, и нажмите на имя устройства.

4. В открывшемся окне свойств управляемого устройства перейдите на закладку **Приложения**.

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

6. В открывшемся окне свойств приложения на закладке **Параметры приложения** выберите раздел **Статистика** → **Точки монтирования**.

   Откроется окно **Точки монтирования**.

   В окне **Точки монтирования** отображается таблица, содержащая следующие столбцы:

   - **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, имеющий текстовый формат. Файл содержит список путей к точкам монтирования, а также метки `[Пространство имен]` и `[Исключена]`.

Просмотр списка точек монтирования в Консоли администрирования

Чтобы просмотреть в Консоли администрирования список точек монтирования:

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 закладку **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 **Приложения**.

   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 → Точки монтирования**.

   Справа в окне отображается таблица **Список точек монтирования**, содержащая следующие столбцы:

   - **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, имеющий текстовый формат. Файл содержит список путей к точкам монтирования, а также метки `[Пространство имен]` и `[Исключена]`.

Просмотр статистики работы приложения и списка точек монтирования в командной строке

Чтобы просмотреть статистику о работе приложения и список точек монтирования, выполните следующую команду:

```
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 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.

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.

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.

Чтобы настроить сбор метрик о ресурсах операционной системы, используемых приложением, выполните следующую команду:

```
kesl-control [-J] --export-metrics [--period <интервал времени между выводами в секундах>|--interactive]
```

где:

- `--period` – периодический вывод результатов в командную строку;
- `--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 Sensor	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.
lfs_system_memory_usage_bytes метка type=virtual Sensor	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 Sensor	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 Sensor	Количество памяти из файла 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_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.

Внутреннее название метрики, метка и тип метрики	Описание и рекомендуемое пороговое значение
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 Sensor	Количество сетевых соединений, в данный момент ожидающих подключения к удаленному серверу.
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 Sensor	Текущее количество входящих перехваченных сетевых соединений в данный момент.
lfs_tproxy_connection_count метка direction=outbound Sensor	Текущее количество исходящих перехваченных сетевых соединений в данный момент.
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.

Внутреннее название метрики, метка и тип метрики	Описание и рекомендуемое пороговое значение
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.
lfs_tproxy_socket_count Sensor	Текущее количество сокетов (слушающие сокеты и сокеты соединений). Перехваченное соединение имеет 2 сокета соединений.
lfs_trafficScanning_object_hanging_count Sensor	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 Sensor	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 Sensor	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 Sensor	Текущий размер кеша точек монтирования перехватчика fanotify.
lfs_oas_cache_file_count Sensor	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 Sensor	Текущий размер кеша точек монтирования Защиты от файловых угроз.
lfs_processManager_cache_size Sensor	Текущее количество активных процессов в системе, находящихся в кеше.
lfs_processManager_cache_hit_count Counter	Число попаданий в кеш процессов в системе.

Внутреннее название метрики, метка и тип метрики	Описание и рекомендуемое пороговое значение
lfs_processManager_cache_miss_count Counter	Число кеш-промахов процессов в системе.
lfs_blockingProcessInterceptor_cache_size Sensor	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_prevention_cache_file_count Sensor	Текущий размер кеша файлов задачи Запрет запуска объектов, не нуждающихся в проверке.
lfs_prevention_cache_file_hit_count Counter	Число попаданий в кеш файлов задачи Запрет запуска объектов, не нуждающихся в проверке.
lfs_prevention_cache_file_miss_count Counter	Число кеш-промахов файлов задачи Запрет запуска объектов, не нуждающихся в проверке.
lfs_prevention_cache_volume_count Sensor	Текущий размер кеша точек монтирования задачи Запрет запуска объектов.
eka_telemetry_metrics_registry_callbacks_exec_duration_milliseconds Sensor	Период времени, который заняло текущее обновление метрик всеми зарегистрированными в реестре клиентами (в миллисекундах).
eka_telemetry_metrics_registry_registered_callbacks Sensor	Текущее количество вызовов функций обновления метрик, которые выполнили MetricsRegistry для всех зарегистрированных клиентов.
eka_telemetry_metrics_registry_scrape_duration_milliseconds Sensor	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.

Обновление баз и модулей приложения

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) может быть недоступна в приложении на территории США.

Обновление баз и модулей приложения Kaspersky Endpoint Security обеспечивает актуальность защиты устройства. Каждый день в мире появляются новые вирусы, вредоносные программы и другие программы, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах приложения. 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.

В процессе обновления базы и модули приложения загружаются и устанавливаются на вашем устройстве. Вы можете получать обновления баз и модулей приложения с серверов обновлений "Лаборатории Касперского", из хранилища Сервера администрирования, из локальных или сетевых директорий и из других источников обновлений.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, в качестве источника обновлений используется директория на SVM.

В процессе обновления модули приложения и базы 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.

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 параметры прокси-сервера в общих параметрах приложения.

Независимо от источника обновлений загрузка пакета обновлений и установка обновления баз и модулей приложения на устройстве выполняется с помощью задачи *Обновление*. В приложении создается предустановленная задача *Обновление*. С помощью этой задачи вы можете выполнять обновление баз и модулей приложения по расписанию и по требованию и настраивать параметры обновления.

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

Если приложение Kaspersky Endpoint Security используется в стандартном режиме или в режиме Агента Endpoint Detection and Response, в Kaspersky Security Center вы можете использовать групповую задачу *Обновление*, которую мастер первоначальной настройки создает после установки MMC-плагина управления или веб-плагина управления Kaspersky Endpoint Security. Вы также можете создавать пользовательские задачи обновления в командной строке и в Kaspersky Security Center.

Вы можете настраивать следующие параметры обновления баз и модулей приложения:

- Выбирать источник, из которого приложение будет получать обновления, в зависимости от используемой схемы обновления.
- 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.
- Настраивать расписание запуска задачи обновления. По умолчанию приложение обновляет базы с периодичностью один раз в 60 минут.

Также вы можете получать автоматически устанавливаемые обновления приложения (автопатчи). В параметрах задачи обновления вы можете выбирать режим загрузки и установки автопачтей: загружать и устанавливать, только загружать или не загружать.

Об обновлении баз и модулей

В процессе обновления на вашем устройстве загружаются и устанавливаются следующие объекты:

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

  Если обновление баз на устройстве прерывается или завершается с ошибкой, приложение продолжает использовать предыдущую установленную версию баз. Если ранее базы приложения не устанавливались, приложение продолжает работу в режиме "без баз". Обновление баз и модулей приложения остается доступным.

  Если обновление баз завершилось успешно, но сами базы повреждены и работа приложения несколько раз подряд завершается с ошибкой, то базы будут автоматически удалены. Приложение продолжит работу в режиме "без баз", обновление баз и модулей приложения останется доступным.

  Базы актуальны, если они были загружены менее трех дней назад. По умолчанию приложение формирует событие *Базы приложения устарели*, если последние установленные обновления баз были опубликованы на серверах "Лаборатории Касперского" более трех, но менее семи дней назад. Если базы не обновляются в течение семи дней, приложение формирует событие *Базы приложения сильно устарели*.

- Модули приложения. Обновление модулей предназначено для устранения уязвимостей в приложении и улучшения методов защиты устройства. Обновления модулей могут менять поведение компонентов приложения и добавлять новые возможности.

  Обновление модулей приложения может быть установлено вне зависимости от состояния приложения (запущено или остановлено, управляется политикой Kaspersky Security Center) и расписания обновлений. Kaspersky Endpoint Security продолжает защищать ваше устройство во время процедуры обновления модулей приложения. В ходе обновления параметры приложения и журнал событий приложения переносятся в новую версию приложения.

  Если во время переноса параметров по какой-либо причине происходит ошибка, для приложения устанавливаются значения по умолчанию.

  Изменения параметров приложения, сделанные после завершения обновления и до перезапуска приложения, не сохраняются.

Если приложение после обновления работает некорректно, оно автоматически откатывается на предыдущую версию. Рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Об источниках и схемах обновления

Источник обновлений – это ресурс, содержащий обновления баз и модулей приложения Kaspersky Endpoint Security. Источником обновлений могут быть FTP-, HTTP- или HTTPS-серверы (например, серверы обновлений "Лаборатории Касперского") и локальные или сетевые директории, смонтированные пользователем.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, обновление баз на защищенных виртуальных машинах выполняется из директории на SVM.

Основным источником обновлений служат серверы обновлений "Лаборатории Касперского". Вы можете указывать другие источники обновлений в параметрах задачи *Обновление*. Если обновление не может быть выполнено из одного источника обновлений, приложение Kaspersky Endpoint Security переключается к следующему источнику.

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

- 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.

- Централизованное обновление. Централизованное обновление обеспечивает снижение внешнего интернет-трафика, а также удобство контроля за обновлением.

  Централизованное обновление состоит из следующих этапов:

  1. Загрузка пакета обновлений в хранилище внутри сети организации.

     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*.

     Если вы управляете приложением с помощью Kaspersky Security Center Cloud Console, в качестве хранилища вы можете использовать хранилища точек распространения (устройств с установленным Агентом администрирования). Подробнее о точках распространения см. в справке Kaspersky Security Center.

  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 из локальной или сетевой директории (SMB/NFS), смонтированной пользователем, или с FTP-, HTTP- или HTTPS-сервера. Вы можете указать пользовательский источник обновлений в параметрах задачи *Обновление*.

Обновление баз и модулей приложения в Web Console

В Web Console вы можете выполнять обновление баз и модулей приложения с помощью задачи *Обновление*. Вы можете использовать автоматически созданную групповую задачу *Обновление*, а также создавать пользовательские задачи обновления.

Чтобы настроить параметры обновления в Web Console:

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

   Откроется список задач.

2. Выполните одно из следующих действий:

   - Если вы хотите изменить параметры задачи, которая выполняется на всех устройствах, входящих в определенную группу администрирования, нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне группу администрирования.

     В списке отобразятся только задачи, настроенные для выбранной группы администрирования.

   - Если вы хотите изменить параметры задачи, которая выполняется на одном или нескольких устройствах (задачи для набора устройств), нажмите на ссылку в поле **Текущий путь** в верхней части окна и выберите в открывшемся окне верхний узел с именем Сервера администрирования.

     В списке отобразятся все задачи, созданные на Сервере администрирования.

3. В списке задач выберите нужную задачу **Обновление** и откройте окно свойств задачи по ссылке в названии задачи.

4. В окне свойств задачи выберите закладку **Параметры приложения**, в списке слева выберите раздел **Источники обновлений**.

5. 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.

6. Выберите раздел **Параметры** и настройте другие параметры обновления.

7. Выберите закладку **Расписание** и настройте расписание запуска задачи обновления.

   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.

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

Задача будет запускаться в соответствии с настроенным расписанием. Вы также можете запускать задачу вручную.

Раздел Источники обновлений задачи Обновление

Параметр	Описание

Таблица источников 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:
	• **Источник обновлений** – 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 (**Включено** или **Выключено**). Вы можете изменить статус с помощью переключателя в таблице или с помощью переключателя **Использовать этот источник** в окне **Источник обновлений**, которое открывается по ссылке с названием источника.
	Источники обновлений в таблице можно **добавлять**, **изменять**, удалять, перемещать **вверх** и **вниз**.
	При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.
	Кнопка доступна, если в таблице выбран только один элемент.
	При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.
	Кнопка доступна, если в таблице выбран только один элемент.
	Изменение параметров выбранного элемента выполняется в отдельном окне.
	При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

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 приложения	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.

Обновление баз и модулей приложения в Консоли администрирования

В Консоли администрирования вы можете выполнять обновление баз и модулей приложения с помощью задачи *Обновление*. Вы можете использовать автоматически созданную групповую задачу *Обновление*, а также создавать пользовательские задачи обновления.

Чтобы настроить параметры 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 закладку **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 **Обновление** 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 раздел **Расписание** и настройте расписание запуска задачи обновления.

   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.

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**.
	При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.
	Кнопка доступна, если в таблице выбран только один элемент.
	При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.
	Кнопка доступна, если в таблице выбран только один элемент.
	Изменение параметров выбранного элемента выполняется в отдельном окне.
	При нажатии на кнопку **Добавить** открывается окно, в котором вы можете указать параметры нового элемента.

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.

Обновление баз и модулей приложения в командной строке

В командной строке вы можете выполнять обновление баз и модулей приложения следующими способами:

- С помощью предустановленной задачи Обновление (*Update*). Вы можете запускать, останавливать, приостанавливать и возобновлять эту задачу вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры обновления, изменяя параметры этой задачи.

- С помощью пользовательских задач обновления (задач типа *Update*). Вы можете запускать пользовательские задачи вручную и настраивать расписание запуска задач.

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.
`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.

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.

Откат обновления баз и модулей приложения

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, откат обновления баз с помощью задачи не поддерживается.

После первого обновления баз приложения становится доступна функция отката баз приложения к их предыдущей версии.

Каждый раз, когда пользователь запускает процесс обновления, приложение Kaspersky Endpoint Security создает резервную копию текущих баз приложения. Это позволяет откатить базы до предыдущей версии, если требуется.

Откат последнего обновления баз используется, например, если новая версия баз приложения содержит недопустимые сигнатуры, что приводит к блокировке безопасных приложений приложением Kaspersky Endpoint Security.

В командной строке для отката обновлений вы можете запускать предустановленную задачу *Откат обновления баз (Rollback)* или создавать и запускать пользовательские задачи отката обновления (задачи типа *Rollback*).

В Kaspersky Security Center вы можете создавать задачи отката обновления для групп администрирования или отдельных устройств с помощью Web Console или Консоли администрирования.

Задача *Откат обновления баз* не имеет параметров.

Защита от файловых угроз

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы устройства. Компонент включается автоматически с параметрами по умолчанию при запуске приложения Kaspersky Endpoint Security, постоянно находится в оперативной памяти устройства и проверяет все открываемые, сохраняемые и запускаемые файлы в режиме реального времени.

При обнаружении вредоносного ПО приложение Kaspersky Endpoint Security может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

На работу компонента влияет режим перехвата файловых операций, который вы можете выбрать в общих параметрах приложения. По умолчанию на время проверки доступ к файлу блокируется.

Если у пользователя с root-правами отсутствует доступ к файлу на удаленной директории, смонтированной на устройстве по протоколу NFS4, приложение блокирует доступ к файлу для всех пользователей.

Если включена защита от файловых угроз и включен Мониторинг контейнеров (Проверка контейнеров, Мониторинг контейнеров), приложение также проверяет все пространства имен и контейнеры во всех поддерживаемых операционных системах.

Вы можете включать и выключать защиту от файловых угроз, а также настраивать параметры защиты:

- Выбирать режим проверки файлов (при открытии, при открытии и изменении).
- Включать и выключать проверку архивов, почтовых баз, сообщений электронной почты в текстовом формате.
- Временно исключать из повторной проверки файлы в текстовом формате.
- Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
- Выбирать действия, которые приложение будет выполнять над зараженными объектами.
- Настраивать *области проверки*. Приложение будет проверять объекты в указанной области файловой системы.
- Настраивать исключения объектов из проверки. *Исключение из проверки* – это совокупность условий, при выполнении которых приложение не проверяет объекты на наличие вирусов и других вредоносных программ. Вы можете исключать из проверки:
  - объекты по именам или маскам;
  - объекты по названиям обнаруженных в объектах угроз;
  - файлы и директории в указанных областях файловой системы;
  - процесс и файлы, изменяемые указанным процессом.

Приложение также автоматически исключает из проверки некоторые внутренние процессы, например, процесс Watchdog-сервера.

- Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
- Включать и выключать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.

Для оптимизации работы компонента Защита от файловых угроз вы можете настроить 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_#]`.

Настройка защиты от файловых угроз в Web Console

В Web Console вы можете настраивать параметры защиты от файловых угроз в свойствах политики (**Параметры приложения** → **Защита устройств от угроз** → **Защита от файловых угроз**).

Настройка защиты от файловых угроз в Консоли администрирования

В Консоли администрирования вы можете управлять защитой от файловых угроз в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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
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 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.

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.

Параметр	Описание
	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**. 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 `*`). 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. 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.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы 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.
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.

Параметр	Описание
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.
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 (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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
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 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.

Параметр	Описание
	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**. 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 `*`). 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. Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек). Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. 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.

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.

Параметр	Описание
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. 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.
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.

Настройка защиты от файловых угроз в командной строке

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.

Параметры задачи Защита от файловых угроз

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Защита от файловых угроз.

Параметры 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.

Параметр	Описание	Значения
`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.
`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_#`.

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`

`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. 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.
`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:		

Параметр	Описание	Значения
`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=" Проверка почтовых баз "`
`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 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_< номер элемента >=*doc`

Параметр	Описание	Значения
Path	Путь к директории с проверяемыми объектами.	< путь к локальной директории > – проверять объекты в указанной директории. Для указания пути вы можете использовать **маски** и **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 *). 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. Shared:NFS – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS.

Параметр	Описание	Значения
		`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).

Параметр	Описание	Значения
Path	Путь к директории с исключаемыми объектами.	< путь к локальной директории > – исключать из проверки объекты в указанной директории (включая вложенные директории). Для указания пути вы можете использовать **маски** и **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 *). 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. Mounted:NFS – исключать из проверки удаленные директории, смонтированные на устройстве по протоколу NFS.

Параметр	Описание	Значения
		`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. `<тип файловой системы>` – исключать из проверки все ресурсы указанной файловой системы устройства.
Секция **[ExcludedForProgram.item_#]** содержит следующие параметры:		
`ProgramPath`	Путь к исключаемому процессу. Если для перехвата системных событий используется обновляемый модуль ядра, указанный процесс исключается из перехвата во всех пространствах имен.	`< полный путь к процессу >` – 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).

Параметр	Описание	Значения
`Path`	Путь к директории с файлами, которые изменяет процесс.	`< путь к локальной директории >` – исключать из проверки объекты в указанной директории. Для указания пути можно использовать **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. `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.

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 < полный путь к конфигурационному файлу > [--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 <полный путь к конфигурационному файлу> [--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.

Особенности проверки символических и жестких ссылок

Приложение Kaspersky Endpoint Security позволяет проверять символические и жесткие ссылки на файлы.

Проверка символических ссылок

Приложение проверяет символические ссылки, только если файл, на который ссылается символическая ссылка, входит в область проверки компонента Защита от файловых угроз.

Если файл, обращение к которому происходит по символической ссылке, не входит в область проверки компонента Защита от файловых угроз, приложение не проверяет этот файл. Если такой файл содержит вредоносный код, безопасность устройства окажется под угрозой.

Проверка жестких ссылок

При обработке файла, имеющего больше одной жесткой ссылки, приложение лечит исходный файл. Если лечение невозможно, приложение удаляет жесткую ссылку и создает вместо нее копию исходного файла с именем удаленной жесткой ссылки. При удалении приложение удаляет обрабатываемую жесткую ссылку, остальные жесткие ссылки на этот файл обработаны не будут.

Когда вы восстанавливаете файл с жесткой ссылкой из резервного хранилища, приложение создает копию исходного файла с именем жесткой ссылки, которая была помещена в резервное хранилище. Связи с остальными жесткими ссылками на исходный файл восстановлены не будут.

Поиск вредоносного ПО

Поиск вредоносного ПО – это однократная полная или выборочная проверка файлов на устройстве по требованию. Приложение Kaspersky Endpoint Security может выполнять несколько задач поиска вредоносного ПО одновременно.

В приложении создается предустановленная задача *Поиск вредоносного ПО (Scan_My_Computer)*. 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.

Если у пользователя с root-правами отсутствует доступ к файлу на удаленной директории, смонтированной на устройстве по протоколу NFSv4, приложение блокирует доступ к файлу для всех пользователей.

В Kaspersky Security Center мастер первоначальной настройки Kaspersky Security Center автоматически создает групповую задачу поиска вредоносного ПО после установки MMC-плагина управления или веб-плагина управления Kaspersky Endpoint Security.

Во время полной проверки диска процессор будет занят. Рекомендуется запускать задачу полной проверки в нерабочее время.

Вы можете настраивать параметры автоматически созданных задач в Kaspersky Security Center и в командной строке, а также создавать пользовательские задачи поиска вредоносного ПО.

При обнаружении вредоносного ПО приложение Kaspersky Endpoint Security может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

Если во время поиска вредоносного ПО приложение было перезапущено контрольной службой или вручную пользователем, выполнение задачи прерывается. В журнале приложения сохраняется событие *OnDemandTaskInterrupted*.

Вы можете запускать задачи поиска вредоносного ПО и настраивать параметры проверки:

- Выбирать объекты операционной системы, которые нужно проверять: файлы, архивы, загрузочные секторы, память процессов и память ядра, объекты автозапуска.
- Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
- Выбирать действия, которые приложение будет выполнять над зараженными объектами.
- Настраивать исключения объектов из проверки:
  - по именам или маскам;
  - по названиям обнаруженных в объектах угроз.

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.

- Включать и выключать использование глобальных исключений и исключений Защиты от файловых угроз при проверке.
- Включать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.
- Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
- Ограничивать набор устройств, загрузочные секторы которых нужно проверять.
- Настраивать области проверки и области исключения из проверки.

Поиск вредоносного ПО в Web Console

В Web Console 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 поиска вредоносного ПО.

Параметры проверки задачи Поиск вредоносного ПО

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.
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.
Области проверки	Таблица, содержащая области, проверяемые задачей. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы. Области проверки в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз. Вы также можете импортировать список областей проверки из файла по кнопке **Импортировать** и экспортировать список областей проверки в файл в формате JSON по кнопке **Экспортировать**. При импорте вам будет предложено заменить список областей проверки или добавить области проверки к уже существующему списку.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области	Поле ввода названия области проверки. Это название будет отображаться в таблице **Области проверки** в разделе **Параметры 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	В раскрывающемся списке 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.
Протокол доступа	В раскрывающемся списке 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. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**.

Параметр	Описание
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать **маски** и **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 `*`). 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. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, приложение проверяет все директории локальной файловой системы.
Название общего ресурса	Поле ввода названия общего ресурса 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 **Протокол доступа** выбран элемент **Пользовательский**.
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.

Раздел Области проверки

Вы можете настроить параметры области проверки для задачи Поиск вредоносного ПО. Приложение позволяет проверять файлы, загрузочные секторы, память клиентского устройства и объекты автозапуска.

Параметры области проверки задачи Поиск вредоносного ПО

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 клиентского 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	По ссылке **Настроить маски устройств** открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.

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.

Раздел Области исключения

В разделе **Области исключения** для задачи Поиск вредоносного ПО вы можете настроить области исключения, исключения по маске и по названию угрозы, а также использование глобальных исключений и исключений Защиты от файловых угроз во время работы задачи.

Параметры исключений из проверки

Параметр	Описание
Настроить области исключения	По ссылке **Настроить области исключения** открывается окно **Области исключения**. В этом окне вы можете задать список исключений из проверки.
Настроить исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Настроить исключения по названию угрозы	По ссылке **Настроить исключения по названию угрозы** открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Параметр	Описание
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 исключения

Окно содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям.

Параметры области исключения

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 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 **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.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

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 работы приложения. Если флажок установлен, приложение исключает эту область из проверки или защиты во время своей работы. Если флажок снят, приложение включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные директории. • **Смонтированная** – удаленные директории, смонтированные на устройстве. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке 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. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная**.

Параметр	Описание
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать **маски** и **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 `*`). 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. Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек). Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса 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 **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле **Путь**. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

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** или **Изменить** 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 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.

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.

При нажатии на кнопку **Добавить** или **Изменить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

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.

Поиск вредоносного ПО в Консоли администрирования

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 поиска вредоносного ПО.

В разделе **Параметры** в свойствах задачи Поиск вредоносного ПО 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 разделе **Исключения** в свойствах задачи Поиск вредоносного ПО 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
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 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.

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.

Параметр	Описание
	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**. 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 `*`). 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. 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.

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.

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.
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.

Параметр	Описание
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.

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
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 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.

Параметр	Описание
	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**. 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 `*`). 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. Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек). Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. 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.

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.

Поиск вредоносного ПО в командной строке

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.

С помощью команды `kesl-control --scan-file` вы можете выполнять *выборочную проверку* указанных файлов и директорий.

Параметры предустановленной задачи 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.

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.
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
`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. `<маска названия устройства>` – 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_< номер элемента >=*doc`

Параметр	Описание	Значения
`Path`	Путь к директории с проверяемыми объектами.	`< путь к локальной директории >` – 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**. 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. 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.

Выборочная проверка файлов и директорий в командной строке

Вы можете выполнять выборочную проверку указанных файлов и директорий с помощью команды `kesl-control --scan-file`.

Выборочная проверка выполняется с параметрами, которые хранятся в предустановленной задаче *Scan_File* (ID:3). Вы можете настраивать параметры выборочной проверки файлов, изменяя параметры этой задачи (см. таблицу ниже).

Чтобы запустить выборочную проверку указанных файлов и директорий, выполните следующую команду:

```
kesl-control --scan-file <путь> [--action <действие>]
```

где:

- `<путь>` – путь к файлу или директории, которые вы хотите проверить. Вы можете указать несколько путей, разделяя их пробелами.

- `--action <действие>` – действие, которое приложение будет выполнять над зараженными объектами. Возможные значения: `DisinfectDeleteIfNotPossible, DisinfectInformIfNotPossible, Inform`. Если вы не укажете ключ `--action`, приложение будет выполнять действие `DisinfectDeleteIfNotPossible`.

В результате выполнения команды создается временная задача проверки файлов, которая автоматически удаляется после завершения. При этом в консоль выводятся результаты проверки.

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи *Scan_File*.

Секции `[ScanScope.item_#]` и `[ExcludedFromScanScope.item_#]`, заданные в задаче *Scan_File*, не учитываются при выполнении выборочной проверки.

Параметры задачи Scan_File

Параметр	Описание	Значения
`ScanFiles`	Включение проверки файлов.	`Yes` (значение по умолчанию) – проверять файлы. `No` – не проверять файлы.
`ScanBootSectors`	Включение проверки загрузочных секторов.	`Yes` – проверять загрузочные секторы. `No` (значение по умолчанию) – не проверять загрузочные секторы.
`ScanComputerMemory`	Включение проверки памяти процессов и памяти ядра.	`Yes` – проверять память процессов и память ядра. `No` (значение по умолчанию) – не проверять память процессов и память ядра.
`ScanStartupObjects`	Включение проверки объектов автозапуска.	`Yes` – проверять объекты автозапуска. `No` (значение 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` (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.

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.
`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.
`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.	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`

Параметр	Описание	Значения
`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.
`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. `<маска названия устройства>` – 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=" Проверка почтовых баз "`
`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 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_< номер элемента >=*doc`
`Path`	Путь к директории с проверяемыми объектами.	`< путь к локальной директории >` – 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**. 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. 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.

Проверка важных областей

Во время проверки важных областей приложение Kaspersky Endpoint Security может проверять загрузочные секторы, объекты автозапуска, память процессов и память ядра.

При обнаружении вредоносного ПО приложение может удалять зараженный файл и завершать вредоносный процесс, запущенный из этого файла.

Если у пользователя с root-правами отсутствует доступ к файлу на удаленной директории, смонтированной на устройстве по протоколу NFSv4, приложение блокирует доступ к файлу для всех пользователей.

Вы можете запускать проверку важных областей и настраивать параметры проверки:

- Выбирать объекты операционной системы, которые нужно проверять. По умолчанию включена проверка загрузочных секторов, памяти процессов и памяти ядра, объектов автозапуска и архивов. Файлы по умолчанию не проверяются во время проверки важных областей.
- Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
- Выбирать действия, которые приложение будет выполнять над зараженными объектами.
- Настраивать исключения объектов из проверки:
  - по именам или маскам;
  - по названиям обнаруженных в объектах угроз.

  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.
- Включать и выключать использование при проверке глобальных исключений и исключений Защиты от файловых угроз.
- Включать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.
- Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
- Ограничивать набор устройств, загрузочные секторы которых нужно проверять.
- Настраивать области проверки и области исключения из проверки.

Проверка важных областей в Web Console

В Web Console 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.

Параметры задачи Проверка важных областей

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.
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 файлах	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.

Параметр	Описание
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.
Действие 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.
Области проверки	Таблица, содержащая области, проверяемые задачей. По умолчанию таблица содержит одну область проверки, включающую все директории локальной файловой системы. Области проверки в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз. Вы также можете импортировать список областей проверки из файла по кнопке **Импортировать** и экспортировать список областей проверки в файл в формате JSON по кнопке **Экспортировать**. При импорте вам будет предложено заменить список областей проверки или добавить области проверки к уже существующему списку.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области	Поле ввода названия области проверки. Это название будет отображаться в таблице **Области проверки** в разделе **Параметры 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	В раскрывающемся списке 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.
Протокол доступа	В раскрывающемся списке 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. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**.

Параметр	Описание
Путь	Поле ввода пути к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать **маски** и **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 `*`). 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. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**. Если в раскрывающемся списке файловых систем выбран тип **Локальная** и не указан путь, приложение проверяет все директории локальной файловой системы.
Название общего ресурса	Поле ввода названия общего ресурса 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 **Протокол доступа** выбран элемент **Пользовательский**.
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.

Раздел Области проверки

Параметры области проверки задачи Проверка важных областей

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 снят.
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 установлен.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти клиентского 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 установлен.
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 установлен.
Устройства для проверки	По ссылке **Настроить маски устройств** открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.

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.

Раздел Области исключения

В разделе **Области исключения** для задачи Проверка важных областей вы можете настроить области исключения, исключения по маске и по названию угрозы, а также использование глобальных исключений и исключений Защиты от файловых угроз во время работы задачи.

Параметры исключений из проверки

Параметр	Описание
Настроить области исключения	По ссылке **Настроить области исключения** открывается окно **Области исключения**. В этом окне вы можете задать список исключений из проверки.
Настроить исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Настроить исключения по названию угрозы	По ссылке **Настроить исключения по названию угрозы** открывается окно **Исключения по названию угрозы**. В этом окне вы можете настроить исключение объектов из проверки по названию угрозы.

Параметр	Описание
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 исключения

Окно содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям.

Параметры области исключения

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 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 **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.

Окно добавления области исключения

В этом окне вы можете добавить или настроить область исключения.

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 работы приложения. Если флажок установлен, приложение исключает эту область из проверки или защиты во время своей работы. Если флажок снят, приложение включает эту область из проверки или защиты во время своей работы. В дальнейшем вы можете исключить эту область из проверки или защиты, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Файловая система, протокол доступа и путь	В раскрывающемся списке вы можете выбрать тип файловой системы, на которой расположены директории, которые вы хотите добавить в исключения из проверки: • **Локальная** – локальные директории. • **Смонтированная** – удаленные директории, смонтированные на устройстве. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS.
Протокол доступа	В раскрывающемся списке 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. Раскрывающийся список доступен, если в раскрывающемся списке файловых систем выбран тип **Смонтированная**.

Параметр	Описание
Путь	Поле ввода пути к директории, которую вы хотите добавить в область исключения. Для указания пути вы можете использовать **маски** и **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 `*`). 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. Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек). Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы. Поле доступно, если в раскрывающемся списке файловых систем выбран тип **Локальная**.
Название общего ресурса	Поле ввода названия общего ресурса 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 **Протокол доступа** выбран элемент **Пользовательский**.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Маски применяются к объектам только внутри директории, указанной в поле **Путь**. По умолчанию список содержит маску ***** (все объекты). Вы можете добавлять, изменять и удалять маски.

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** или **Изменить** 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 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.

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.

При нажатии на кнопку **Добавить** или **Изменить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

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 важных областей в Консоли администрирования

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 разделе **Параметры** в свойствах задачи Проверка важных областей 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 разделе **Исключения** в свойствах задачи Проверка важных областей 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
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 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.

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.

Параметр	Описание
	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**. 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 `*`). 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. 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.

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.
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.

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.
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.

Параметр	Описание
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.

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
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 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.

Параметр	Описание
	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**. 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 `*`). 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. Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек). Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. 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.

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.

Проверка важных областей в командной строке

В командной строке вы можете выполнять проверку важных областей операционной системы защищаемого устройства с помощью предустановленной задачи Проверка важных областей (*Critical_Areas_Scan*).

Вы можете запускать, останавливать, приостанавливать и возобновлять эту задачу вручную и настраивать расписание запуска задачи. Вы можете настраивать параметры проверки, изменяя параметры этой задачи.

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.
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.

Параметр	Описание	Значения
`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.
`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.

Параметр	Описание	Значения
`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. `< маска имени устройства >` – 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_< номер элемента >=*doc`
`Path`	Путь к директории с проверяемыми объектами.	`< путь к локальной директории >` – 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.

Параметр	Описание	Значения
`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).
`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**. 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. 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.

Проверка съемных дисков

Kaspersky Endpoint Security может проверять следующие съемные диски при подключении их к защищаемому устройству: CD/DVD-приводы, Blu-ray диски, флеш-накопители (включая USB-модемы), внешние жесткие диски и дискеты.

Если проверка съемных дисков включена, приложение Kaspersky Endpoint Security контролирует подключение съемных дисков к защищаемому устройству и при обнаружении подключенного съемного диска проверяет диск и его загрузочные секторы на вирусы и другие вредоносные программы.

По умолчанию приложение не контролирует подключение съемных дисков и не проверяет их.

Настройка проверки съемных дисков в Web Console

В Web Console вы можете настраивать параметры проверки съемных дисков в свойствах политики (**Параметры приложения** → **Защита устройств от угроз** → **Проверка съемных дисков**).

Настройка проверки съемных дисков в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры проверки съемных дисков в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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 Blu-ray дисков) только файлы **определенных типов** и не распаковывать составные объекты. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Проверка важных областей*. 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. • **Подробная проверка** – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Поиск вредоносного ПО*.

Параметр	Описание
Действие при подключении CD/DVD-привода	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять приложение при подключении CD/DVD-приводов и Blu-ray дисков к устройству пользователя: • **Не проверять** CD/DVD-приводы и Blu-ray диски при подключении (значение по умолчанию). • **Быстрая проверка** – проверять на CD/DVD-приводах и Blu-ray дисках только файлы **определенных типов**. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Проверка важных областей*. 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. • **Подробная проверка** – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. 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.

Настройка проверки съемных дисков в командной строке

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 Blu-ray дискам (см. параметр `ScanOpticalDrives`).	`DetailedScan` – проверять все файлы на съемных дисках (за исключением CD/DVD-приводов и Blu-ray дисков). 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 Blu-ray дисков) 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 Blu-ray дисков при подключении к устройству.	`DetailedScan` – проверять все файлы на CD/DVD-приводах и Blu-ray дисках. Детализированная проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Scan_File* (ID:3). `QuickScan` – проверять на CD/DVD-приводах и Blu-ray дисках 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 Blu-ray диски 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

Вы можете выполнять проверку контейнеров и образов на наличие вредоносного ПО в режиме реального времени и по требованию:

- Компонент *Мониторинг контейнеров (Проверка контейнеров, Мониторинг контейнеров)* позволяет проверять запускаемые контейнеры и пространства имен в реальном времени.
- С помощью задач *Проверка контейнеров* вы можете выполнять проверку контейнеров и образов по требованию.

Для использования функциональности проверки контейнеров требуется лицензия, которая включает эту функцию.

Приложение поддерживает интеграцию с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Поддерживается интеграция с системой управления контейнерами Docker версии 28.5.2 и ниже.

Мониторинг контейнеров

По умолчанию компонент Мониторинг контейнеров включен. Приложение проверяет в реальном времени запущенные контейнеры и пространства имен.

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.

Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен. При этом статус компонента Мониторинг контейнеров в командной строке отображается как `Задача доступна и не выполняется`, в Kaspersky Security Center отображается как `Остановлена`.

Вы можете включать и выключать компонент Мониторинг контейнеров, а также настраивать параметры проверки контейнеров и пространств имен в реальном времени:

- Выбирать действие, которое приложение будет выполнять над контейнером при обнаружении зараженного объекта.

  Этот параметр доступен при использовании приложения по лицензии, которая включает эту функцию.

- Настраивать интеграцию приложения Kaspersky Endpoint Security с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

  Поддерживается интеграция с системой управления контейнерами Docker версии 28.5.2 и ниже.

Настройка мониторинга контейнеров в Web Console

В Web Console вы можете настраивать параметры проверки контейнеров в свойствах политики (**Параметры приложения → Общие настройки → Настройки проверки контейнеров**).

Настройка мониторинга контейнеров в Консоли администрирования

В Консоли администрирования вы можете управлять работой компонента Мониторинг контейнеров в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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. Поддерживается использование системы управления контейнерами Docker версии 28.5.2 и ниже.
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.
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.

Настройка мониторинга контейнеров в командной строке

В командной строке вы можете включать и выключать проверку 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.

При проверке пространств имен и контейнеров в реальном времени используются общие параметры проверки контейнеров. Вы можете просматривать и изменять эти параметры с помощью специальных команд управления Kaspersky Endpoint Security:

- Вы можете выводить текущие значения общих параметров проверки контейнеров в консоль или в конфигурационный файл. Этот файл вы можете использовать для изменения параметров.
- Вы можете изменять все общие 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 `< имя параметра >=< значение параметра >`. Текущие значения параметров вы можете получить с помощью команды вывода общих параметров проверки контейнеров.

Чтобы вывести в консоль текущие значения общих параметров проверки контейнеров, выполните следующую команду:

```
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.

Чтобы вывести в файл текущие значения общих параметров проверки контейнеров, выполните следующую команду:

```
kesl-control --get-container-settings --file <путь к конфигурационному файлу> [--json]
```

где:

- `--file <путь к конфигурационному файлу>` – путь к файлу, в который будут сохранены общие 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 общих параметров проверки контейнеров с помощью конфигурационного файла:

1. Выведите общие 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 <путь к конфигурационному файлу> [--json]
   ```

   где:

   - `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу с общими 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 общих параметров проверки контейнеров, заданные в файле, будут импортированы в приложение.

Чтобы изменить значения общих параметров проверки контейнеров с помощью ключей командной строки, выполните следующую команду:

```
kesl-control --set-container-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

где `<имя параметра>=<значение параметра>` – имя и значение одного из общих параметров проверки контейнеров.

Значения указанных общих параметров проверки контейнеров будут изменены.

Проверка контейнеров и образов по требованию

Во время выполнения задачи *Проверка контейнеров* приложение Kaspersky Endpoint Security проверяет контейнеры и образы на наличие вирусов и других вредоносных программ. Приложение может выполнять одновременно несколько задач проверки контейнеров.

Для использования задачи Проверка контейнеров требуется лицензия, которая включает эту функцию.

Приложение поддерживает интеграцию с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Поддерживается интеграция с системой управления контейнерами Docker версии 28.5.2 и ниже.

Вы можете запускать проверку контейнеров и настраивать параметры проверки:

- Указывать контейнеры и образы, которые нужно проверять, по имени или маске имени.
- Включать проверку всех слоев образов и контейнеров.
- Выбирать действие, которое приложение будет выполнять над контейнером, и действие, которое приложение будет выполнять над образом при обнаружении зараженного объекта.
- Настраивать параметры проверки объектов внутри контейнеров или образов:
  - Включать и выключать проверку архивов, почтовых баз, сообщений электронной почты в текстовом формате.
  - Ограничивать размер проверяемого объекта и продолжительность проверки объекта.
  - Выбирать действия, которые приложение будет выполнять над зараженными объектами.
  - Настраивать исключения объектов из проверки:
    - по именам или маскам;
    - по названиям обнаруженных в объектах угроз.
  - Включать и выключать использование глобальных исключений при проверке.
  - Настраивать использование эвристического анализатора и технологии iChecker во время проверки.
  - Включать и выключать запись в журнал информации о проверенных незараженных объектах, о проверке объектов в составе архивов и о необработанных объектах.

Проверка контейнеров в Web Console

В Web Console 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.

Параметры задачи Проверка контейнеров

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.
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.

Параметр	Описание
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.
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.
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.
Действие при обнаружении угрозы	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 контейнер, 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.

Параметр	Описание
Маска имени	Поле ввода имени или маски имени проверяемых образов. По умолчанию указана маска * – выполняется проверка всех образов.
Действие при обнаружении угрозы	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.

Раздел Области исключения

В разделе **Области исключения** для задачи Проверка контейнеров вы можете настроить исключения по маске и по названию угрозы, а также использование глобальных исключений во время работы задачи.

Параметры исключений из проверки

Параметр	Описание
Настроить исключения по маске	По ссылке **Настроить исключения по маске** открывается окно **Исключения по маске**. В этом окне вы можете настроить исключение объектов из проверки по маске имени.
Настроить исключения по названию угрозы	По ссылке **Настроить исключения по названию угрозы** 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** или **Изменить** 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 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.

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.

При нажатии на кнопку **Добавить** или **Изменить** открывается окно **Название угрозы**. В этом окне вы можете задать название угрозы, исключаемой из проверки.

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 контейнеров в Консоли администрирования

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 разделе **Параметры** в свойствах задачи Проверка контейнеров 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 разделе **Исключения** в свойствах задачи Проверка контейнеров 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.
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.

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.

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).

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.

Проверка контейнеров в командной строке

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 команды `kesl-control --scan-container` вы можете выполнять *выборочную проверку* указанных контейнеров и образов.

Параметры задачи Проверка контейнеров

В таблице описаны все доступные значения и значения по умолчанию для всех параметров проверки контейнеров и образов.

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).
		Примеры:
		Проверять контейнер с именем my_container:
		`ContainerNameMask=my_container`
		Проверять все контейнеры, имена которых начинаются с my_container:
		`ContainerNameMask=my_container*`
		Проверять все контейнеры, 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).
		Примеры:
		Проверять образы с именем my_image и значением тега latest:
		`ImageNameMask=my_image:latest`
		Проверять все образы, имена которых начинаются с my_image_, имеющие любое значения тега:
		`ImageNameMask=my_image*`

`DeepScan`	Проверка всех слоев образов и запущенных контейнеров.	`Yes` – проверять все слои. `No` (значение по умолчанию) – не проверять все слои.
`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.
`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.*`

Параметр	Описание	Значения
`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.
`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.

Выборочная проверка контейнеров и образов

Вы можете выполнять выборочную проверку указанных контейнеров и образов с помощью команды `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).

Чтобы запустить выборочную проверку контейнеров, выполните следующую команду:

```
kesl-control --scan-container <идентификатор/имя [:тег ]>
```

где `<идентификатор/имя [:тег ]>` – имя или идентификатор контейнера или образа. Для проверки нескольких объектов вы можете использовать **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.

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.

Примеры:
Проверка контейнера с именем my_container:
`kesl-control --scan-container my_container`
Проверка образа с именем my_image (все теги):
`kesl-control --scan-container my_image*`

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:

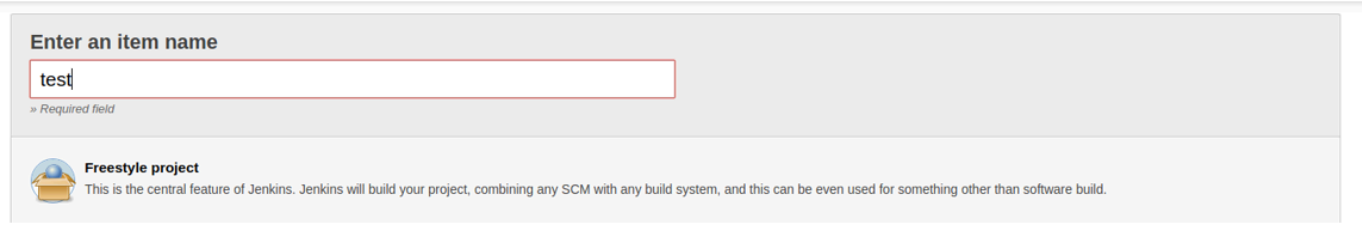
1. Установите Kaspersky Endpoint Security на узле Jenkins.
2. Установите Docker Engine на узле Jenkins.

   Дополнительная информация приведена в документации Docker Engine.
3. Предоставьте пользователю Jenkins права администратора приложения Kaspersky Endpoint Security:

   `kesl-control --grant-role admin <имя пользователя Jenkins>`
4. Добавьте пользователя Jenkins в группу docker:

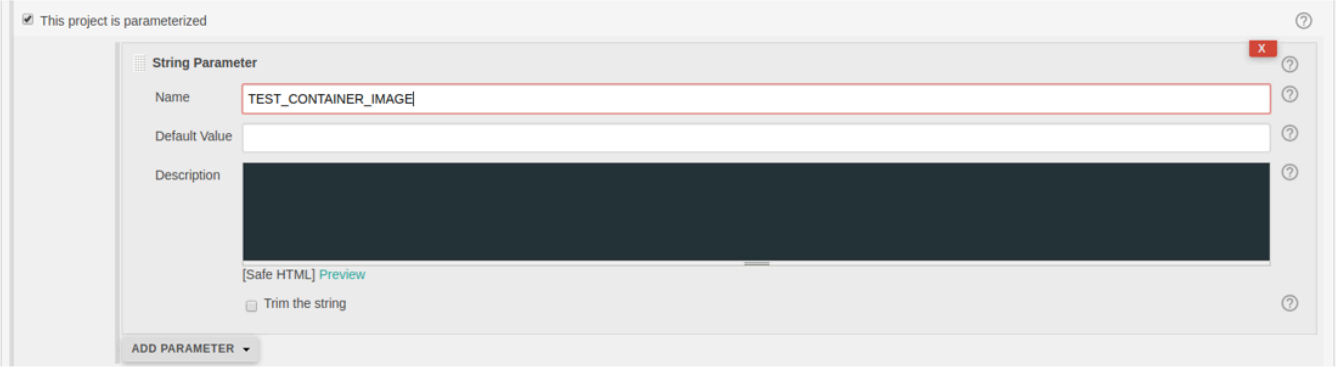
   `sudo usermod -aG docker <имя пользователя Jenkins>`

   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.

Управление сетевым экраном

Во время работы в локальных сетях и интернете устройство подвержено не только заражению вирусами и другими вредоносными приложениями, но и различного рода атакам, использующим уязвимости операционных систем и программного обеспечения. Сетевой экран операционной системы защищает данные, которые хранятся на устройстве пользователя, блокируя большую часть угроз для операционной системы, когда устройство подключено к интернету или локальной сети.

Сетевой экран операционной системы позволяет обнаружить все сетевые соединения на устройстве пользователя и предоставить список их IP-адресов. Компонент Управление сетевым экраном позволяет задать статус этих сетевых соединений при помощи настройки сетевых пакетных правил.

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. Все исходящие соединения по умолчанию разрешены за исключением случаев, когда указаны соответствующие запрещающие правила компонента Управление сетевым экраном.

По умолчанию компонент Управление сетевым экраном выключен.

Перед включением компонента Управление сетевым экраном выключите другие средства управления сетевым экраном операционной системы.

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 требуется, сохраните пользовательские правила сетевого экрана до включения компонента Управление сетевым экраном.

Если управление сетевым экраном включено, Kaspersky Endpoint Security проверяет сетевой экран операционной системы и блокирует любую попытку изменить параметры сетевого экрана, например, когда какое-либо приложение или утилита пытается добавить или удалить какое-либо правило сетевого экрана. Kaspersky Endpoint Security проверяет сетевой экран операционной системы каждые 60 секунд и, если требуется, восстанавливает набор правил сетевого экрана, созданных с помощью приложения. Периодичность проверки изменить невозможно.

Kaspersky Endpoint Security по-прежнему проверяет сетевой экран операционной системы, когда управление сетевым экраном выключено. Это позволяет приложению восстанавливать динамические правила.

Вы можете включать и выключать управление сетевым экраном, а также настраивать следующие параметры:

- Настраивать список сетевых пакетных правил, которые приложение Kaspersky Endpoint Security будет применять при обнаружении попытки установить сетевое соединение. Вы можете добавлять и удалять сетевые пакетные правила, а также изменять приоритет выполнения сетевого пакетного правила.

  В некоторых операционных системах, основанных на кодовой базе Red Hat Enterprise Linux, правила сетевого экрана, созданные в приложении Kaspersky Endpoint Security, можно просмотреть только с помощью команд управления (команда `kesl-control -F --query`).

- Выбирать действия по умолчанию, применяемые к входящим соединениям и пакетам, если другие сетевые пакетные правила не применяются к этому виду соединений.

- Устанавливать соответствие сетевых адресов предустановленным сетям. Вы можете добавлять IP-адреса или подсети в доступные сети и удалять адреса из доступных сетей.

- Включать и выключать автоматическое добавление разрешающих правил для портов Агента администрирования.

О сетевых пакетных правилах

Сетевое пакетное правило представляет собой разрешающее или запрещающее действие, которое совершает Kaspersky Endpoint Security, обнаружив попытку сетевого соединения.

Правила используются для ввода ограничений на сетевые пакеты независимо от приложения. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных.

Все исходящие соединения разрешены по умолчанию (параметр действие по умолчанию) за исключением случаев, когда указаны соответствующие запрещающие правила Управления сетевым экраном. Действие по умолчанию выполняется с самым низким приоритетом: если не сработало никакое другое сетевое пакетное правило или другие сетевые пакетные правила не указаны, соединение разрешается.

Управление сетевым экраном задает по умолчанию некоторые сетевые пакетные правила. Вы можете создавать собственные сетевые пакетные правила и указывать приоритетность выполнения для каждого сетевого пакетного правила.

О динамических правилах

Приложение Kaspersky Endpoint Security позволяет добавлять и удалять в сетевой экран *динамические правила*, необходимые для правильной работы приложения. Например, Агент администрирования добавляет динамические правила, которые разрешают соединение с Kaspersky Security Center, инициируемые как приложением, так и Kaspersky Security Center. Правила Защиты от шифрования тоже являются динамическими.

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 не контролирует динамические правила и не блокирует доступ к сетевым ресурсам для компонентов приложения. 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.

Вы можете просмотреть набор динамических правил (с помощью команды `kesl-control -F --query`), но не можете изменить параметры динамических правил.

О предустановленных доступных сетях

Доступная сеть представляет собой заданную группу IP-адресов или подсетей. С помощью доступной сети вы можете использовать одно и то же правило для нескольких IP-адресов или подсетей, не создавая отдельное правило для каждого IP-адреса или подсети. Доступную сеть можно использовать в качестве значения параметра "удаленный адрес" при создании сетевого пакетного правила. В Kaspersky Endpoint Security предусмотрене три предустановленные сети:

- **Публичная**. Сеть, не защищенная антивирусным приложением, брандмауэром или фильтрами (таким как сети интернет-кафе).
- **Локальная**. Сеть, у пользователей которой есть право доступа к файлам и принтерам на этом устройстве (таким как локальные или домашние сети).
- **Доверенная**. Безопасная сеть, в которой устройства не подвержены атакам или несанкционированным попыткам доступа к данным.

Вы не можете создать новую или удалить предустановленную сеть, но можете добавлять IP-адреса и подсети в сеть или удалять их из нее.

Управление сетевым экраном в Web Console

В Web Console вы можете настраивать параметры управления сетевым экраном в свойствах политики (**Параметры приложения** → **Защита сетевых соединений и средств коммуникации** → **Сетевой экран**).

Управление сетевым экраном в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры управления сетевым экраном в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.

Параметр	Описание
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**

Параметр	Описание
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**.
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**.

Управление сетевым экраном в командной строке

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`.

Параметры задачи Управление сетевым экраном

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`.

Параметр	Описание	Значения
`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.
`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.

Параметр	Описание	Значения
`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.		
`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 в командной строке

Чтобы добавить сетевое пакетное правило, выполните следующую команду:

```
kesl-control --add-rule [--name <название правила>] [--action <действие>] [--protocol <протокол>] [--direction <направление>] [--remote <удаленный адрес>[:<порт или диапазон портов>]] [--local <локальный адрес>[:<порт или диапазон портов>]] [--at <индекс>]
```

где:

- `--name <название правила>` – название сетевого пакетного правила.
- `--action <действие>` – действие, применяемое к соединениям, указанным в сетевом пакетном правиле.
- `--protocol <протокол>` – тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность.
- `--direction <направление>` – направление отслеживаемой сетевой активности.
- `--remote <удаленный адрес [:<порт или диапазон портов>]>` – сетевой адрес удаленного устройства. Вы можете указать имя предустановленной сетевой зоны в качестве удаленного адреса.
- `--local <локальный адрес [:<порт или диапазон портов>]>` – сетевой адрес устройства с установленным приложением Kaspersky Endpoint Security.
- `--at <индекс>` – 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.

Примеры:
Чтобы создать правило, блокирующее все входящие и создаваемые соединения по протоколу TCP через порт 23, выполните следующую команду:

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote any
```

Чтобы создать правило, блокирующее входящие и создаваемые соединения по протоколу TCP через порт 23 для сетевой зоны Публичные, выполните следующую команду:

```
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 <название правила>`
- `kesl-control --del-rule --index <индекс>`

где:

- `--name <название правила>` – название сетевого пакетного правила.
- `--index <индекс>` – 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 <название правила> --at <индекс>`
- `kesl-control --move-rule --index <индекс> --at <индекс>`

где:

- `--name <название правила>` – название сетевого пакетного правила.
- `--index <индекс>` – текущий индекс правила в списке сетевых пакетных правил.
- `--at <индекс>` – новый индекс правила в списке сетевых пакетных правил.

Настройка сетевых зон в командной строке

Чтобы добавить сетевой адрес в зону, выполните следующую команду:

```
kesl-control --add-zone <зона> --address <адрес>
```

где:

- `<зона>` – предустановленное имя сетевой зоны. Возможные значения: `Public`, `Local`, `Trusted`.
- `<адрес>` – сетевой адрес или подсеть.

Чтобы удалить сетевой адрес из зоны, выполните одну из следующих команд:

- `kesl-control --del-zone <зона> --address <адрес>`
- `kesl-control --del-zone <зона> --index <индекс адреса в зоне>`

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.

Защита от веб-угроз

Компонент Защита от веб-угроз позволяет проверять входящий трафик, передаваемый по протоколам HTTP, HTTPS и FTP, веб-сайты и IP-адреса, предотвращать загрузку вредоносных файлов из интернета, а также блокировать доступ к фишинговым, рекламным и прочим опасным веб-сайтам. Защита от веб-угроз использует для перехвата соединений порт 9879. Если порт 9879 занят, то приложение для перехвата соединений автоматически выбирает любой свободный порт.

Остановка или запуск приложения или компонента Защита от веб-угроз приводят к разрыву соединений в перехватываемых портах, например HTTPS.

По умолчанию Защита от веб-угроз выключена. При этом она включается автоматически, если на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в свойствах политики не установлен) и в системе обнаружен один из следующих исполняемых файлов браузеров, в том числе и snap-формата:

- chrome;
- chromium;
- chromium-browser;
- firefox;
- firefox-esr;
- google-chrome;
- opera;
- yandex-browser.

Вы можете включать и выключать Защиту от веб-угроз, а также настраивать параметры защиты:

- Выбирать действие, которое приложение будет выполнять над веб-ресурсом, на котором обнаружен опасный объект.
- Настраивать список доверенных веб-адресов. Приложение не проверяет содержание веб-сайтов, веб-адреса которых указаны в этом списке.
- Выбирать объекты, которые приложение будет обнаруживать во время проверки входящего трафика.
- Настраивать проверку зашифрованных соединений для проверки HTTPS-трафика.

  Для проверки FTP-трафика в параметрах проверки сетевого трафика должен быть настроен контроль всех сетевых портов.

При открытии веб-сайта приложение выполняет следующие действия:

1. Проверяет надежность веб-сайта с помощью загруженных баз приложения.
2. Проверяет надежность веб-сайта с помощью **эвристического анализа**, если он включен.

   Во время эвристического анализа приложение Kaspersky Endpoint Security анализирует активность приложений в операционной системе. Эвристический анализ может обнаружить опасные объекты, о которых нет записей в базах приложения Kaspersky Endpoint Security.
3. Проверяет надежность веб-сайта с помощью репутационных баз "Лаборатории Касперского", если включено использование Kaspersky Security Network.

   > Рекомендуется включить использование Kaspersky Security Network, чтобы увеличить эффективность защиты от веб-угроз.
4. Запрещает или разрешает открыть веб-сайт.

При попытке открытия опасного веб-сайта приложение выполняет следующие действия:

- Для HTTP- или FTP-трафика приложение блокирует доступ и показывает предупреждение.
- Для HTTPS-трафика в браузере отображается страница с ошибкой.

> Удаление сертификатов приложения может привести к некорректной работе компонента Защита от веб-угроз.

> Если вы настроили исключения из перехвата трафика приложением Kaspersky Endpoint Security, они влияют на работу компонента Защита от веб-угроз.

Настройка защиты от веб-угроз в Web Console

В Web Console вы можете настраивать параметры защиты от веб-угроз в свойствах политики (**Параметры приложения** → **Защита сетевых соединений и средств коммуникации** → **Защита от веб-угроз**).

Настройка защиты от веб-угроз в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от веб-угроз в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.

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**.

Параметр	Описание
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.

Настройка защиты от веб-угроз в командной строке

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`	Включает или выключает проверку 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`	Включает или выключает проверку 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`	Включает или выключает использование эвристического анализа для проверки веб-страниц на наличие фишинговых ссылок.	`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`	Включает или выключает проверку 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.

Параметр	Описание	Значения
`CheckOther`	Включает или выключает проверку 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`	Включает или выключает 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**. 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). Использование масок для указания IP-адресов не поддерживается.

Проверка сетевого трафика

Параметры проверки сетевого трафика используются в работе компонентов Защита от веб-угроз, Защита от сетевых угроз, Защита от почтовых угроз и Веб-Контроль. Компоненты Защита от веб-угроз, Защита от почтовых угроз и Веб-Контроль могут расшифровывать и проверять сетевой трафик. По умолчанию проверка зашифрованных соединений включена.

Вы можете настраивать следующие параметры проверки сетевого трафика:

- Включать и выключать проверку зашифрованных соединений.
- Выбирать действие, выполняемое приложением при обнаружении недоверенного сертификата.
- Выбирать действие, выполняемое приложением при возникновении ошибки проверки сетевого трафика на сайте.
- Включать и выключать использование интернета при проверке сертификатов.
- Просматривать и настраивать список доверенных доменов. Приложение не будет проверять соединения, установленные при посещении указанных доменов.
- Настраивать список корневых сертификатов, которые приложение будет считать доверенными во время проверки зашифрованных соединений.
- Настраивать исключения из перехвата трафика. Вы можете указывать соединения, которые приложение будет исключать из перехвата трафика. Исключаемое соединение определяется следующими параметрами:
  - Направление трафика – входящий или исходящий.
  - IP-адрес удаленного устройства – 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).

Исключения из перехвата трафика применяются только для соединений по протоколу TCP и не влияют на работу сетевых пакетных правил. Исключения из перехвата трафика влияют на работу компонентов Защита от веб-угроз, Защита от сетевых угроз и Веб-Контроль.

Вы также можете настраивать исключения из перехвата трафика для приложения Kaspersky Endpoint Security средствами операционной системы.

- Настраивать список сетевых портов, контролируемых приложением. Вы можете указывать определенные сетевые порты или диапазоны сетевых портов для проверки.

  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.

- Выбирать режим перехвата трафика, который приложение использует в своей работе.

При изменении параметров проверки сетевого трафика приложение формирует событие *NetworkSettingsChanged*.

О режимах перехвата сетевого трафика

Приложение может использовать в своей работе один из двух режимов перехвата сетевого трафика:

- *Использовать технологию eBPF*. Если выбран этот режим, приложение использует для перехвата трафика технологию eBPF. Если приложение не смогло использовать технологию eBPF, для перехвата сетевого трафика будет использоваться утилита iptables.

- *Использовать утилиту iptables*. Если выбран этот режим, приложение использует для перехвата трафика утилиту iptables. Этот режим выбран по умолчанию.

В режиме **Использовать технологию 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 простанствами 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.

Если ваше устройство чувствительно к атакам перечислением сетевых портов (например, на локальном устройстве настроен сетевой экран операционной системы с фильтрацией портов), то не рекомендуется выбирать режим **Использовать технологию eBPF**. Также не рекомендуется использовать этот режим перехвата трафика на устройствах периметра сети организации.

В случае если устройство находится в изолированном сегменте сети, в локальной сети или внутри периметра сети организации, допустимо выбирать режим перехвата трафика **Использовать технологию eBPF**.

Вы можете выбрать режим перехвата трафика в Web Console, в Консоли администрирования и в командной строке.

Для изменения режима перехвата трафика требуется перезапустить приложение. Во время перезапуска происходит разрыв установленных сетевых соединений.

Настройка проверки сетевого трафика в Web Console

В Web Console вы можете настраивать параметры проверки сетевого трафика в свойствах политики (**Параметры приложения** → **Общие настройки** → **Настройки сети** и **Параметры приложения** → **Доверенная зона**).

Настройка проверки сетевого трафика в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры проверки сетевого трафика в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.

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.

Настройка проверки сетевого трафика в командной строке

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 < путь к конфигурационному файлу > [--json]
```

где:

- `--file < путь к конфигурационному файлу >` – 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 < путь к конфигурационному файлу > [--json]
   ```

где:

- `--file <путь к конфигурационному файлу>` – 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 <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

где `<имя параметра>=<значение параметра>` – 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 <путь к сертификату>
```

где:

`<путь к сертификату>` – 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 <субъект сертификата>
```

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 <удаленный IP-адрес> --dst-port <порт назначения>
```

где:

- <in|out> – направление трафика в исключаемом соединении. Вы можете настроить исключение для входящего трафика или для исходящего трафика.
- < 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.

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 < удаленный IP-адрес > --dst-port < порт назначения >
```

где:

- <in|out> – направление трафика в исключаемом соединении.
- < удаленный IP-адрес > – адрес удаленного устройства в формате IPv4 или IPv6, трафик на который или с которого исключается из перехвата (в зависимости от направления трафика).
- < порт назначения > – порт на защищенном устройстве (исключение для входящего трафика) или порт на удаленном устройстве (исключение для исходящего трафика).

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.

Если приложение использует технологию eBPF для перехвата трафика, правила kesl_bypass не применяются.

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.

Защита от сетевых угроз

Компонент Защита от сетевых угроз позволяет проверять входящий сетевой трафик на действия, характерные для сетевых атак.

Приложение проверяет входящий трафик для TCP-портов, номера которых приложение Kaspersky Endpoint Security получает из актуальных баз приложения. Защита от сетевых угроз использует для перехвата соединений порт 9789.

Для проверки сетевого трафика компонент Защита от сетевых угроз принимает подключения по всем портам, номера которых получает из баз приложения. При проверке сети это может выглядеть как открытый порт на устройстве, даже если никакое приложение в системе его не прослушивает. Неиспользуемые порты рекомендуется закрывать средствами сетевого экрана.

Текущие соединения для перехватываемых TCP-портов сбрасываются при включении Защиты от сетевых угроз.

Если Защита от сетевых угроз включена, при обнаружении попытки сетевой атаки на защищаемое устройство приложение блокирует сетевую активность со стороны атакующего устройства и создает событие *Обнаружена сетевая атака*. Событие содержит информацию об атакующем устройстве. По умолчанию сетевой трафик со стороны атакующего устройства блокируется на один час. По истечении времени блокировки приложение разблокирует устройство.

По умолчанию Защита от сетевых угроз выключена.

Вы можете включать и выключать Защиту от сетевых угроз, а также настраивать параметры защиты:

- Выбирать действие, которое приложение будет выполнять при обнаружении сетевой активности, характерной для сетевых атак.
- Включать и выключать блокировку сетевой активности при обнаружении попытки сетевой атаки.
- Задавать продолжительность блокировки атакующего устройства.
- Настраивать список IP-адресов, сетевая активность которых не блокируется приложением.

С помощью команд управления заблокированными устройствами в командной строке вы можете посмотреть список заблокированных устройств и вручную разблокировать эти устройства. В Kaspersky Security Center нет инструментов мониторинга и управления заблокированными устройствами, кроме событий *Обнаружена сетевая атака*.

Если вы настроили исключения из перехвата трафика приложением Kaspersky Endpoint Security, они влияют на работу компонента Защита от сетевых угроз.

Настройка защиты от сетевых угроз в Web Console

В Web Console вы можете настраивать параметры защиты от сетевых угроз в свойствах политики (**Параметры приложения → Защита сетевых соединений и средств коммуникации → Защита от сетевых угроз**).

Настройка защиты от сетевых угроз в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от сетевых угроз в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.
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.

Настройка защиты от сетевых угроз в командной строке

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.

Параметры 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.

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 и расширенные версии протоколов – POP3S, SMTPS и IMAPS – в почтовых клиентах МойОфис Почта и Органайзер Р7-Офис. Другие протоколы Защита от почтовых угроз не поддерживает.

Для работы компонента Защита от почтовых угроз в параметрах сети должны контролироваться сетевые порты 25, 465, 587, 110, 995, 143 и 993. 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. Вы можете включать, выключать и настраивать параметры Защиты от почтовых угроз с помощью Web Console, Консоли администрирования и командной строки.

Настройка защиты от почтовых угроз в Web Console

В Web Console вы можете настраивать параметры защиты от почтовых угроз в свойствах политики (**Параметры приложения** → **Защита сетевых соединений и средств коммуникации** → **Защита от почтовых угроз**).

Настройка защиты от почтовых угроз в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от почтовых угроз в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.

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.

Настройка защиты от почтовых угроз в командной строке

В командной строке вы можете управлять защитой от почтовых угроз с помощью предустановленной задачи Защита от почтовых угроз (*Mail_Monitoring*).

Задача Защита от почтовых угроз запущена по умолчанию. Вы можете запускать и останавливать эту задачу вручную.

Для запуска и остановки задачи Защита от почтовых угроз из командной строки требуются права роли Администратор.

Вы можете настраивать параметры защиты от почтовых угроз, изменяя параметры предустановленной задачи Защита от почтовых угроз.

В таблице ниже описаны доступные значения и значения по умолчанию для параметров, которые вы можете указать для задачи Защита от почтовых угроз.

Параметр	Описание	Значения
`CheckIncomingMessagesOnly`	*Область защиты* – это объекты, которые проверяет компонент во время своей работы: входящие и исходящие сообщения или только входящие сообщения.	`Yes` – приложение проверяет только входящие сообщения. `No` (по умолчанию) – приложение проверяет входящие и исходящие сообщения.
`ScanFileArchive`	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).	`Yes` (по умолчанию) – приложение проверяет вложенные архивы. `No` – приложение не проверяет вложенные архивы.
`ScanFileOffice`	Включает или выключает проверку вложенных файлов офисных форматов.	`Yes` (по умолчанию) – приложение проверяет вложенные файлы офисных форматов. `No` – приложение не проверяет вложенные файлы офисных форматов.
`UseSizeLimit`	Ограничивает размер проверяемых вложенных архивов.	`Yes` – приложение исключает из проверки вложенные в сообщения электронной почты архивы, размер которых больше заданного с помощью аргумента `SizeLimit`. `No` (по умолчанию) – приложение проверяет архивы любого размера, вложенные в сообщения электронной почты.
`SizeLimit`	Задает максимальный размер проверяемых вложенных архивов.	1 – 9999 (МБ).
`UseTimeLimit`	Ограничивает максимальную продолжительность проверки вложенных архивов.	`Yes` – приложение завершает проверку вложенных архивов через указанное с помощью аргумента `TimeLimit` время. `No` (по умолчанию) – время проверки вложенных архивов не ограничено.
`TimeLimit`	Задает максимальную продолжительность проверки вложенных архивов.	1 – 9999 (сек.)
`ExtensionFilter`	Настраивает фильтрацию почтовых вложений.	`Disable` – приложение не фильтрует файлы, вложенные в сообщения электронной почты. `Rename` (по умолчанию) – приложение заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_). Таким образом, чтобы открыть файл, пользователю нужно переименовать файл. `Delete` – приложение удаляет из сообщений электронной почты вложенные файлы указанных типов.

Параметр	Описание	Значения

`ExtensionMasks`	Задает расширения для типов вложений, которые нужно переименовывать или удалять из сообщений электронной почты.	Список из нескольких расширений задается следующим образом:
		`[ExtensionMasks.item_0000]`
		`UseExtensionMask=Yes`
		`ExtensionMask=*.txt`
		`[ExtensionMasks.item_0001]`
		`UseExtensionMask=Yes`
		`ExtensionMask=*.run`
		`[ExtensionMasks.item_0002]`
		`UseExtensionMask=Yes`
		`ExtensionMask=*.exe`
		`...`
		По умолчанию обрабатываются файлы с расширениями TXT, RUN, EXE, JS, JSE, MSI, SCR, VBE, VBS, SH.
		Для изменения списка расширений необходимо экспортировать параметры задачи в INI-файл, затем отредактировать список в файле и импортировать INI-файл в приложение.

`UseAnalyzer`	Включает или выключает использование эвристического анализатора.	`Yes` (по умолчанию) – эвристический анализатор включен. `No` – эвристический анализатор выключен.
`AnalyzerLevel`	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.	`Light` – наименее детализированная проверка, минимальная нагрузка на систему. `Medium` (по умолчанию) – средняя детализация при проверке, сбалансированная нагрузка на систему. `Deep` – наиболее детализированная проверка, максимальная нагрузка на систему.
`ActionOnThreat`	Действие, которое выполняет Защита от почтовых угроз при обнаружении угрозы во входящих почтовых сообщениях. Параметр `ActionOnThreat` не применим к исходящим сообщениям. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения.	`DisinfectDeleteIfNotPossible` (по умолчанию) – 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. `DisinfectBlockIfNotPossible` – 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. `Block` – блокировать. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением.

Защита от атак BadUSB

Некоторые вирусы изменяют встроенное программное обеспечение USB-устройств так, чтобы операционная система определяла USB-устройство как клавиатуру. В результате вирус может выполнять команды под вашей учетной записью, например загрузить вредоносное приложение.

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

Когда к устройству подключается USB-устройство, определенное операционной системой как клавиатура, приложение предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) цифровой код, сформированный приложением. Эта процедура называется авторизацией клавиатуры.

Если код введен правильно, приложение сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется.

> При подключении авторизованной клавиатуры через другой USB-порт устройства приложение снова запрашивает ее авторизацию.

Если цифровой код введен неправильно, приложение формирует новый. Вы можете настроить число попыток ввода цифрового кода. Если цифровой код введен неправильно несколько раз или закрыто окно авторизации клавиатуры, приложение блокирует ввод с этой клавиатуры. По истечении времени блокировки USB-устройства или перезагрузке операционной системы приложение снова предлагает пройти авторизацию клавиатуры.

Приложение разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.

По умолчанию компонент Защита от атак BadUSB выключен. Вы можете включать, выключать и настраивать параметры Защиты от атак BadUSB с помощью Web Console, Консоли администрирования и командной строки.

Настройка защиты от атак BadUSB в Web Console

В Web Console вы можете настраивать параметры защиты от атак BadUSB в свойствах политики (**Параметры приложения → Защита устройств от угроз → Защита от атак BadUSB)**.

Настройка защиты от атак BadUSB в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от веб-угроз в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Базовая защита → Защита от атак Bad USB**).

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. Значение по умолчанию: 5.
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). Значение по умолчанию: 5.
Запретить использование экранной клавиатуры для авторизации USB-устройств	Если флажок установлен, приложение запрещает использование экранной клавиатуры для авторизации USB-устройства, с которого невозможно ввести код авторизации. По умолчанию флажок снят.

Настройка защиты от атак BadUSB в командной строке

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 не запрещает использование экранной клавиатуры для авторизации USB-устройств, с которых невозможно ввести код авторизации.

Защита от удаленного вредоносного шифрования

Компонент Защита от шифрования позволяет защитить ваши файлы в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования.

Для использования компонента требуется лицензия, которая включает эту функцию.

Если защита от шифрования включена, приложение Kaspersky Endpoint Security проверяет действия удаленных устройств с файловыми ресурсами, расположенным в общих сетевых директориях защищаемого устройства, на наличие вредоносного шифрования. Если приложение расценивает действия удаленного устройства, получающего доступ к общим сетевым ресурсам, как вредоносное шифрование, приложение создает и включает правило для сетевого экрана операционной системы, которое блокирует сетевой трафик от скомпрометированного устройства. Скомпрометированное устройство добавляется в список недоверенных устройств, доступ к общим сетевым директориям для всех недоверенных устройств блокируется. Приложение создает событие *Обнаружено шифрование*, которое содержит информацию о скомпрометированном устройстве.

По умолчанию приложение блокирует доступ недоверенных устройств к сетевым файловым ресурсам на 30 минут. По истечении времени блокировки приложение удаляет скомпрометированное устройство из списка недоверенных устройств, доступ устройства к сетевым файловым ресурсам автоматически восстанавливается.

Правила сетевого экрана, созданные компонентом Защита от шифрования, нельзя удалить с помощью утилиты iptables, так как приложение восстанавливает набор правил каждую минуту.

По умолчанию Защита от удаленного вредоносного шифрования выключена.

Вы можете включать и выключать защиту от вредоносного шифрования, а также настраивать параметры защиты:

- Выбирать действие, которое приложение будет выполнять при обнаружении шифрования: информировать пользователя или блокировать устройство, осуществляющее вредоносное шифрование.

  Если выбрано действие *Информировать*, приложение все равно проверяет действия удаленных устройств с сетевыми файловыми ресурсами на наличие вредоносного шифрования, когда защита от шифрования включена. В случае обнаружения вредоносного шифрования создается событие *Обнаружено шифрование*, но скомпрометированное устройство не блокируется.

- Задавать продолжительность блокировки недоверенного устройства.

- Указывать файлы и директории, которые приложение защищает от вредоносного шифрования.

- Указывать файлы и директории, которые исключены из защиты от вредоносного шифрования.

  Приложение не расценивает действия как шифрование, если активность шифрования обнаружена в директориях, исключенных из защиты от шифрования.

С помощью команд управления заблокированными устройствами в командной строке вы можете посмотреть список заблокированных устройств и вручную разблокировать эти устройства. В Kaspersky Security Center нет инструментов мониторинга и управления заблокированными устройствами, кроме событий *Обнаружено шифрование*.

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.

Компонент Защита от шифрования корректно работает с протоколами SMB1, SMB2, SMB3, NFS3, TCP/UDP и IP/IPv6. Работа с протоколами NFS2 и NFS4 не поддерживается. Рекомендуется настроить параметры сервера таким образом, чтобы протоколы NFS2 и NFS4 было невозможно использовать для подключения ресурсов.

Приложение Kaspersky Endpoint Security не блокирует доступ к сетевым файловым ресурсам, пока действия устройства не расцениваются как вредоносные. Таким образом, минимум один файл будет зашифрован, прежде чем приложение обнаружит вредоносную активность.

Настройка защиты от шифрования в Web Console

В Web Console вы можете настраивать параметры защиты от шифрования в свойствах политики (**Параметры приложения → Защита устройств от угроз → Защита на основе анализа поведения → Защита от шифрования**).

Настройка защиты от шифрования в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от шифрования в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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
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 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 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.

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** – 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**. 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. Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек). Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. 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.

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
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 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**. 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 `*`). 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. По умолчанию указан путь **/** – приложение исключает из проверки все директории локальной файловой системы.

Параметр	Описание
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.

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.

Настройка защиты от шифрования в командной строке

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).

Параметр	Описание	Значения
`Path`	Путь к директории с защищаемыми объектами.	`<путь к локальной директории>` – защищать локальную директорию, доступную через SMB/NFS. Для указания пути вы можете использовать **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. `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`.
`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).

Параметр	Описание	Значения
`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**. 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. `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.

Управление 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:

- При обнаружении вредоносного шифрования приложение блокирует доступ удаленного устройства к общим сетевым директориям защищаемого устройства.
- При обнаружении попытки сетевой атаки на защищаемое устройство приложение блокирует сетевой трафик со стороны атакующего устройства.

Вы можете изменять продолжительность блокировки в параметрах защиты от сетевых угроз и защиты от удаленного вредоносного шифрования. По истечении заданного периода времени приложение разблокирует устройство.

Если вы управляете приложением с помощью командной строки, вы можете использовать команды управления заблокированными устройствами, чтобы посмотреть список устройств, заблокированных в результате работы приложения на устройстве, и вручную разблокировать эти устройства до истечения времени блокировки. В Kaspersky Security Center нет инструментов мониторинга и управления заблокированными устройствами, кроме событий *Обнаружена сетевая атака* и *Обнаружено шифрование*.

Чтобы просмотреть список заблокированных устройств, выполните следующую команду:

```
kesl-control --get-blocked-hosts
```

В результате выполнения команды приложение выводит список заблокированных устройств в консоль.

Чтобы разблокировать устройства, выполните следующую команду:

```
kesl-control --allow-hosts <адрес>
```

где `<адрес>` – 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.

В результате выполнения команды приложение разблокирует указанные устройства.

Примеры:
Адреса IPv4:
```
dec - 192.168.0.1
dec - 192.168.0.0/24
```
Адреса IPv6:
```
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210%1
hex - 2001:db8::ae21:ad12
hex - ::ffff:255.255.255.254
hex - ::
```

Контроль приложений

Компонент Контроль приложений позволяет управлять запуском приложений на защищаемых устройствах. Контроль приложений снижает риск заражения устройства, ограничивая доступ пользователей к приложениям. Вы можете получать информацию о приложениях, установленных на защищаемых устройствах с помощью задачи Инвентаризация.

Для использования компонента требуется лицензия, которая включает эту функцию.

Запуск приложений регулируется с помощью *правил контроля приложений*.

Компонент Контроль приложений может работать в одном из двух режимов:

- *Список запрещенных*. Режим, при котором приложение Kaspersky Endpoint Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений. По умолчанию компонент Контроль приложений работает в этом режиме.
- *Список разрешенных*. Режим, при котором приложение Kaspersky Endpoint Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.

Если правила контроля приложений сформированы максимально полно, Kaspersky Endpoint Security запрещает запуск всех новых, не проверенных администратором локальной сети организации приложений, но обеспечивает работоспособность операционной системы и проверенных приложений, которые нужны пользователям для выполнения должностных обязанностей.

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.

По умолчанию Контроль приложений выключен. Вы можете включать и выключать Контроль приложений, а также настраивать параметры работы компонента:

- Выбирать режим компонента Контроль приложений: *список разрешенных* или *список запрещенных*.
- Создавать правила контроля приложений для каждого режима компонента.
- Выбирать действие, которое приложение Kaspersky Endpoint Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего правилам. Kaspersky Endpoint Security может *применять правила* и выполнять заданные в правилах действия или *тестировать правила* и только информировать о попытке запуска приложения, удовлетворяющего правилам.
- Экспортировать и импортировать настроенные параметры Контроля приложений.

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 приложений, то Kaspersky Endpoint Security не блокирует скрипт, запущенный из этого интерпретатора. Если запуск хотя бы одного из скриптов, указанных в командной строке интерпретатора, запрещен правилами Контроля приложений, то Kaspersky Endpoint Security блокирует все скрипты, указанные в командной строке интерпретатора. Исключение: cat script.py | python.

О правилах контроля приложений

Правило контроля приложений представляет собой набор параметров, которые содержат условия срабатывания правила и действия компонента Контроль приложений при срабатывании правила (разрешение или запрет пользователям запускать приложение):

- Принадлежность приложения к категории приложений. *Категория приложений* – это группа приложений, обладающих общими признаками. Например, категория, в которую входят исполняемые файлы установленных приложений, или категория приложений, необходимых для работы, в которую входит стандартный набор приложений, используемых в организации. Вы можете использовать одну и ту же категорию только в одном правиле.

  Использование KL-категорий приложения Kaspersky Security Center не поддерживается приложением Kaspersky Endpoint Security.

- Разрешение или запрет выбранным пользователям и/или группам пользователей запускать приложения. Вы можете указать пользователя и/или группу пользователей, которым разрешен или запрещен запуск приложений из указанной категории.

- Условие срабатывания правила. Условие представляет собой соответствие "тип условия – критерий условия – значение условия". На основании условий срабатывания правила приложение Kaspersky Endpoint Security применяет или не применяет правило к приложению. В правилах используются включающие и исключающие условия:

  - *Включающие условия*. Kaspersky Endpoint Security применяет правило к приложению, если приложение соответствует хотя бы одному включающему условию.

  - *Исключающие условия*. Kaspersky Endpoint Security не применяет правило к приложению, если приложение соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию.

  Условия срабатывания правила формируются с помощью следующих критериев:

  - имя исполняемого файла приложения;

  - имя директории с исполняемым файлом приложения;

  - хеш исполняемого файла приложения. Допускается использование только SHA256.

  Для каждого критерия, используемого в условии, вам нужно указать его значение.

Для указания имен файлов и директорий вы можете использовать **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.

Если параметры запускаемого приложения соответствуют критериям, указанным во включающем условии, правило срабатывает. В этом случае Kaspersky Endpoint Security выполняет действие, указанное в правиле. Если параметры приложения соответствуют критериям, указанным в исключающем условии, Kaspersky Endpoint Security не контролирует запуск приложения.

Правила контроля приложений могут иметь один из следующих *статусов работы*:

- *Включено* – правило включено, Kaspersky Endpoint Security применяет это правило для контроля приложений.
- *Выключено* – правило выключено и не используется для контроля приложений.
- *Тест* – Kaspersky Endpoint Security разрешает запуск приложений, которые удовлетворяют условиям правила, но регистрирует информацию о запуске этих приложений в отчете.

Статус работы правила имеет более высокий приоритет чем действие, указанное в правиле.

Режим тестирования правил контроля приложений

Чтобы убедиться, что правила Контроля приложений не блокируют приложения, необходимые для работы, рекомендуется включить *тестирование правил* контроля приложений. В этом режиме Kaspersky Endpoint Security не будет блокировать запуск сторонних приложений, но будет отправлять 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 результатам 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 for 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.

Настройка контроля приложений в Web Console

В Web Console вы можете настраивать параметры контроля приложений в свойствах политики (**Параметры приложения** → **Контроль безопасности** → **Контроль приложений**).

Настройка контроля приложений в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры контроля приложений в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.

Параметр	Описание
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.

Настройка контроля приложений в командной строке

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 команду `kesl-control --set-settings` с флагом `--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.

Параметры задачи Контроль приложений

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Контроль приложений.

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.

Параметр	Описание	Значения
`IncludeFileNames.item_#`	Имя исполняемого файла, на которое срабатывает правило.	Для указания имени файла вы можете использовать **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.
`IncludeFolders.item_#`	Имя директории с исполняемым файлом приложения, на которое срабатывает правило.	Для указания имени директории вы можете использовать **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.
`IncludeHashes.item_#`	Хеш SHA256 исполняемого файла, на который срабатывает правило.	Допускается использование только SHA256.
`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**. 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.
`ExcludeFolders.item_#`	Имя директории с исполняемым файлом приложения, на которое срабатывает правило.	Для указания имени директории вы можете использовать **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.
`ExcludeHashes.item_#`	Хеш SHA256 исполняемого файла, на который срабатывает правило.	Допускается использование только SHA256.

Параметр	Описание	Значения
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.		
`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.

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 <путь к конфигурационному файлу>
```

где:

`--file <путь к конфигурационному файлу>` – путь к конфигурационному файлу с параметрами категорий.

Файл с параметрами категорий должен иметь такую структуру:

```
[
     {
          "Exclude" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)",
   "(FileHash == <хеш исполняемого файла>)" ],
          "GUID" : "<уникальный идентификатор категории>",
          "Include" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)",
   "(FileHash == <хеш исполняемого файла>)" ],
          "Name" : "<название категории 1>"
     },
   {
          "Exclude" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)",
   "(FileHash == <хеш исполняемого файла>)" ],
          "GUID" : "<уникальный идентификатор категории>",
          "Include" : [ "(FilePath like <полный путь к исполняемому файлу приложения>)",
   "(FileHash == <хеш исполняемого файла>)" ],
          "Name" : "<название категории 2>"
     }
]
```

Для указания имени файла в полях `Exclude` и `Include` вы можете использовать **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.

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 <название категории 1> <название категории 2> … <название категории N>] --file <путь к конфигурационному файлу>
```

где:

- `<название категории 1> <название категории 2> … <название категории 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 <путь к конфигурационному файлу>` – путь к конфигурационному файлу с параметрами категорий.

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 <путь к конфигурационному файлу>] [--json]
```

где:

- `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу формата JSON, в который будут выведены параметры.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ --json, параметры будут выведены в формате INI.

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 <название категории 1> <название категории 2> ... <название категории N>] [--file <путь к конфигурационному файлу>] [--json]
```

где:

- `<название категории 1> <название категории 2> ... <название категории N>` – названия категорий, информацию о которых вы хотите просмотреть. Если вы хотите просмотреть информацию о нескольких категориях, укажите названия категорий через пробел.
- `--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу формата JSON, в который будут выведен список категорий.
- `--json` – выводить параметры в формате JSON. Если вы не укажете ключ --json, параметры будут выведены в формате INI.

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 configuration file>] [--json]
```

где:

- `--file <path to 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 configuration file>] [--json]
```

где:

- `--file <path to 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
```

Экспорт и импорт параметров Контроля приложений

Для упрощения настройки компонента Контроль приложений на устройствах пользователей вы можете экспортировать и импортировать параметры Контроля приложений и список категорий приложений.

Экспорт и импорт параметров Контроля приложений в Web Console

В Web Console вы можете экспортировать и импортировать параметры Контроля приложений и список категорий приложений в свойствах управляемого устройства (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → закладка **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → закладка **Параметры приложения** → раздел **Контроль приложений**).

По нажатию на кнопку **Экспортировать** в блоке **Параметры Контроля приложений** открывается окно, в котором вам нужно указать файл, в который вы хотите сохранить настроенные параметры. По нажатию на кнопку **Импортировать** в блоке **Параметры Контроля приложений** открывается окно, в котором вам нужно указать файл, из которого вы хотите импортировать параметры.

По нажатию на кнопку **Экспортировать** в блоке **Категории приложений** открывается окно, в котором вам нужно указать файл, в который вы хотите сохранить добавленные категории приложений. По нажатию на кнопку **Импортировать** в блоке **Категории приложений** открывается окно, в котором вам нужно указать файл, из которого вы хотите импортировать категории приложений.

Экспорт и импорт параметров Контроля приложений в Консоли администрирования

В Консоли администрирования вы можете экспортировать и импортировать параметры Контроля приложений и список категорий приложений в свойствах управляемого устройства (**Управляемые устройства** → закладка **Устройства** → окно свойств устройства → раздел **Приложения** → <название приложения> → кнопка **Свойства** → окно **Параметры <название приложения>** → раздел **Контроль приложений**).

По нажатию на кнопку **Экспортировать** в блоке **Параметры Контроля приложений** открывается окно, в котором вам нужно указать файл, в который вы хотите сохранить настроенные параметры. По нажатию на кнопку **Импортировать** в блоке **Параметры Контроля приложений** открывается окно, в котором вам нужно указать файл, из которого вы хотите импортировать параметры.

По нажатию на кнопку **Экспортировать** в блоке **Категории приложений** открывается окно, в котором вам нужно указать файл, в который вы хотите сохранить добавленные категории приложений. По нажатию на кнопку **Импортировать** в блоке **Категории приложений** открывается окно, в котором вам нужно указать файл, из которого вы хотите импортировать категории приложений.

Экспорт и импорт параметров Контроля приложений в командной строке

В командной строке вы можете экспортировать и импортировать параметры Контроля приложений и список категорий приложений с помощью команд управления Контролем приложений.

Инвентаризация

Задача Инвентаризация позволяет получить информацию обо всех исполняемых файлах приложений, хранящихся на клиентских устройствах. Получение информации о приложениях, установленных на устройствах, может быть полезно, например, для создания правил контроля приложений.

Для использования задачи требуется лицензия, которая включает эту функцию.

Вы можете настраивать следующие параметры инвентаризации:

- Выбирать типы объектов, которые приложение будет обнаруживать на устройстве в ходе инвентаризации (файлы, скрипты).
- Настраивать области инвентаризации (пути к директориям, в которых нужно искать исполняемые файлы приложений).
- Настраивать исключения из инвентаризации.
- Выбирать действие, которое приложение Kaspersky Endpoint Security выполняет с категорией приложений "Золотой образ" ("Golden Image") по завершении задачи Инвентаризация. В категорию можно добавлять приложения, обнаруженные на устройстве в результате выполнения задачи, можно оставить категорию без изменений или удалить.
- Включать и выключать передачу на Сервер администрирования Kaspersky Security Center информации о приложениях, которые обнаружены на устройстве в результате выполнения задачи Инвентаризация. Если информация о приложениях на устройстве передается на Сервер администрирования, она может использоваться для настройки через Kaspersky Security Center категорий приложений, на основе которых создаются правила компонента Контроль приложений.

Настройка инвентаризации в Web Console

В Web Console вы можете выполнять инвентаризацию приложений защищаемого устройства с помощью задачи *Инвентаризация*.

Вы можете создавать и запускать пользовательские задачи инвентаризации. Вы можете настраивать параметры инвентаризации, изменяя параметры этих 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" 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". Если категория отсутствует, она будет создана. Если категория существует, список приложений в ней будет обновлен. • **Удалить** – удалять категорию приложений "Золотой образ" после выполнения инвентаризации. Вы можете использовать категорию "Золотой образ" 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	Таблица, содержащая области инвентаризации, проверяемые приложением. Приложение проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит одну область инвентаризации – /usr/bin. Области инвентаризации в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз. Вы также можете импортировать список областей инвентаризации из файла по кнопке **Импортировать** и экспортировать список областей инвентаризации в файл в формате JSON по кнопке **Экспортировать**. При импорте вам будет предложено заменить список областей инвентаризации или добавить области инвентаризации к уже существующему списку.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область проверки для задачи Инвентаризация.

Параметры области инвентаризации

Параметр	Описание
Название области	Поле ввода названия области инвентаризации. Это название будет отображаться в таблице раздела **Параметры 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 инвентаризации во время выполнения задачи. Если флажок снят, приложение не обрабатывает эту область инвентаризации 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 инвентаризации. Для указания пути вы можете использовать **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. Поле не должно быть пустым. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы.

Параметр	Описание
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.

Раздел Области исключения

В разделе **Области исключения** для задачи Инвентаризация вы можете настроить области исключения 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
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 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 **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.

Окно добавления области 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**. 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. Поле не должно быть пустым.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Вы можете добавлять, изменять и удалять маски.

Настройка инвентаризации в Консоли администрирования

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" 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** – удалять категорию приложений "Золотой образ" после выполнения инвентаризации. Вы можете использовать категорию "Золотой образ" 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**. 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. 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.

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
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 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. 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.
Маски	Список содержит маски имен объектов, которые приложение исключает из проверки. Вы можете добавлять, изменять и удалять маски.

Настройка инвентаризации в командной строке

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.

Параметры задачи Инвентаризация

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Инвентаризация.

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" после выполнения инвентаризации. `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` – удалять категорию приложений "Золотой образ" после выполнения инвентаризации.
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.
`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).

Параметр	Описание	Значения
`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**. 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 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.

Контроль устройств

Компонент *Контроль устройств* позволяет управлять доступом пользователей к устройствам, которые установлены на клиентском устройстве или подключены к нему (например, к жестким дискам, камерам или модулям Wi-Fi). Управление доступом позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных.

Компонент Контроль устройств включается автоматически с параметрами по умолчанию при запуске приложения Kaspersky Endpoint Security.

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.

  - *Блокировать* – запрещать доступ к устройствам этого типа.

  - *В зависимости от шины подключения* – разрешать или запрещать доступ к устройствам в зависимости от режима доступа для шины, по которой подключено устройство.

  - *По правилам* – 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). 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.

  - *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.

- **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.

  - *Блокировать* – запрещать доступ к устройствам, подключенным по этой шине подключения.

  Например, может быть запрещен доступ ко всем устройствам, подключенным по шине USB.

По умолчанию для всех типов устройств выбран режим доступа *В зависимости от шины подключения*, для шин подключения выбран режим доступа *Разрешать*. В соответствии с этими параметрами Контроль устройств предоставляет пользователям полный доступ ко всем устройствам.

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.

При выключении компонента Контроль устройств приложение разблокирует доступ к заблокированным устройствам.

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.

Вы можете включать и выключать Контроль устройств, а также настраивать параметры работы компонента:

- Выбирать режим работы приложения при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств: блокировать или только информировать о попытке доступа к устройству.
- Выбирать режим доступа к устройствам в зависимости от их типа.
- Выбирать режим доступа к устройствам в зависимости от шины, по которой подключаются устройства.
- Исключать отдельные устройства из области действия Контроля устройств, добавляя их в список доверенных устройств. *Доверенные устройства* – это устройства, к которым у пользователей есть полный доступ. Например, вы можете разрешить доступ к конкретным USB-устройствам или только к USB-накопителям, при этом доступ к остальным USB-устройствам будет запрещен. Кроме того, вы можете указать пользователей или группы пользователей, для которых устройства будут доверенными.

  Вы можете управлять списком доверенных устройств через командную строку или с помощью Kaspersky Security Center.

  Вы можете добавлять устройства в список доверенных по идентификатору или маске идентификатора устройства. Вы можете получить информацию об устройствах, установленных на клиентских устройствах или подключенных к ним, с помощью командной строки на клиентском устройстве или с помощью Kaspersky Security Center. Передача информации на Сервер администрирования Kaspersky Security Center включена по умолчанию.

  Информация об устройствах передается, если клиентское устройство находится под управлением активной политики и выполнена синхронизация с Агентом администрирования (выполняется с частотой, указанной в свойствах политики Агента администрирования, по умолчанию – каждые 15 минут).

Если вы управляете приложением с помощью Kaspersky Security Center, для добавления устройств в список доверенных вы также можете использовать:

- Список устройств, обнаруженных на управляемых клиентских устройствах. Список отображается в свойствах политики в Web Console или в Консоли администрирования.
- Список устройств, сформированный на основе событий Контроля устройств в Kaspersky Security Center. Вы можете сформировать этот список в свойствах политики в Консоли администрирования.

В Консоли администрирования вы также можете экспортировать настроенный список доверенных устройств в файл и импортировать список устройств из файла.

- Настраивать расписание доступа для устройств хранения данных (жесткие диски, съемные диски, дискеты, CD/DVD-приводы).

  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.

- Настраивать правила доступа к устройствам в зависимости от их типа. Вы можете разрешать или запрещать доступ для указанных пользователей в указанное время.
- Разрешать пользователю запрашивать временный доступ к заблокированному устройству и предоставлять пользователю доступ к устройству.

  Предоставление доступа к заблокированному устройству доступно, только если в организации развернуто приложение Kaspersky Security Center 16.2 и клиентское устройство имеет возможность установить связь с Сервером администрирования.

Настройка контроля устройств в Web Console

В Web Console вы можете настраивать параметры контроля устройств в свойствах политики (**Параметры приложения** → **Контроль безопасности** → **Контроль устройств**).

Настройка контроля устройств в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры контроля устройств в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.

Параметр	Описание
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.
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.

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. • **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 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, 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.

Настройка шаблона 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.

Чтобы изменить шаблон сообщения в Web Console:

1. В окне свойств политики выберите **Параметры приложения** → **Контроль безопасности** → **Контроль устройств**.

2. В блоке **Шаблоны сообщений** нажмите на ссылку **Сообщения о блокировке устройства**.

3. В открывшемся окне **Шаблоны сообщений** настройте шаблон сообщения Контроля устройств на закладке **Сообщение пользователю**.

   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**.

   Также вы можете восстановить текст шаблона сообщения, нажав на кнопку **Восстановить по умолчанию**.

4. Нажмите на кнопку **OK**.

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

Чтобы 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 закладку **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 закладке **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**.

Настройка Контроля устройств в командной строке

В командной строке вы можете управлять контролем устройств с помощью предустановленной задачи Контроль устройств (*Device_Control*).

Задача Контроль устройств по умолчанию не запущена. Вы можете запускать и останавливать задачу вручную.

Вы можете настраивать параметры контроля устройств, изменяя параметры предустановленной задачи Контроль устройств.

С помощью команд управления Контролем устройств вы также можете:

- просматривать и экспортировать в файл список подключенных устройств;
- просматривать и изменять список доверенных устройств.

Параметры задачи Контроль устройств

В таблице описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Контроль устройств.

Параметры задачи Контроль устройств

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.

Параметр	Описание	Значения
`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.
`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.

Параметр	Описание	Значения
`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.
`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.

Параметр	Описание	Значения
`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.
`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=< идентификатор нужного устройства >` *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.		

Параметр	Описание	Значения
`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. `<имя пользователя>` – 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>`), для которого устройство будет доверенным. `@<название группы>` – 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.

`DaysHours`	Интервалы времени для расписания.	`All` (значение по умолчанию) – расписание действует 24/7 (без ограничений по времени).
		
		`<день недели>` – 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.
		
		`<час>` – часы [0:24]. Для часов можно указывать только интервалы.
		
		Примеры:
		Расписание schedule_1, действующее 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`
		Расписание schedule_2, действующее 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`
		Расписание schedule_3, действующее 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. `<имя пользователя>` – 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>`), для которого применяется правило доступа. `@<название группы>` – название группы пользователей (локальной или доменной), для которых применяется правило доступа.

Параметр	Описание	Значения
`[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. `<имя пользователя>` – 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>`), для которого применяется правило доступа. `@<название группы>` – название группы пользователей (локальной или доменной), 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`.
`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. `<имя пользователя>` – 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>`), для которого применяется правило доступа. `@<название группы>` – название группы пользователей (локальной или доменной), 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`.

Параметр	Описание	Значения
`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. `<имя пользователя>` – 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>`), для которого применяется правило доступа. `@<название группы>` – название группы пользователей (локальной или доменной), 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.

Просмотр и экспорт списка подключенных устройств в командной строке

Чтобы просмотреть список подключенных устройств, выполните следующую команду:

```
kesl-control --get-device-list [--all] [--json]
```

где:

- `--all` – выводить список всех подключенных устройств.
- `--json` – выводить список подключенных устройств в формате JSON.

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.

Чтобы экспортировать список подключенных устройств, выполните следующую команду:

```
kesl-control --get-device-list --export <файл>
```

где `<файл>` – полный путь к файлу в формате JSON, в который будет сохранен список подключенных устройств.

Экспорт выполняется в формате списка доверенных устройств.

Управление 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.

Чтобы просмотреть список доверенных устройств, выполните следующую команду:

```
kesl-control --trusted-devices --list
```

Чтобы добавить устройство в список доверенных устройств, выполните следующую команду:

```
kesl-control --trusted-devices --add <идентификатор>
```

где `<идентификатор>` – идентификатор устройства или маска идентификатора устройства.

Чтобы удалить устройство из списка доверенных устройств, выполните следующую команду:

```
kesl-control --trusted-devices --delete <идентификатор>
```

где `<идентификатор>` – идентификатор устройства или маска идентификатора устройства.

Чтобы импортировать список доверенных устройств из файла, выполните следующую команду:

```
kesl-control --trusted-devices --merge|--add|--replace --file <файл>
```

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 <файл>` – полный путь к файлу в формате JSON, из которого будет импортирован список доверенных устройств.

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.

Предоставление доступа к устройству в Web Console

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.

При получении от пользователя запроса на временный доступ к устройству администратор может создать ключ доступа из файла запроса в Web Console.

Для предоставления временного доступа к устройству администратор должен иметь права на чтение, запись и выполнение для функции **Шифрование данных** (**Пользователи и роли** → **Роли** → <роль пользователя> → окно свойств роли пользователя → закладка **Права доступа** → <название приложения> → **Шифрование данных** → **Чтение/Запись/Выполнение**).

Чтобы создать ключ доступа к заблокированному устройству:

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.

Получение временного доступа к устройству 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 `kesl-control --request-temporary-device-access`.

Чтобы запросить временный доступ к заблокированному устройству, выполните следующую команду:

```
kesl-control --request-temporary-device-access --device-id <идентификатор устройства>
--access-duration <длительность доступа> --path <путь к файлу запроса доступа>
```

где:

`--device-id <идентификатор устройства>` – идентификатор заблокированного устройства, к которому вы хотите получить доступ.

`--access-duration <длительность доступа>` – период времени, на который вы хотите получить доступ к устройству (в часах). Возможные значения: 1–100.

`--path <путь к файлу запроса доступа>` – 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 с помощью команды `kesl-control --upload-temporary-device-access-key`, чтобы получить временный доступ к устройству.

Чтобы получить временный доступ к заблокированному устройству, выполните следующую команду:

```
kesl-control --upload-temporary-device-access-key --path <путь к файлу с ключом
доступа>
```

где:

`--path <путь к файлу с ключом доступа>` – 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.

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 сайт, доступ к которому ограничен Веб-Контролем, приложение Kaspersky Endpoint Security блокирует доступ или показывает сообщение-предупреждение о том, что сайт не рекомендован для посещения.

Kaspersky Endpoint Security контролирует только HTTP- и HTTPS-трафик.

Веб-Контроль позволяет настраивать доступ к сайтам следующими способами:

- По категориям содержания. Категоризацию содержания сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных сайтов (входит в состав баз приложения). Вы можете ограничить доступ пользователей, например, к категории содержания "Социальные сети" или другим категориям.

- По категориям типов данных. Вы можете ограничить доступ пользователей к данным на сайте и, например, скрыть графические изображения. Приложение определяет тип данных по формату файла, а не по расширению.

  > Приложение не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, приложение определит тип данных "Архивы", а не "Графические файлы".

- По веб-адресу. Вы можете указать адрес или маску адреса.

Вы можете использовать одновременно несколько способов регулирования доступа к сайтам. Например, вы можете ограничить доступ к категории типов данных "Файлы офисных приложений" только для категории содержания "Веб-почта".

По умолчанию для всех веб-ресурсов выбрано *правило по умолчанию* **Разрешать**. В соответствии с этим правилом Веб-Контроль разрешает пользователям доступ к веб-ресурсам, если не заданы другие *правила доступа к веб-ресурсам*.

Вы можете изменить для Веб-Контроля правило по умолчанию, согласно которому приложение будет регулировать доступ к веб-ресурсам, которые не попадают под действие других правил, и задать *правило по умолчанию* **Блокировать**. В соответствии с этим правилом Веб-Контроль запрещает пользователям доступ к веб-ресурсам, если не заданы другие *правила доступа к веб-ресурсам*.

> Если вы настроили исключения из перехвата трафика приложением Kaspersky Endpoint Security, они влияют на работу компонента Веб-Контроль.

О правилах доступа к веб-ресурсам

Правило доступа к веб-ресурсам представляет собой набор фильтров и действие, которое приложение выполняет при посещении пользователями описанных в правиле веб-ресурсов в указанное в расписании работы правила время. Фильтры позволяют задать веб-ресурсы, доступ к которым контролирует компонент Веб-Контроль.

Доступны следующие фильтры:

- **Фильтр по категориям содержания**. Веб-Контроль может распределять веб-ресурсы по категориям содержания. Вы можете контролировать доступ пользователей к веб-ресурсам, имеющим определенное этими категориями содержание. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории содержания, приложение выполняет действие, указанное в правиле.

- **Фильтр по категориям типов данных**. Веб-Контроль может распределять веб-ресурсы по категориям типов данных. Вы можете контролировать доступ пользователей к размещенным на веб-ресурсах данным, относящимся к определенным типам данных. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории типов данных, приложение выполняет действие, указанное в правиле.

- **Фильтр по адресам веб-ресурсов**. Вы можете контролировать доступ пользователей ко всем адресам веб-ресурсов или к отдельным адресам веб-ресурсов и/или группам адресов веб-ресурсов.

  Если задан и фильтр по категориям содержания и/или по категориям типов данных, и фильтр по адресам веб-ресурсов, и заданные адреса веб-ресурсов и/или группы адресов веб-ресурсов принадлежат к выбранным категориям содержания или категориям типов данных, приложение контролирует доступ не ко всем веб-ресурсам выбранных категорий содержания и/или категорий типов данных, а только к заданным адресам веб-ресурсов и/или группам адресов веб-ресурсов.

- **Фильтр по именам пользователей и групп пользователей**. Вы можете задавать пользователей и/или группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом. Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

- **Расписание работы правила**. Вы можете задавать расписание работы правила. Расписание работы правила определяет время, когда приложение контролирует доступ к веб-ресурсам, указанным в правиле. Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Для каждого правила вы можете задать действие, которое Веб-Контроль выполняет при посещении пользователем веб-ресурса, удовлетворяющего параметрам 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-жалобу администратору локальной сети организации об ошибочной блокировке и получить доступ к запрошенному веб-ресурсу.

- *Информировать*. Веб-Контроль выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может отправить сообщение-жалобу администратору локальной сети организации об ошибочном предупреждении. При этом доступ пользователя к веб-ресурсу не блокируется.

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к этому сайту по правилу 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 содержания "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.

Если не создано ни одного запрещающего правила, расшифровка HTTPS-трафика не выполняется.

Настройка Веб-Контроля в Web Console

В Web Console вы можете настраивать параметры Веб-Контроля в свойствах политики (**Параметры приложения** → **Контроль безопасности** → **Веб-Контроль**).

Настройка Веб-Контроля в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры Веб-Контроля в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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**.
	При нажатии на кнопку **Вниз** выбранный элемент перемещается вниз в таблице.
	Кнопка доступна, если в таблице выбран только один элемент.
	При нажатии на кнопку **Вверх** выбранный элемент перемещается вверх в таблице.
	Кнопка доступна, если в таблице выбран только один элемент.
	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.

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.
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).

Настройка шаблонов сообщений Веб-Контроля

В зависимости от действия, заданного в свойствах правил Веб-Контроля, при попытке пользователя получить доступ к веб-ресурсам приложение выводит сообщение (подменяет ответ HTTP-сервера HTML-страницей с сообщением) одного из следующих типов:

- Сообщение-предупреждение. Такое сообщение предупреждает пользователя о том, что посещение веб-ресурса не рекомендуется и/или не соответствует корпоративной политике безопасности. Приложение выводит сообщение-предупреждение, если в параметрах правила, описывающего этот веб-ресурс, выбрано действие **Информировать**.

  Если, по мнению пользователя, предупреждение ошибочно, по ссылке из предупреждения пользователь может отправить уже сформированное сообщение-жалобу администратору локальной сети организации.

- Сообщение о блокировке веб-ресурса. Приложение выводит сообщение о блокировке веб-ресурса, если в параметрах правила, которое описывает этот веб-ресурс, выбрано действие **Блокировать**.

  Если, по мнению пользователя, блокировка доступа к веб-ресурсу была ошибочна, по ссылке из сообщения о блокировке веб-ресурса пользователь может отправить уже сформированное сообщение-жалобу администратору локальной сети организации.

Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и сообщения-жалобы для отправки администратору локальной сети организации предусмотрены шаблоны. Вы можете изменять их содержание.

Чтобы изменить шаблон сообщения в Web Console:

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

   Откроется список политик.

2. Выберите группу администрирования, содержащую устройства, на которых применяется политика. Для этого нажмите на ссылку в поле Текущий путь в верхней части окна и выберите группу администрирования в открывшемся окне.

   В списке отобразятся политики, настроенные для выбранной группы администрирования.

3. Нажмите на название нужной политики в списке.

   Откроется окно свойств политики.

4. В окне свойств политики выберите **Параметры приложения** → **Контроль безопасности** → **Веб-Контроль**.

5. В блоке **Шаблоны сообщений** настройте шаблоны сообщений Веб-Контроля на следующих закладках:

   - **Предупреждение**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу.

   - **Сообщение о блокировке**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу.

   - **Сообщение администратору**. Поле ввода содержит шаблон сообщения-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. 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 закладках **Предупреждение и Сообщение о блокировке** вы можете добавлять переменные и ссылки в тексты сообщений для пользователя, используя кнопки **Добавить переменную** и **Добавить ссылку**.

   Вы можете восстановить текст шаблона сообщения, нажав на кнопку **Восстановить по умолчанию**.

6. Нажмите на кнопку **ОК**.

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

Чтобы 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 закладку **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 → Веб-Контроль**.
5. В блоке **Шаблоны сообщений** нажмите на кнопку **Настроить**.
6. В открывшемся окне **Шаблоны сообщений** настройте шаблоны сообщений Веб-Контроля на следующих закладках:

   - **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 закладках **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 **ОК**.
8. Нажмите на кнопку **Применить**.

Настройка Веб-Контроля в командной строке

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.

Параметры задачи Веб-Контроль

В таблице ниже описаны все доступные значения и значения по умолчанию для всех параметров, которые вы можете указать для задачи Веб-Контроль.

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.

Параметр	Описание	Значения
`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.	–
`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, GenerativeAITools`
`[Rules.item_#.FormatCategories.item_#]`	Секция для указания категории типов данных.	–
`FormatCategories.item_#.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.	`< имя пользователя >` – имя пользователя, для которого применяется правило. `@< название группы >` – 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:		

Параметр	Описание	Значения
`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.
`Name`	Название расписания.	
`DaysHours`	Интервалы времени для расписания.	`< день недели >` – 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. `< час >` – 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 <путь к конфигурационному файлу>] [--json]
```

где:

`--file <путь к конфигурационному файлу>` – 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 <путь к конфигурационному файлу>] [--json]
```

где:

`--file <путь к конфигурационному файлу>` – 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
```

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 целостности системы

Приложение Kaspersky Endpoint Security позволяет контролировать целостность операционной системы защищаемого устройства в режиме реального времени и по требованию.

- Компонент *Контроль целостности системы* позволяет в реальном времени отслеживать изменения в файлах и директориях, которые вы включили в область мониторинга в параметрах компонента. Вы можете отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве.

- С помощью задач *Проверка целостности системы* вы можете проверять наличие изменений в файлах и директориях, которые вы включили в область мониторинга, путем сравнения текущего состояния контролируемого объекта с ранее зафиксированным состоянием.

Для использования функциональности контроля целостности системы требуется лицензия, которая включает эту функцию.

Обнаружив изменения файлов и директорий из области мониторинга, приложение Kaspersky Endpoint Security формирует события об изменениях в списках контроля доступа к объектам. 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.

Контроль целостности системы в реальном времени

Компонент Контроль целостности системы позволяет определять каждое изменение объекта, включенного в область мониторинга, путем перехвата файловых операций в режиме реального времени.

Во время работы компонента Контроль целостности системы приложение контролирует изменение следующих параметров файлов:

- содержимое (write (), truncate (), etc.);

- метаданные (правообладание (chmod/chown));

- отметки времени (utimensat);

- расширенные атрибуты (setxattr) и другие.

Контрольная сумма файла не рассчитывается.

Технологические ограничения операционной системы Linux не позволяют приложению определять, какой пользователь или процесс внес изменение в файл.

По умолчанию Контроль целостности системы выключен. Вы можете включать и выключать Контроль целостности системы, а также настраивать параметры работы компонента:

- Настраивать области мониторинга для контроля целостности системы. Приложение отслеживает операции с файлами в областях мониторинга, указанных в параметрах компонента Контроль целостности системы. Для работы компонента требуется указать хотя бы одну область мониторинга. По умолчанию задана область мониторинга *Внутренние объекты "Лаборатории Касперского"* (/opt/kaspersky/kesl/).

  Вы можете указать несколько областей мониторинга. Вы можете изменять области мониторинга в режиме реального времени.

  > Приложение не отслеживает изменения файлов (атрибутов и содержимого) с жесткими ссылками, которые расположены вне области мониторинга.

- Настраивать исключение объектов из мониторинга по маске имени.

- Настраивать области исключения для контроля целостности системы. Исключения задаются для каждой отдельной области мониторинга и работают только для указанной области. Вы можете указать несколько областей исключения из мониторинга.

  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.

> При добавлении директории в область мониторинга или в область исключения приложение не проверяет, существует ли такая директория.

Настройка контроля целостности системы в Web Console

В Web Console вы можете настраивать параметры контроля целостности системы в свойствах политики (**Параметры приложения** → **Контроль безопасности** → **Контроль целостности системы**).

Настройка контроля целостности системы в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры контроля целостности системы в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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**.

Параметр	Описание
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.

Параметр	Описание
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.

Настройка контроля целостности системы в командной строке

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.

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.
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**. 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. 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.

Параметр	Описание	Значения
`Path`	Путь к директории с объектами, исключаемыми из мониторинга.	Для указания пути вы можете использовать **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. 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).

Проверка целостности системы

Во время выполнения задачи *Проверка целостности системы* изменение каждого объекта определяется путем сравнения текущего состояния контролируемого объекта с исходным состоянием. Сравнение может выполняться по следующим критериям:

- хеш файла;
- время изменения файла;
- размер файла.

Исходное состояние контролируемых объектов фиксируется в качестве *снимка состояния системы*. Снимок состояния системы содержит пути к контролируемым объектам и их метаданные.

Снимок состояния системы может содержать персональные данные.

Снимок состояния системы создается во время первого выполнения задачи проверки целостности системы на устройстве. Если вы создали несколько задач проверки целостности системы, для каждой задачи создается отдельный снимок состояния системы. Задача выполняется, только если снимок состояния системы содержит информацию об объектах, которые относятся к области мониторинга, настроенной для задачи. Если снимок состояния системы не соответствует области мониторинга, приложение Kaspersky Endpoint Security формирует событие о нарушении целостности системы.

Снимок состояния системы обновляется при изменении параметров задачи (например, при добавлении новой области мониторинга), а также при запуске задачи с параметром `RebuildBaseline=Yes` (или установленном флажке **Обновлять снимок состояния системы при каждом запуске задачи** в свойствах задачи в Kaspersky Security Center).

Приложение создает хранилище для снимков состояния системы на защищаемом устройстве. По умолчанию 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.

Вы можете удалить снимок состояния системы, удалив соответствующую задачу проверки целостности системы.

Вы можете запускать проверку целостности системы по требованию и настраивать параметры проверки:

- Включать и выключать обновление снимка состояния системы каждый раз после завершения задачи проверки целостности системы.
- Выбирать критерии, по которым выполняется сравнение текущего состояния контролируемого файла с исходным состоянием: использовать хеш и время изменения файла или только размер файла.
- Настраивать области мониторинга для проверки целостности системы.
- Настраивать области исключения из проверки целостности системы. Вы можете указывать пути к исключаемым файлам и директориям и исключать отдельные объекты по маске имени.

Проверка целостности системы в Web Console

В Web Console 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.

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 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.

Параметр	Описание
Области мониторинга	Таблица, содержащая области мониторинга, проверяемые задачей. По умолчанию таблица содержит область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kesl/). Области мониторинга в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз. Вы также можете импортировать список областей мониторинга из файла по кнопке **Импортировать** и экспортировать список областей мониторинга в файл в формате JSON по кнопке **Экспортировать**. При импорте вам будет предложено заменить список областей мониторинга или добавить области мониторинга к уже существующему списку.

Окно добавления области проверки

В этом окне вы можете добавить или настроить область мониторинга для задачи Проверка целостности системы.

Параметры области мониторинга

Параметр	Описание
Название области	Поле ввода названия области мониторинга. Это название будет отображаться в таблице раздела **Параметры 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**. 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. Поле не должно быть пустым. По умолчанию указан путь **/** – приложение проверяет все директории локальной файловой системы.
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.

Раздел Области исключения

В разделе **Области исключения** для задачи Проверка целостности системы вы можете настроить области исключения из проверки и исключения по маске.

Окно Области исключения

Таблица содержит области исключения из мониторинга 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 мониторинга

Параметр	Описание
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 задачи.

Элементы в таблице можно добавлять, изменять и удалять.

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.

Окно добавления области 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**. 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. 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.

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).

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

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.

Параметр	Описание
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.

Параметр	Описание
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**. 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. 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.

Раздел Области 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**. 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. 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).

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).

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 командной строке

В командной строке вы можете выполнять проверку целостности системы на устройстве с помощью пользовательских задач *Проверка целостности системы* (задач типа *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**. 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. 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.

Параметр	Описание	Значения
`Path`	Путь к директории с объектами, исключаемыми из мониторинга.	Для указания пути вы можете использовать **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. 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).

Анализ поведения

Компонент Анализ поведения позволяет контролировать вредоносную активность приложений в операционной системе. При обнаружении вредоносной активности приложение Kaspersky Endpoint Security может завершать процесс приложения, осуществляющего вредоносную активность.

Компонент Анализ поведения включается автоматически с параметрами по умолчанию при запуске приложения Kaspersky Endpoint Security.

Для оптимальной работы компонента Анализ поведения рекомендуется включить компонент Защита от веб-угроз.

Вы можете включать и выключать Анализ поведения, а также настраивать параметры работы компонента:

- Выбирать действие, которое Kaspersky Endpoint Security будет выполнять при обнаружении вредоносной активности в операционной системе: информировать пользователя или блокировать приложение, осуществляющее вредоносную активность.
- Исключать активность процессов из проверки компонентом Анализ поведения и компонентами MDR и EDR Expert (on-premise).

  Приложение автоматически исключает из проверки активность процесса Watchdog-сервера. Это исключение удалить нельзя.

По умолчанию на операционной системе СинтезМ-Клиент конфигурация службы auditd 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.

Если у пользователя с root-правами отсутствует доступ к файлу на удаленной директории, смонтированной на устройстве по протоколу NFSv4, приложение блокирует доступ к файлу для всех пользователей.

Настройка анализа поведения в Web Console

В Web Console вы можете настраивать параметры анализа поведения приложений в свойствах политики (**Параметры приложения** → **Защита устройств от угроз** → **Защита на основе анализа поведения** → **Анализ поведения**).

Настройка анализа поведения в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры анализа поведения приложений в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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**. 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. Поле ввода не должно быть пустым.
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-premise)	Флажок включает или выключает исключение процесса из телеметрии, которую собирают компоненты MDR и EDR Expert (on-premise). По умолчанию флажок снят.

Настройка анализа поведения в командной строке

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.
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**. 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.
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.
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-premise).	Yes – исключать активность указанного процесса из телеметрии, которую собирают компоненты MDR и EDR Expert (on-premise). No (значение по умолчанию) – не исключать активность указанного процесса из телеметрии.

Параметр	Описание	Значения
`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`		`True` (значение по умолчанию) – приложение Kaspersky Endpoint Security использует службу auditd в монопольном режиме. `False` – служба auditd используется в режиме многоадресной рассылки.

Защита от эксплойтов

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на устройстве для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимое приложение. При обработке этих данных уязвимое приложение выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО. Если попытка запустить исполняемый файл из уязвимого приложения не была произведена пользователем, приложение Kaspersky Endpoint Security блокирует запуск этого файла или информирует пользователя. По умолчанию Защита от эксплойтов выключена.

Для работы компонента Защита от эксплойтов требуется включить компонент Анализ поведения и использование обновляемого модуля ядра. Для оптимальной работы компонента Защита от эксплойтов рекомендуется также включить компонент Защита от веб-угроз.

Вы можете включать и выключать Защиту от эксплойтов, а также настраивать параметры работы компонента:

- Выбирать действие, которое приложение будет выполнять при обнаружении эксплойта.
- Настраивать исключения объектов из проверки. Исключение из проверки – это совокупность условий, при выполнении которых приложение не проверяет объекты на наличие вирусов и других вредоносных программ. Вы можете исключать из проверки:
  - объекты по названиям обнаруженных в объектах угроз;
  - файлы и директории, расположенные по указанным путям;
  - файлы с указанной хеш-суммой.

Настройка защиты от эксплойтов в Web Console

В Web Console вы можете настраивать параметры защиты от эксплойтов в свойствах политики (**Параметры приложения → Защита устройств от угроз → Защита на основе анализа поведения → Защита от эксплойтов**).

Настройка защиты от эксплойтов в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры защиты от эксплойтов в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.
Блок **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.

Параметр	Описание
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**.
Комментарий	Поле ввода комментария (необязательное).
Использовать это исключение	Флажок включает или выключает использование этого исключения во время работы приложения. По умолчанию флажок установлен.

Настройка защиты от эксплойтов в командной строке

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.
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.

Параметр	Описание	Значения
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

Функциональность KSN может быть недоступна в приложении на территории США.

Для повышения эффективности защиты устройств и данных пользователей приложение Kaspersky Endpoint Security может использовать облачную базу знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения – Kaspersky Security Network (KSN). Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции на различные угрозы, высокую производительность компонентов защиты и снижение количества ложных срабатываний.

Использование Kaspersky Security Network является добровольным. Вы можете включить или выключить использование KSN в любой момент.

Инфраструктурные решения Kaspersky Security Network

Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения для работы с репутационными базами "Лаборатории Касперского":

- *Kaspersky Security Network (KSN)* – это решение, которое позволяет получать информацию от "Лаборатории Касперского", а также отправлять в "Лабораторию Касперского" данные об объектах, обнаруженных на устройствах пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.

- *Kaspersky Private Security Network (KPSN)* – это решение, которое позволяет пользователям устройств с установленным приложением Kaspersky Endpoint Security получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих устройств. KPSN разработан для корпоративных клиентов, не имеющих возможности использовать Kaspersky Security Network, например, по следующим причинам:

  - отсутствие подключения локальных рабочих мест к интернету;

  - 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.

Варианты использования Kaspersky Security Network

Существует два варианта использования KSN:

- **Расширенный режим KSN** – вы можете получать информацию из базы знаний "Лаборатории Касперского", при этом приложение Kaspersky Endpoint Security автоматически отправляет в Kaspersky Security Network статистическую информацию, полученную в результате своей работы. Также приложение может отправлять в "Лабораторию Касперского" для дополнительной проверки файлы (или части файлов), которые злоумышленники могут использовать для нанесения вреда устройству или данным.

- **Стандартный режим KSN** – вы можете получать информацию из базы знаний "Лаборатории Касперского", при этом приложение Kaspersky Endpoint Security не отправляет анонимную статистику и данные о типах и источниках угроз.

Вы можете выбрать вариант использования Kaspersky Security Network с помощью Web Console, Консоли администрирования или командной строки.

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.

Облачный режим работы Kaspersky Endpoint Security

Облачный режим – это режим работы приложения Kaspersky Endpoint Security, при котором используется облегченная версия баз вредоносного ПО. Это позволяет снизить нагрузку на оперативную память устройства.

Работу приложения с облегченными базами вредоносного ПО обеспечивает Kaspersky Security Network.

Если приложение Kaspersky Endpoint Security используется в стандартном режиме и вы используете KSN в работе приложения, вы можете включать облачный режим работы приложения.

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.

Kaspersky Endpoint Security переходит к использованию облегченной версии баз вредоносного ПО после включения облачного режима и выполнения очередного обновления баз и модулей приложения. Если облачный режим выключается, Kaspersky Endpoint Security загружает полную версию баз приложения с серверов "Лаборатории Касперского" в ходе очередного обновления баз и модулей приложения.

Если вы не используете KSN или облачный режим выключен, Kaspersky Endpoint Security использует полную версию баз приложения.

Облачный режим выключается автоматически, если выключено использование KSN.

Использование службы прокси-сервера KSN

Устройства пользователей, работающие под управлением Сервера администрирования, могут взаимодействовать с KSN напрямую или при помощи службы прокси-сервера KSN на Сервере администрирования.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, взаимодействие с инфраструктурой KSN обеспечивает служба прокси-сервера KSN. Взаимодействие с KSN напрямую не поддерживается. Если прокси-сервер KSN недоступен, KSN не используется в работе приложения.

Прокси-сервер KSN предоставляет следующие возможности:

- Устройство пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение устройством пользователя запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в свойствах Сервера администрирования. Подробнее о прокси-сервере KSN см. в справке Kaspersky Security Center.

Если приложение Kaspersky Endpoint Security используется в стандартном режиме, вы можете настраивать параметры использования прокси-сервера KSN в работе приложения с помощью Web Console или Консоли администрирования Kaspersky Security Center.

Настройка параметров прокси-сервера KSN с помощью командной строки недоступна.

В Kaspersky Security Center вы можете настраивать следующие параметры использования прокси-сервера KSN приложением Kaspersky Endpoint Security:

- включать и выключать использование Сервера администрирования в качестве прокси-сервера KSN;
- разрешать или запрещать взаимодействие с серверами KSN напрямую, если служба прокси-сервера KSN недоступна.

Настройка использования Kaspersky Security Network в Web Console

В Web Console вы можете настраивать параметры использования Kaspersky Security Network в работе приложения в свойствах политики (**Параметры приложения** → **Общие настройки** → **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 закладке **Активы (Устройства)**.

Настройка использования Kaspersky Security Network в Консоли администрирования

В Консоли администрирования вы можете настраивать использование Kaspersky Security Network в работе приложения Kaspersky Endpoint Security в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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 закладке **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	Флажок включает или выключает режим работы, при котором приложение Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО. 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 для защиты виртуальных сред приложение может взаимодействовать с инфраструктурой KSN только с помощью прокси-сервера KSN.
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.

Настройка использования Kaspersky Security Network в командной строке

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 <путь к конфигурационному файлу> [--json] [--accept-ksn]
```

где:

- `--file <путь к конфигурационному файлу>` – 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`.

Проверка подключения к Kaspersky Security Network с помощью командной строки

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 `Выключен`, 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": `Kaspersky Security Network` или `Kaspersky Private Security Network`.

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 с помощью командной строки

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.

Дополнительные параметры работы приложения

Вы можете настраивать следующие дополнительные параметры работы приложения:

- Использование прокси-сервера в работе приложения.
- Глобальные исключения – исключение точек монтирования из перехвата файловых операций для компонентов Защита от файловых угроз, Защита от шифрования, Мониторинг контейнеров и задач Поиск вредоносного ПО, Проверка важных областей, Проверка контейнеров и Проверка съемных дисков.
- Исключение памяти процессов из проверки.
- Режим перехвата файловых операций.
- Обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.
- Отслеживание стабильности работы приложения.
- Параметры запуска приложения.
- Ограничение на использование памяти и ресурсов процессора для задач проверки.
- Ограничение на использование резидентной памяти приложением.
- Ограничение на количество задач выборочной проверки, которые может одновременно запустить непривилегированный пользователь.
- Параметры отправки информации в хранилище Kaspersky Security Center.
- Разрешения на управление задачами.
- Отмена запуска запланированных задач на устройстве, работающем от аккумулятора.
- Параметры перехвата системных событий.
- Дополнительные параметры телеметрии.

Настройка 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". Вы можете включить использование Сервера администрирования в качестве прокси-сервера для доступа к серверам активации в Web Console или в Консоли администрирования.

Вы можете настраивать следующие исключения при использовании прокси-сервера в Web Console, в Консоли администрирования или в командной строке:

- Для компонентов EDR Expert (on-premise), NDR (KATA) и Sandbox, которые обеспечивают интеграцию с решениями Detection and Response. Вы можете указать компоненты, в работе которых не будет использоваться прокси-сервер.

- Для веб-адресов. Вы можете сформировать список адресов, для подключения к которым не будет использоваться прокси-сервер.

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 не поддерживается использование Сервера администрирования Kaspersky Security Center в качестве прокси-сервера для доступа к серверам активации "Лаборатории Касперского".

Настройка параметров прокси-сервера в Web Console

В Web Console вы можете настраивать параметры использования прокси-сервера в свойствах политики (**Параметры приложения** → **Общие настройки** → **Настройки сети**).

Настройка параметров прокси-сервера в Консоли администрирования

В Консоли администрирования вы можете настраивать использование прокси-сервера в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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 для защиты виртуальных сред, 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-premise)** – не использовать прокси-сервер при подключении к серверам, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise) 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**, **удалять** адреса в таблице. 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.

Настройка параметров прокси-сервера в командной строке

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 `<протокол подключения>://[<пользователь>[:<пароль>]@]<адрес прокси-сервера>:<номер порта>`, где:

- `<пользователь>` – имя пользователя для аутентификации на прокси-сервере.
- `<пароль>` – пароль пользователя для авторизации на прокси-сервере.
- `<адрес прокси-сервера>` – IP-адрес или доменное имя прокси-сервера.
- `<номер порта>` – 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 `<адрес>[:<номер порта>]`. 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-premise), 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-premise) 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 глобальных исключений

Вы можете настраивать исключение точек монтирования из перехвата файловых операций для компонентов Защита от файловых угроз и Защита от шифрования, а также из проверки задачами Поиск вредоносного ПО, Проверка важных областей и Проверка контейнеров. Исключение точек монтирования позволяет исключать из перехвата файловых операций локальные или удаленные директории, смонтированные на устройстве. Кроме того, глобальные исключения влияют на работу компонента Мониторинг контейнеров (Проверка контейнеров, Мониторинг контейнеров) и задачи Проверка съемных дисков.

Настройка глобальных исключений в Web Console

В Web Console вы можете настраивать глобальные исключения в свойствах политики (**Параметры приложения** → **Доверенная зона** → **Точки монтирования**).

Настройка глобальных исключений в Консоли администрирования

В Консоли администрирования вы можете настраивать глобальные исключения в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.
	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**. 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. Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек). Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории. 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**.

Настройка глобальных исключений в командной строке

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:<тип файловой системы>` – 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.
- `<путь, содержащий маску /mnt/user* или /mnt/**/user_share>` – исключать из перехвата объекты, находящиеся в точках монтирования, имена которых содержат указанную **маску**.

  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.

  Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек).

  Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`.

  Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

> 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.

Исключение памяти процессов из проверки

Вы можете настраивать исключения из проверки памяти процессов. Приложение не будет проверять память указанных процессов.

Настройка исключений в Web Console

В Web Console вы можете настраивать исключения памяти процессов из проверки в свойствах политики (**Параметры приложения** → **Общие настройки** → **Производительность**).

Настройка исключений в Консоли администрирования

В Консоли администрирования вы можете настраивать исключения памяти процессов из проверки в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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 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.

Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек).

Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`.

Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

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.

Настройка исключений 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 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.

Вы можете указать несколько процессов, память которых требуется исключить из проверки.

Выбор режима перехвата файловых операций

Режим перехвата файловых операций влияет на работу компонентов Защита от файловых угроз и Контроль устройств.

- Приложение может блокировать на время проверки доступ к файлам, которые проверяет компонент Защита от файловых угроз. По умолчанию доступ блокируется: любое обращение к проверяемому файлу ожидает результатов проверки. 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.

  Вы можете выключить блокировку доступа к файлам, которые проверяет компонент Защита от файловых угроз. В этом случае проверка выполняется в асинхронном режиме.

- Приложение может блокировать доступ к файлам на устройстве на время, пока компонент Контроль устройств определяет возможность предоставления доступа к устройству. По умолчанию доступ блокируется: любое обращение к файлам на контролируемом устройстве ожидает результатов проверки. Приложение разрешает доступ к файлам, если в результате проверки Контроль устройств разрешает доступ к устройству с файлами.

  Вы можете выключить блокировку доступа к файлам на устройстве, которое контролирует компонент Контроль устройств. В этом случае Контроль устройств определяет возможность предоставления доступа к устройству в асинхронном режиме.

Если не включен блокирующий режим перехвата файловых операций, компоненты Защита от файловых угроз и Контроль устройств, а также запрет запуска объектов работают в режиме информирования, независимо от установленного режима работы.

Настройка в Web Console

В Web Console вы можете настраивать режим перехвата файловых операций в свойствах политики (**Параметры приложения** → **Общие настройки** → **Настройки обнаружения**).

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать режим перехвата файлов в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры приложения**, блок **Режим перехвата файловых операций**).

Флажок **Блокировать доступ к файлам во время проверки** включает или выключает блокировку доступа к файлам на время проверки компонентами Защита от файловых угроз и Контроль устройств.

По умолчанию флажок установлен.

Если флажок снят, на время проверки обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме.

Настройка в командной строке

В командной строке вы можете настраивать режим перехвата файловых операций с помощью параметра `FileBlockDuringScan` 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 `FileBlockDuringScan` может принимать следующие значения:

- `Yes` (значение по умолчанию) – блокировать доступ к файлам на время проверки компонентами Защита от файловых угроз и Контроль устройств.
- `No` – не блокировать доступ к файлам на время проверки. Обращение к любому файлу разрешается, проверка выполняется 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, если во время проверки этот файл сможет, например, изменить свое имя до принятия приложением решения о статусе этого файла.

Настройка обнаружения приложений, которые злоумышленники могут использовать для нанесения вреда

Вы можете включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным. Такие приложения сами по себе не имеют вредоносных функций, но эти приложения могут быть использованы злоумышленниками. Подробную информацию о легальных приложениях, которые могут быть использованы злоумышленниками для нанесения вреда устройствам или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского".

Настройка в Web Console

В Web Console вы можете настраивать параметры обнаружения легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным, в свойствах политики (**Параметры приложения** → **Общие настройки** → **Настройки обнаружения**).

Настройка в Консоли администрирования

В Консоли администрирования вы можете включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным, в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры приложения**, блок **Параметры проверки**).

Флажок **Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным** включает или выключает обнаружение легальных приложений, через которые злоумышленники могут навредить устройству или данным пользователя.

По умолчанию флажок снят.

Настройка в командной строке

В командной строке вы можете включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным, с помощью параметра `DetectOtherObjects` 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 `DetectOtherObjects` может принимать следующие значения:

- `Yes` – включить обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.
- `No` – не включать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.

Включение мониторинга стабильности работы приложения

Вы можете включать и выключать мониторинг стабильности работы приложения Kaspersky Endpoint Security, который позволяет отслеживать количество нештатных остановок приложения и уведомлять администратора о нестабильной работе приложения, а также настраивать параметры мониторинга.

Настройка в Web Console

В Web Console вы можете включать и выключать мониторинг стабильности работы приложения в свойствах политики (**Параметры приложения** → **Общие настройки** → **Производительность**).

Настройка в Консоли администрирования

В Консоли администрирования вы можете включать и выключать мониторинг стабильности работы приложения в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры приложения**, блок **Дополнительные параметры приложения**).

Флажок **Включить мониторинг стабильности работы приложения** включает или выключает отслеживание состояния работы приложения Kaspersky Endpoint Security.

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>*.

Настройка в командной строке

В командной строке вы можете настраивать параметры мониторинга 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.

Настройка параметров запуска приложения

Вы можете настраивать параметры запуска приложения.

Настройка ограничения в Web Console

В Web Console вы можете настраивать параметры запуска приложения в свойствах политики (**Параметры приложения** → **Общие настройки** → **Взаимодействие с пользователем**).

Настройка ограничения в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры запуска приложения в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.

Настройка ограничения 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.

Ограничение на использование резидентной памяти приложением

Вы можете настраивать ограничение на использование резидентной памяти приложением. По умолчанию установлено автоматическое ограничение.

Настройка ограничения в Web Console

В Web Console вы можете настраивать ограничение на использование резидентной памяти приложением в свойствах политики (**Параметры приложения** → **Общие настройки** → **Производительность**).

Настройка ограничения в Консоли администрирования

В Консоли администрирования вы можете настраивать ограничение на использование резидентной памяти приложением в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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

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.

Настройка ограничения в командной строке

В командной строке вы можете настраивать ограничение на использование резидентной памяти приложением с помощью параметра `MaxMemory` в конфигурационном файле kesl.ini.

Параметр `MaxMemory` может принимать следующие значения:

- `off` – использование резидентной памяти не ограничено.
- `< значение >%` – значение от 1 до 100 в процентах от объема памяти.
- `< значение >MB` – значение в мегабайтах.

- `lowest/< значение >%/< значение >MB` – наименьшее значение между значением в процентах и значением в мегабайтах.
- `highest/< значение >%/< значение >MB` – наибольшее значение между значением в процентах и значением в мегабайтах.
- `auto` – до 50% доступной памяти, но не менее 2 ГБ и не более 16 ГБ.

Значение по умолчанию: `auto`.

Ограничение на использование памяти и ресурсов процессора

Вы можете настраивать ограничение на использование памяти для задач проверки. По умолчанию установлено ограничение 8192 мегабайт.

> Рекомендуется указывать ограничение на использование памяти для задач проверки ниже ограничения на использование резидентной памяти, чтобы избежать использования всей доступной памяти задачами проверки и перезапуска приложения.

Также вы можете настраивать ограничение на использование ресурсов процессора для задач проверки. По умолчанию ограничение не установлено. При настройке ограничения рекомендуется обратить 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, требуется установить значение `15` в качестве ограничения на использование ресурсов процессора. ограничение на использование ресурсов процессора должно быть целым числом и находиться в пределах от 10 до 100. Кроме того, ограничение на использование ресурсов процессора используется не для всех задач приложения, а только для задач *Поиск вредоносного ПО*, *Проверка важных областей*, *Инвентаризация* и *Проверка контейнеров*, поэтому загрузка процессора при ограничении может превышать желаемое значение.

Настройка ограничения в Web Console

В Web Console вы можете настраивать параметры ограничения на использование памяти и ресурсов процессора для задач проверки в свойствах политики (**Параметры приложения** → **Общие настройки** → **Производительность**).

Настройка ограничения в Консоли администрирования

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 (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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

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 (при условии, что максимальная совокупная загрузка всех ядер принимается за 100%). 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.

Настройка ограничения в командной строке

В командной строке вы можете настраивать ограничение на использование ресурсов процессора для задач типа *ODS*, *ContainerScan* и *InventoryScan* с помощью параметров `UseOnDemandCPULimit` и `OnDemandCPULimit` 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.

Параметр `UseOnDemandCPULimit` может принимать следующие значения:

- `Yes` – включить ограничение потребления ресурсов процессора для задач типа *ODS*, *ContainerScan* и *InventoryScan*.
- `No` – выключить ограничение потребления ресурсов процессора для задач.

Параметр `OnDemandCPULimit` позволяет задать максимальное значение нагрузки на все ядра процессора (в процентах) при работе задач типа *ODS*, *ContainerScan* и *InventoryScan*. Значение параметра должно быть целым числом и находиться в пределах от 10 до 100. Значение по умолчанию 100.

В командной строке вы можете настраивать ограничение на использование памяти для задач типа *ODS*, *ContainerScan* и *InventoryScan* с помощью параметра `ScanMemoryLimit` в конфигурационном файле kesl.ini. Значение по умолчанию: 8192.

Ограничение на количество задач выборочной проверки

Вы можете настраивать ограничение на количество задач выборочной проверки, которые может одновременно запустить на устройстве непривилегированный пользователь. Количество задач, которые может запустить пользователь с root-правами, не ограничивается.

Настройка ограничения в Консоли администрирования

В Консоли администрирования вы можете настраивать ограничение на количество задач выборочной проверки, которые может одновременно запустить на устройстве непривилегированный пользователь, в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры приложения**, блок **Производительность**).

По нажатию на кнопку **Настроить** в блоке **Производительность** открывается окно **Параметры производительности задач проверки**, в котором в блоке **Количество задач выборочной проверки** в поле ввода **Максимальное количество задач выборочной проверки** вы можете указать значение от 0 до 100000. Значение по умолчанию: 0. Если задано значение 0, непривилегированный пользователь не может запускать задачи выборочной проверки.

Настройка ограничения в командной строке

В командной строке вы можете настраивать ограничение на количество одновременно запущенных задач выборочной проверки с помощью параметра `LimitNumberOfScanFileTasks` 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 `LimitNumberOfScanFileTasks` может принимать значения от 0 до 100000. Если задано значение 0, непривилегированный пользователь не может запускать задачи выборочной проверки. Значение по умолчанию: 5.

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.

Общий список файлов, помещенных на карантин приложениями "Лаборатории Касперского" на клиентских устройствах, формируется в Kaspersky Security Center и доступен в Web Console (**Операции** → **Хранилища** → **Карантин**) и 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 Web Console (**Операции** → **Хранилища** → **Резервное хранилище**) и в Консоли администрирования (**Дополнительно** → **Хранилища** → **Резервное хранилище**).

Информация о необработанных файлах отображается в списке активных угроз в Web Console (**Операции** → **Хранилища** → **Активные угрозы**) и в Консоли администрирования (**Дополнительно** → **Хранилища** → **Активные угрозы**).

Информация об устройствах, установленных на клиентском устройстве или подключенных к нему, отображается в списке оборудования в Web Console (**Операции** → **Хранилища** → **Оборудование**) и в Консоли администрирования (**Дополнительно** → **Хранилища** → **Оборудование**). Информация передается, если включен компонент Контроль устройств.

Информация о приложениях, обнаруженных на клиентском устройстве, отображается в списке приложений в Web Console (**Операции** → **Приложения сторонних производителей** → **Реестр приложений**) и в Консоли администрирования (**Дополнительно** → **Управление приложениями** → **Реестр приложений**). Информация передается, если включен компонент Контроль приложений.

Включение и выключение отправки информации в Web Console

В Web Console вы можете настраивать параметры интеграции с Сервером администрирования в свойствах политики (**Параметры приложения** → **Общие настройки** → **Интеграция с KSC**, блок **Передача данных на Сервер администрирования**, ссылка **Дополнительные настройки**) и в свойствах управляемого устройства (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → закладка **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → закладка **Параметры приложения** → раздел **Параметры хранилищ**, блок **Параметры передачи данных на Сервер администрирования**).

Параметры передачи данных на Сервер администрирования в свойствах политики в Web Console описаны в Приложении 5.

Параметры передачи данных на Сервер администрирования в свойствах управляемого устройства описаны в таблице ниже.

Параметры передачи данных на Сервер администрирования в свойствах устройства

Параметр	Описание
Уведомлять о файлах резервного хранилища	Флажок включает или выключает передачу на Сервер администрирования информации о файлах в резервном хранилище. По умолчанию флажок снят.
Уведомлять о файлах карантина	Флажок включает или выключает передачу на Сервер администрирования информации о файлах, помещенных на карантин. По умолчанию флажок снят.
Уведомлять о необработанных файлах	Флажок включает или выключает отправку уведомлений о файлах, не обработанных во время проверки, на Сервер администрирования. По умолчанию флажок снят.
Уведомлять 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 снят.
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. По умолчанию флажок снят.

Включение и выключение отправки информации в Консоли администрирования

В Консоли администрирования вы можете включать и выключать отправку информации на Сервер администрирования в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры хранилищ**, блок **Передача данных на Сервер администрирования**) и в свойствах управляемого устройства (**Управляемые устройства** → закладка **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.

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 и изменять 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.

Настройка в Web Console

В Web Console вы можете настраивать параметрами разрешений на просмотр и управление задачами в свойствах политики (**Параметры приложения** → **Общие настройки** → **Взаимодействие с пользователем**).

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать разрешение на просмотр и управление задачами в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.

Отмена запуска задач при работе от аккумулятора

Вы можете включать и выключать отмену запуска запланированных задач на устройстве, работающем от аккумулятора. Отмена запуска задач, для которых настроено расписание запуска, позволяет снизить потребление ресурсов и продлить время работы от аккумулятора.

Если включена отмена запуска запланированных задач и устройство работает от аккумулятора, приложение Kaspersky Endpoint Security отменяет запуск по расписанию следующих задач:

- всех задач проверки (выборочная проверка, проверка контейнеров, выборочная проверка контейнеров, проверка важных областей, поиск вредоносного ПО);
- инвентаризации;
- обновления баз и модулей приложения;
- поиска IOC;
- проверки целостности системы.

Вы можете запускать нужные задачи вручную.

Настройка в Web Console

В Web Console вы можете настраивать отмену запуска запланированных задач в свойствах политики (**Параметры приложения** → **Общие настройки** → **Производительность**).

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать отмену запуска запланированных задач в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры приложения**, блок **Производительность**).

Флажок **Пропускать запланированные задачи при работе от аккумулятора** 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).

Настройка в командной строке

В командной строке вы можете настраивать отмену запуска запланированных задач с помощью параметра `PowerSaveMode` 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 `PowerSaveMode` может принимать следующие значения:

- `Yes` (значение по умолчанию) – пропускать запуск задач, для которых настроено расписание запуска, если устройство работает от аккумулятора.
- `No` – запускать задачи по расписанию независимо от источника питания, к которому подключено устройство (сеть или аккумулятор).

Настройка параметров перехвата системных событий

Для полноценной работы приложение должно использовать перехват системных событий – файловых операций и запуска процессов. Если приложение не использует перехват системных событий, проверка файлов в режиме реального времени не выполняется, уровень защиты устройства снижается.

Если операционная система на устройстве поддерживает технологию fanotify, вы можете выбрать, какой механизм приложение должно использовать для перехвата системных событий:

- Системный механизм перехвата на основе технологии fanotify. Этот механизм используется по умолчанию.
- Механизм перехвата на основе *обновляемого модуля ядра*. Использование обновляемого модуля ядра позволяет оптимизировать перехват файловых операций и перехват запуска процессов приложением Kaspersky Endpoint Security. Обновляемый модуль ядра выполняет перехват файловых операций при открытии, переименовании и изменении файлов. Производительность приложения увеличивается за счет использования кеша файлов и процессов, не нуждающихся в проверке.

  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.

  Обновляемый модуль ядра входит в комплект поставки приложения.

Для операционных систем, не поддерживающих технологию fanotify, выбор механизма перехвата недоступен. Приложение использует для перехвата системных событий специальный модуль ядра для защиты от файловых угроз. Этот модуль автоматически компилируется при запуске Защиты от файловых угроз при наличии необходимых пакетов и утилит компиляции.

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

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).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8).

  > 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 Stream 8.
- Debian GNU/Linux 12.0.
- Red Hat Enterprise Linux 7.4.
- Red Hat Enterprise Linux 8.10.
- SberLinux 8.10.
- SberLinux 9.1.

- SberLinux 9.6.
- SberLinux 9.7.
- SberOS 3.4.
- SberOS 3.5.
- 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 релиз 11.
- Альт Сервер релиз 11.
- Альт Образование 11.
- РЕД ОС 7.3.
- РЕД ОС 8.
- РОСА "Кобальт" 7.9 Рабочая станция.
- РОСА "Кобальт" 7.9 Сервер.
- РОСА "Хром" 12 Рабочая станция.
- РОСА "Хром" 12 Сервер.

32-битные операционные системы и операционные системы для архитектуры Arm 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.

Вы можете проверить соответствие вашего устройства требованиям для установки обновляемого модуля ядра с помощью утилиты Kaspersky ULKM tool.

Если ваша операционная система соответствует требованиям, вы можете выбрать механизм перехвата на основе обновляемого модуля ядра в ходе установки приложения. В результате будет установлен обновляемый модуль ядра. Вы также можете установить обновляемый модуль ядра позже, если 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. Вы можете выбирать механизм перехвата системных событий в **Web Console**, в Консоли администрирования или в **командной строке**.

   В командной строке вы можете настраивать параметры перехвата системных событий с помощью параметров `InterceptorMode`, `InterceptorFallbackStrategy` и `InterceptorApplyStrategy` в общих параметрах приложения.

   > Параметры отображаются и доступны для изменения только на устройствах, где операционная система поддерживает технологию fanotify.

   Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

   Параметр `InterceptorMode` позволяет выбрать механизм перехвата системных событий, который приложение использует в своей работе. Параметр может принимать следующие значения:

   - `UseFanotify` – использовать технологию fanotify для перехвата системных событий.
   - `UseUpdatableKernelModule` – использовать обновляемый модуль ядра для перехвата системных событий.

   Параметр `InterceptorFallbackStrategy` применяется, если выбран обновляемый модуль ядра. Параметр позволяет указать действие, которое приложение выполняет в случае ошибки запуска обновляемого модуля ядра. Параметр может принимать следующие значения:

   - `FallbackToFanotify` – перейти к использованию технологии fanotify для перехвата системных событий в случае ошибки запуска обновляемого модуля ядра.
   - `FallbackToLimitedMode` – не использовать перехват системных событий в случае ошибки запуска обновляемого модуля ядра. Если приложение не использует перехват системных событий, проверка файлов в режиме реального времени не выполняется, уровень защиты устройства снижается.

Параметр `InterceptorApplyStrategy` применяется, если выбран обновляемый модуль ядра. 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:

- `RestartServiceAutomatically` (рекомендованное значение) – 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.

В Web Console вы можете настраивать параметры перехвата системных событий в свойствах политики (**Параметры приложения** → **Общие настройки** → **Настройки взаимодействия с ОС**).

Параметры применяются только на устройствах, где операционная система поддерживает технологию fanotify.

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.

Для корректной работы приложения требуется, чтобы переход к использованию обновляемого модуля ядра выполнялся после автоматического перезапуска приложения.

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.

Вы можете просматривать информацию о состоянии и доступности обновляемого модуля ядра на устройстве:

- В Web Console или в Консоли администрирования с помощью статуса функционального компонента **Обновляемый модуль ядра**.
- В командной строке в выводе команды `kesl-control --app-info`.

Информация о состоянии 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.

Проверка возможности установки обновляемого модуля ядра

Вы можете проверить соответствие вашего устройства требованиям для установки обновляемого модуля ядра с помощью утилиты Kaspersky ULKM tool.

Чтобы запустить утилиту с помощью Kaspersky Security Center 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.

   Как установить Агент администрирования

   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.

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.

   Описание процедуры удаленной установки см. в справке Kaspersky Security Center.

   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.
- *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.

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

"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.

Чтобы выключить "безопасный" режим работы приложения:

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
```

Настройка параметров перехвата в Web Console

В Web Console вы можете настраивать параметры перехвата системных событий в свойствах политики (**Параметры приложения** → **Общие настройки** → **Настройки взаимодействия с ОС**).

Параметры применяются только на устройствах, где операционная система поддерживает технологию fanotify.

Настройка параметров перехвата в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры перехвата системных событий в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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**.

Настройка параметров перехвата в командной строке

В командной строке вы можете настраивать параметры перехвата системных событий с помощью параметров `InterceptorMode`, `InterceptorFallbackStrategy` и `InterceptorApplyStrategy` в общих параметрах приложения.

Параметры отображаются и доступны для изменения только на устройствах, где операционная система поддерживает технологию fanotify.

Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Параметр `InterceptorMode` позволяет выбрать механизм перехвата системных событий, который приложение использует в своей работе. Параметр может принимать следующие значения:

- `UseFanotify` – использовать технологию fanotify для перехвата системных событий.
- `UseUpdatableKernelModule` – использовать обновляемый модуль ядра для перехвата системных событий.

Параметр `InterceptorFallbackStrategy` применяется, если выбран обновляемый модуль ядра. Параметр позволяет указать действие, которое приложение выполняет в случае ошибки запуска обновляемого модуля ядра. Параметр может принимать следующие значения:

- `FallbackToFanotify` – перейти к использованию технологии fanotify для перехвата системных событий в случае ошибки запуска обновляемого модуля ядра.
- `FallbackToLimitedMode` – не использовать перехват системных событий в случае ошибки запуска обновляемого модуля ядра. Если приложение не использует перехват системных событий, проверка файлов в режиме реального времени не выполняется, уровень защиты устройства снижается.

Параметр `InterceptorApplyStrategy` применяется, если выбран обновляемый модуль ядра. 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:

- `RestartServiceAutomatically` (рекомендованное значение) – 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.

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.

Настройка в Web Console

В Web Console вы можете настраивать дополнительные параметры сбора телеметрии в свойствах политики (**Параметры приложения** → **Общие настройки** → **Настройки взаимодействия с ОС**).

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать дополнительные параметры сбора телеметрии в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.

Параметр	Описание
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**.

Настройка 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*).

Вы можете изменять значения параметров с помощью команды `kesl-control --set-settings 20`, используя конфигурационный файл, который содержит все параметры задачи, или используя ключи командной строки в формате `< имя параметра >=< значение параметра >`.

Параметр `TelemetrySource` позволяет указать источник телеметрии. Параметр может принимать следующие значения:

- `Default` (значение по умолчанию) – использовать для сбора телеметрии технологию eBPF и службу auditd.
- `OnlyEBPF` – использовать для сбора телеметрии только технологию eBPF.

Параметр `UseTelemetryMonopolyMode` позволяет указать режим использования службы auditd, если она используется для сбора телеметрии. Параметр может принимать следующие значения:

- `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.

По умолчанию для хранения резервных копий файлов используется директория /var/opt/kaspersky/kesl/common/objects-backup/. В этой директории также хранятся файлы, помещенные на карантин. Вы можете изменять директорию для хранения объектов резервного хранилища и карантина с помощью командной строки.

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.

Вы можете настраивать параметры резервного хранилища на устройстве с помощью политики 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.
- Максимальный размер резервного хранилища. По умолчанию размер резервного хранилища не ограничен.

Путь к директории, в которой хранятся объекты резервного хранилища и карантина (этот параметр настраивается только с помощью командной строки).

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.

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**) и в Web Console (**Операции → Хранилища → Резервное хранилище**). Вы можете просматривать свойства файлов, находящихся в резервных хранилищах на защищенных устройствах, и удалять из него файлы. Kaspersky Security Center не копирует файлы из резервных хранилищ на Сервер администрирования, все файлы размещаются в резервных хранилищах на защищенных устройствах. Восстановление файлов выполняется на защищенном устройстве.

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.

Для выполнения действий с файлами в резервном хранилище в Kaspersky Security Center вам нужно включить передачу данных на Сервер администрирования о файлах резервного хранилища.

Настройка параметров резервного хранилища в Web Console

В Web Console вы можете настраивать параметры резервного хранилища в свойствах политики (**Параметры приложения** → **Общие настройки** → **Отчеты и хранилище**) и в свойствах управляемого устройства (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → закладка **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → закладка **Параметры приложения** → раздел **Параметры хранилищ**).

Параметры резервного хранилища в свойствах политики в Web Console описаны в Приложении 5.

Параметры резервного хранилища в свойствах управляемого устройства описаны в таблице ниже.

Параметры резервного хранилища в свойствах устройства

Параметр	Описание
Хранить объекты не более (дней)	Поле ввода для указания периода хранения объектов в резервном хранилище. Доступные значения: 1–10000. Если флажок снят, период хранения объектов в резервном хранилище не ограничен. Значение по умолчанию: 30.
Ограничить размер резервного хранилища до (МБ)	Поле ввода для указания максимального размера резервного хранилища (в мегабайтах). Если флажок снят, размер резервного хранилища не ограничен. Значение по умолчанию: 1024.

Настройка параметров резервного хранилища в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры резервного хранилища в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры хранилищ**) и в свойствах управляемого устройства (**Управляемые устройства** → закладка **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: 1–999999. Если флажок снят, размер резервного хранилища не ограничен. По умолчанию флажок снят.

Настройка параметров 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.

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 – 999999 0 – размер резервного хранилища не ограничен. Значение по умолчанию: 0.
`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 объектами резервного хранилища в командной строке

В командной строке с помощью команд управления резервным хранилищем вы можете выполнять следующие действия с объектами резервного хранилища:

- Просматривать информацию об объектах резервного хранилища.
- Удалять из резервного хранилища все или только указанные объекты.
- Восстанавливать объекты из резервного хранилища.

Восстановление зараженных объектов может привести к заражению устройства.

Просмотр информации об объектах резервного хранилища

Чтобы просмотреть информацию об объектах резервного хранилища, выполните следующую команду:

```
kesl-control -B --query ["<условия фильтра>"] [-n <количество>] [--json]
```

где:

- `<условия фильтра>` – 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 объектах резервного хранилища.
- `<количество>` – 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.

Восстановление объектов из резервного хранилища

Чтобы восстановить объект с исходным именем в исходное местоположение, выполните следующую команду:

```
kesl-control -B --restore <идентификатор объекта>
```

где < идентификатор объекта > – числовой идентификатор, который приложение присвоило объекту при помещении в резервное хранилище.

Чтобы восстановить объект с новым именем в указанную директорию, выполните следующую команду:

```
kesl-control -B --restore < идентификатор объекта > --file < путь к файлу >
```

где --file < путь к файлу > – 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.

Удаление объектов из резервного хранилища

Чтобы удалить выбранные объекты из резервного хранилища, выполните следующую команду:

```
kesl-control -B --mass-remove --query "< условия фильтра >"
```

где < условия фильтра > – одно или несколько логических выражений в формате < поле > < операция сравнения > '< значение >', скомбинированных с помощью логического оператора and, для ограничения результатов запроса.

Примеры:
Чтобы удалить объект с ID=15:

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

Чтобы 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
```

Интеграция с решениями Detection and Response

Решения Detection and Response от "Лаборатории Касперского" представляют собой системы безопасности, предназначенные для обнаружения сложных угроз и признаков атак на разных уровнях инфраструктуры организации. Решения Detection and Response предоставляют вам информацию об обнаруженной угрозе и позволяют управлять действиями по реагированию на обнаружения.

Приложение Kaspersky Endpoint Security может взаимодействовать со следующими решениями Detection and Response от "Лаборатории Касперского":

- Kaspersky Endpoint Detection and Response Expert (on-premise) на платформе Open Single Management Platform (OSMP). Интеграцию обеспечивает компонент приложения Kaspersky Endpoint Security – Endpoint Detection and Response Expert (on-premise) (далее также *EDR Expert (on-premise)*).
- 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-premise) (далее также *EDR Expert (on-premise)*).
  - 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*).

Если вы используете приложение Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response, поддерживается интеграция только с Kaspersky Endpoint Detection and Response Expert (on-premise) 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 в журнал systemd может записываться большое количество событий. Если вы хотите выключить запись событий аудита в systemd, вам нужно отключить сокет systemd-journald-audit и перезагрузить операционную систему.

Чтобы отключить сокет systemd-journald-audit, выполните следующие команды:

```
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 for 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-premise)

О действиях по реагированию по командам от решений Detection and Response

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-premise), 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-premise), 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-premise), 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-premise) и с Kaspersky Endpoint Detection and Response (KATA) 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-premise) 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-premise), 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-premise) 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-premise), 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-premise), 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.

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) или с Kaspersky Endpoint Detection and Response (KATA) задача для поиска IOC на устройстве с установленным Kaspersky Endpoint Security создается и запускается на стороне соответствующего решения Detection and Response.

  При интеграции с Kaspersky Endpoint Detection and Response Optimum поиск IOC выполняется с помощью задачи поиска IOC (*IOC Scan*). Вы можете создавать задачи поиска IOC вручную.

- 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 решения Kaspersky Endpoint Detection and Response Expert (on-premise).

- Запрет запуска объектов.

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise), с Kaspersky Endpoint Detection and Response (KATA) или с Kaspersky Endpoint Detection and Response Optimum вы можете включить применение правил запрета запуска объектов. Приложение Kaspersky Endpoint Security будет запрещать запуск объектов или открытие документов, соответствующих критериям правил запрета.

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) или с Kaspersky Endpoint Detection and Response (KATA) приложение получает правила запрета запуска от Kaspersky Endpoint Detection and Response Expert (on-premise) или от Kaspersky Endpoint Detection and Response (KATA).

  При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете настраивать правила запрета запуска объектов в Web Console.

- Сбор форензики.

  При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) 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 решения Kaspersky Endpoint Detection and Response Expert (on-premise).

Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise)

Kaspersky Endpoint Detection and Response Expert (on-premise) – решение для кибербезопасности бизнеса, позволяющее защититься от большинства киберрисков и покрыть основные сценарии распространения угроз. Компоненты Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise).

При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) приложение Kaspersky Endpoint Security может выполнять следующие функции:

- Отправлять данные о событиях на устройствах (телеметрию) на сервер сбора телеметрии на платформе OSMP (далее также *сервер сбора телеметрии OSMP*). Приложение Kaspersky Endpoint Security передает на сервер сбора телеметрии 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 сервера действий по реагированию на платформе OSMP (далее также *сервер действий по реагированию OSMP*).

Интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premise) обеспечивает компонент приложения Kaspersky Endpoint Security – Endpoint Detection and Response Expert (on-premise) (далее также *EDR Expert (on-premise)*).

Во время интеграции с решением Kaspersky Endpoint Detection and Response Expert (on-premise) устройства с Kaspersky Endpoint Security устанавливают защищенные соединения по протоколу HTTPS с сервером действий по реагированию OSMP и с сервером сбора телеметрии OSMP. Для обеспечения безопасности соединения используются следующие сертификаты, выданные серверами OSMP:

- Сертификат сервера. Соединение шифруется с помощью TLS-сертификата сервера. Вы можете повысить уровень безопасности соединения, включив проверку сертификата сервера на стороне Kaspersky Endpoint Security. Для этого вам нужно добавить сертификат сервера перед включением интеграции с решением Kaspersky Endpoint Detection and Response Expert (on-premise).

- Сертификат клиента. Этот сертификат используется для дополнительной защиты подключения с помощью двусторонней аутентификации (то есть проверки устройств с приложением Kaspersky Endpoint Security серверами OSMP). Один и тот же сертификат клиента может использоваться несколькими устройствами. По умолчанию сервер не выполняет проверку сертификатов клиентов, но двусторонняя аутентификация может быть включена на стороне Kaspersky Endpoint Detection and Response Expert (on-premise). В этом случае вам нужно включить двустороннюю аутентификацию в параметрах компонента EDR Expert (on-premise) и добавить сертификат клиента (криптоконтейнер с сертификатом и закрытым ключом).

Сертификаты для защиты соединения с серверами OSMP предоставляет администратор платформы OSMP.

Если в общих параметрах приложения Kaspersky Endpoint Security настроено использование прокси-сервера, то для подключения к серверам OSMP используется прокси-сервер.

Чтобы использовать функциональность Kaspersky Endpoint Detection and Response Expert (on-premise), вам нужно активировать компонент EDR Expert (on-premise). Если основная лицензия, по которой вы используете приложение Kaspersky Endpoint Security, не включает функциональность Kaspersky Endpoint Detection and Response Expert (on-premise), вам нужно приобрести отдельную лицензию для этой функциональности и добавить в приложение лицензионный ключ EDR Expert (on-premise).

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионных ключей на SVM.

Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise) состоит из следующих этапов:

1. **Включение необходимых компонентов Kaspersky Endpoint Security**

   Компонент EDR Expert (on-premise) может использовать данные, полученные от следующих компонентов:

   - Защита от файловых угроз.
   - Защита от сетевых угроз.
   - Защита от веб-угроз.
   - Защита от шифрования.
   - Контроль приложений.
   - Контроль устройств.
   - Контроль целостности системы.

Для полноценной интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Expert (on-premise) требуется включить компонент Анализ поведения. Если Анализ поведения выключен, необходимые данные телеметрии не передаются (кроме запросов на синхронизацию и данных об обнаружении угроз от других компонентов защиты).

При использовании механизма eBPF для получения системной телеметрии в компоненте Анализ поведения (доступный на 64-битных операционных системах с версией ядра 4.18 и выше с поддержкой eBPF) данные телеметрии будут более полными.

2. **Активация компонента EDR Expert (on-premise)**

   Убедитесь, что соблюдено одно из следующих условий:

   - Вы используете приложение Kaspersky Endpoint Security по лицензии, которая включает в себя функциональность Kaspersky Endpoint Detection and Response Expert (on-premise).
   - Вы приобрели отдельную лицензию на использование функциональности Kaspersky Endpoint Detection and Response Expert (on-premise) и добавили в приложение лицензионный ключ EDR Expert (on-premise).

     Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, лицензионный ключ для активации дополнительной функциональности добавляется на SVM.

3. **Включение компонента EDR Expert (on-premise)**

   По умолчанию интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise) выключена. Для включения интеграции вам нужно включить компонент EDR Expert (on-premise) и настроить его параметры:

   - С помощью Kaspersky Security Center Web Console.
   - С помощью командной строки.

   Настройка интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) в Консоли администрирования Kaspersky Security Center не поддерживается.

   Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) вам нужно выбрать режим интеграции *EDR Expert (OSMP)* в параметрах компонента EDR Expert (on-premise). Если вы используете Web Console, в параметрах политики выберите вариант **Endpoint Detection and Response Expert (версия 8.0 и выше)**. Если вы используете командную строку, в параметрах задачи установите значение параметра `Mode=EDRExpertOnPrem`. Чтобы настраивать интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise) на устройстве, в Web Console требуется настроить "замки" для обеих версий (версия 8.0 и выше и версия 7.1 и ниже).

Если вы хотите использовать функциональность запрета запуска объектов, вы можете включить применение правил запрета запуска объектов компонента EDR Expert (on-premise).
Вы можете проверить статус работы компонента EDR Expert (on-premise):

- С помощью *Отчета о статусе компонентов приложения* в Web Console.

  Подробную информацию о работе с отчетами см. в справке Kaspersky Security Center.

- В свойствах устройства в Web Console (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → **Общие** → **Компоненты**).
- С помощью командной строки, выполнив команду `kesl-control --app-info`.

Как подготовить эталонный образ для корректной интеграции с EDR Expert (on-premise)

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-premise), 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.

Настройка интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) в Web Console

В Web Console вы можете включать и выключать компонент EDR Expert (on-premise) и настраивать параметры интеграции приложения Kaspersky Endpoint Security с Kaspersky Endpoint Detection and Response Expert (on-premise) в свойствах политики (**Параметры приложения** → **Встроенные агенты** → **Endpoint Detection and Response Expert (on-premise)**).

Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) вам нужно включить компонент EDR Expert (on-premise) и выбрать вариант **Endpoint Detection and Response Expert (версия 8.0 и выше)**, то есть режим интеграции *EDR Expert (OSMP)*.

Для параметров интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise) 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-premise) станут доступными для изменения.

Настройка интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) в командной строке

В командной строке вы можете управлять интеграцией приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (on-premise) на платформе OSMP с помощью предустановленной задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise) (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-premise) в параметрах задачи вам нужно выбрать режим интеграции *EDR Expert (OSMP)* и настроить нужные параметры интеграции.

Вы можете настраивать параметры интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise), изменяя параметры предустановленной задачи.

По умолчанию задача *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise)* 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-premise).

Параметры интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise)

В таблице ниже описаны параметры предустановленной задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise) (KATAEDR)*, которые вы можете настраивать при интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise).

Задача также позволяет настраивать параметры интеграции с компонентом Kaspersky Endpoint Detection and Response (KATA). Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) в параметрах задачи вам нужно выбрать режим интеграции *EDR Expert (OSMP)* (параметр `Mode=EDRExpertOnPrem`).

Параметры интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise)

Параметр	Описание	Значение
`Mode`	Режим интеграции. Для интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) 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 (OSMP). Позволяет включить интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premise).
`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-premise)* 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`	Включение и выключение отправки 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`.

Параметр	Описание	Значение
`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 (on-premise)* и добавить сертификат клиента перед 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`	Включение и выключение отправки только телеметрии с индикатором атаки (Indicator of Attack, IOA). *Индикатор атаки* – описание подозрительного поведения объектов в IT-инфраструктуре организации, которое может являться признаком целевой атаки на эту организацию.	`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`	Включение и выключение регулирования количества событий, отправляемых на сервер сбора телеметрии OSMP.	`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

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 <файл> --server-type response
```

где `<файл>` – 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 <файл> --server-type response
   ```

   где `<файл>` – 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-premise)* 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 <файл> --server-type telemetry
```

где <файл> – 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 <файл> --server-type telemetry
```

где < файл > – 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-premise)* 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 Anti Targeted Attack Platform

Приложение Kaspersky Endpoint Security совместимо с решением Kaspersky Anti Targeted Attack Platform, которое предназначено 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 может выполнять следующие функции:

  - Отправлять данные о событиях на устройствах (телеметрию) на сервер с компонентом Central Node, обеспечивающий взаимодействие с Kaspersky Endpoint Detection and Response (KATA) (далее также *сервер KATA*). Приложение Kaspersky Endpoint Security передает на сервер с компонентом Central Node на платформе Kaspersky Anti Targeted Attack Platform 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 Anti Targeted Attack Platform.

  Поддерживается интеграция с Kaspersky Endpoint Detection and Response (KATA) версии 7.1 и ниже.

- Kaspersky 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. 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. При интеграции приложения Kaspersky Endpoint Security с Sandbox на платформе Kaspersky Anti Targeted Attack Platform приложение отправляет файлы на проверку на сервер с компонентом Central Node, обеспечивающий взаимодействие с Sandbox.

Интеграцию с компонентами на платформе Kaspersky Anti Targeted Attack Platform обеспечивают следующие компоненты приложения Kaspersky Endpoint Security:

- Компонент Endpoint Detection and Response Expert (on-premise) (далее также *EDR Expert (on-premise)*).

  Начиная с версии Kaspersky Endpoint Security 12.4 для Linux компонент Endpoint Detection and Response (KATA) переименован в Endpoint Detection and Response Expert (on-premise). 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-premise).

- Компонент Network Detection and Response (KATA) (далее также *NDR (KATA)*).

- Компонент *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.

Во время интеграции с решением Kaspersky Anti Targeted Attack Platform устройства с Kaspersky Endpoint Security устанавливают защищенные соединения по протоколу HTTPS с серверами с компонентом Central Node, обеспечивающими интеграцию. Для обеспечения безопасности соединения используются следующие сертификаты, выданные серверами Central Node:

- Сертификат сервера. Соединение шифруется с помощью TLS-сертификата сервера. Вы можете повысить уровень безопасности соединения, включив проверку сертификата сервера на стороне Kaspersky Endpoint Security. Для этого вам нужно добавить сертификат сервера перед включением интеграции с решением Kaspersky Anti Targeted Attack Platform.

- Сертификат клиента. Этот сертификат используется для дополнительной защиты подключения с помощью двусторонней аутентификации (то есть проверки устройств с приложением Kaspersky Endpoint Security серверами Central Node). Один и тот же сертификат клиента может использоваться несколькими устройствами. По умолчанию сервер не выполняет проверку сертификатов клиентов, но двусторонняя аутентификация может быть включена на стороне Kaspersky Anti Targeted Attack Platform. В этом случае вам нужно включить двустороннюю аутентификацию в параметрах компонента EDR Expert (on-premise), NDR (KATA) или Sandbox и добавить сертификат клиента (криптоконтейнер с сертификатом и закрытым ключом).

Сертификаты для защиты соединения с серверами, обеспечивающими взаимодействие с компонентами решения Kaspersky Anti Targeted Attack Platform, предоставляет администратор Kaspersky Anti Targeted Attack Platform.

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.

Чтобы использовать функциональность Kaspersky Endpoint Detection and Response (KATA), вам нужно активировать компонент EDR Expert (on-premise). Если основная лицензия, по которой вы используете приложение Kaspersky Endpoint Security, не включает функциональность Kaspersky Endpoint Detection and Response Expert (on-premise), вам нужно приобрести отдельную лицензию для этой функциональности и добавить в приложение лицензионный ключ EDR Expert (on-premise).

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионных ключей на SVM.

Интеграция с компонентами решения Kaspersky Endpoint Detection and Response (KATA) и Kaspersky Network Detection and Response (KATA) состоит из следующих этапов:

1. **Включение необходимых компонентов Kaspersky Endpoint Security**

   Компоненты EDR Expert (on-premise) и NDR (KATA) могут использовать данные, полученные от следующих компонентов:

   - Защита от файловых угроз.
   - Защита от сетевых угроз.
   - Защита от веб-угроз.
   - Защита от шифрования.
   - Контроль приложений.

- Контроль устройств.
- Контроль целостности системы.

Для полноценной интеграции приложения Kaspersky Endpoint Security с Kaspersky Anti Targeted Attack Platform требуется включить компонент Анализ поведения. Если Анализ поведения выключен, необходимые данные телеметрии не передаются (кроме запросов на синхронизацию и данных об обнаружении угроз от других компонентов защиты).

При использовании механизма eBPF для получения системной телеметрии в компоненте Анализ поведения (доступный на 64-битных операционных системах с версией ядра 4.18 и выше с поддержкой eBPF) данные телеметрии будут более полными.

2 Активация компонента EDR Expert (on-premise)

Для интеграции с Kaspersky Endpoint Detection and Response (KATA) вам нужно активировать компонент EDR Expert (on-premise). Убедитесь, что соблюдено одно из следующих условий:

- Вы используете приложение Kaspersky Endpoint Security по лицензии, которая включает в себя функциональность Kaspersky Endpoint Detection and Response Expert (on-premise).
- Вы приобрели отдельную лицензию на использование функциональности Kaspersky Endpoint Detection and Response Expert (on-premise) и добавили в приложение лицензионный ключ EDR Expert (on-premise).

  Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, лицензионный ключ для активации дополнительной функциональности добавляется на SVM.

Активировать компонент NDR (KATA) не требуется, основные лицензии Kaspersky Endpoint Security включают в себя функциональность интеграции с Kaspersky Network Detection and Response (KATA).

3 Включение компонента EDR Expert (on-premise)

По умолчанию интеграция с Kaspersky Endpoint Detection and Response (KATA) выключена. Для включения интеграции вам нужно включить компонент EDR Expert (on-premise) и настроить его параметры:

- С помощью Kaspersky Security Center Web Console.
- С помощью Консоли администрирования Kaspersky Security Center.
- С помощью командной строки.

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-premise). Если вы используете Web Console, в параметрах политики выберите вариант **Endpoint Detection and Response Expert (версия 7.1 и ниже)**. Если вы используете командную строку, в параметрах задачи установите значение параметра `Mode=EDRKATA`. 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 хотите использовать функциональность запрета запуска объектов, вы можете включить применение правил запрета запуска объектов компонента EDR Expert (on-premise).

4. **Включение компонента NDR (KATA)**

   По умолчанию интеграция с Kaspersky Network Detection and Response (KATA) выключена. Для включения интеграции вам нужно включить компонент NDR (KATA) и настроить его параметры:

   - С помощью Kaspersky Security Center Web Console.
   - С помощью Консоли администрирования Kaspersky Security Center.
   - С помощью командной строки.

Вы можете проверить статус работы компонентов EDR Expert (on-premise) и NDR (KATA):

- С помощью *Отчета о статусе компонентов приложения* в Web Console.

  Подробную информацию о работе с отчетами см. в справке Kaspersky Security Center.

- В свойствах устройства в Web Console (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → **Общие** → **Компоненты**).

- С помощью командной строки, выполнив команду `kesl-control --app-info`.

Настройка интеграции с Kaspersky Endpoint Detection and Response (KATA) в Web Console

В Web Console вы можете настраивать параметры интеграции приложения с Kaspersky Endpoint Detection and Response (KATA) в свойствах политики (**Параметры приложения** → **Встроенные агенты** → **Endpoint Detection and Response Expert (on-premise)**).

Для интеграции с Kaspersky Endpoint Detection and Response (KATA) вам нужно включить компонент EDR Expert (on-premise) и выбрать вариант **Endpoint Detection and Response Expert (версия 7.1 и ниже)**, то есть режим интеграции *EDR (KATA)*.

Чтобы применить на устройствах значение параметра **Максимальная задержка отправки событий (сек.)**, заданное в блоке параметров **Настройка передачи данных** для компонента Endpoint Detection and Response Expert (KATA) в политике в Web Console, требуется закрыть "замки" для блоков параметров **Настройка передачи данных** и **Регулирование количества запросов** в свойствах политики. Чтобы разрешить изменять локально на устройстве значение параметра `MaximumDataTransferTime` в секции `[EventTransferSettings]` для задачи KATAEDR в режиме интеграции EDR (KATA), требуется снять "замки" для блоков параметров **Настройка передачи данных** и **Регулирование количества запросов** в свойствах политики.

Настройка интеграции с Kaspersky Endpoint Detection and Response (KATA) в Консоли администрирования

В Консоли администрирования вы можете включать и выключать компонент EDR Expert (on-premise) и настраивать параметры интеграции приложения Kaspersky Endpoint Security с компонентом Kaspersky Endpoint Detection and Response (KATA) в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Detection and Response → EDR Expert (on-premise)**).

Если в Web Console для компонента EDR Expert (on-premise) выбран вариант **Endpoint Detection and Response Expert (версия 8.0 и выше)**, то есть режим интеграции EDR Expert (OSMP), 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 (KATA)

Параметр	Описание
Включить Endpoint Detection and Response Expert (on-premise)	Флажок включает или выключает компонент EDR Expert (on-premise), 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-premise).
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`.
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. Если архив защищен паролем, введите пароль в поле **Пароль криптоконтейнера**. • **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`.

Настройка интеграции с Kaspersky Endpoint Detection and Response (KATA) в командной строке

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-premise) (KATAEDR)*.

Задача также позволяет настраивать параметры интеграции с решением Kaspersky Endpoint Detection and Response Expert (on-premise). 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-premise)* 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-premise).

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-premise) (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-premise). 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-premise) 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 (OSMP). Позволяет включить интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premise).
`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-premise)* 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`	Включение и выключение 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`.

Параметр	Описание	Значение
`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 <файл>
```

где `<файл>` – путь к файлу, содержащему сертификат сервера.

Чтобы добавить или заменить сертификат клиента:

1. Выполните следующую команду:

```
kesl-control [-R] --add-kataedr-client-certificate <файл>
```

где `< файл >` – 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 KATA, если в параметрах сервера KATA включена проверка сертификата клиента и в параметрах задачи *Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise)* 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
```

Настройка интеграции с Kaspersky Network Detection and Response (KATA) в Web Console

В Web Console вы можете настраивать параметры интеграции приложения с Kaspersky Network Detection and Response (KATA) в свойствах политики (**Параметры приложения** → **Встроенные агенты** → **Network Detection and Response (KATA)**).

Чтобы применить на устройствах значение параметра **Максимальная задержка отправки событий (сек.)**, заданное в блоке параметров **Настройка передачи данных** для компонента Network Detection and Response (KATA) в политике в Web Console, требуется закрыть "замки" для блоков параметров **Настройка передачи данных** и **Регулирование количества запросов** в свойствах политики. Чтобы разрешить изменять локально на устройстве значение параметра `MaximumDataTransferTime` в секции `[EventTransferSettings]` для задачи KATANDR, требуется снять "замки" для блоков параметров **Настройка передачи данных** и **Регулирование количества запросов** в свойствах политики.

Настройка интеграции с Kaspersky Network Detection and Response (KATA) в Консоли администрирования

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 (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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.

Параметр	Описание
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. Если архив защищен паролем, введите пароль в поле **Пароль криптоконтейнера**. • **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`.
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`.

Настройка интеграции с Kaspersky Network Detection and Response (KATA) в командной строке

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)*.

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`.

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 <файл>
```

где `<файл>` – путь к файлу, содержащему сертификат сервера.

Чтобы добавить или заменить сертификат клиента:

1. Выполните одну следующую команду:

   ```
   kesl-control [-R] --add-katandr-client-certificate <файл>
   ```

   где `<файл>` – 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 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

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 на платформе Open Single Management Platform (OSMP) или на платформе Kaspersky Anti Targeted Attack Platform. В зависимости от платформы взаимодействие приложения Kaspersky Endpoint Security с Sandbox обеспечивает *сервер Sandbox* – сервер OSMP или сервер с компонентом Central Node.

Интеграцию с Sandbox обеспечивает компонент приложения Kaspersky Endpoint Security *Sandbox*.

Во время интеграции с Sandbox устройства с Kaspersky Endpoint Security устанавливают защищенные соединения по протоколу HTTPS с серверами, обеспечивающими интеграцию. Для обеспечения безопасности соединения используются следующие сертификаты, выданные сервером OSMP или сервером Central Node:

- Сертификат сервера. Соединение шифруется с помощью TLS-сертификата сервера. Вы можете повысить уровень безопасности соединения, включив проверку сертификата сервера на стороне Kaspersky Endpoint Security. Для этого вам нужно добавить сертификат сервера перед включением интеграции с Sandbox.
- Сертификат клиента. Этот сертификат используется для дополнительной защиты подключения с помощью двусторонней аутентификации (то есть проверки устройств с приложением Kaspersky Endpoint Security сервером OSMP или сервером Central Node). Один и тот же сертификат клиента может использоваться несколькими устройствами. По умолчанию сервер не выполняет проверку сертификатов клиентов, но двусторонняя аутентификация может быть включена на стороне платформы OSMP или Kaspersky Anti Targeted Attack Platform. В этом случае вам нужно включить двустороннюю аутентификацию в параметрах компонента Sandbox и добавить сертификат клиента (криптоконтейнер с сертификатом и закрытым ключом).

Сертификаты для защиты соединения с серверами, обеспечивающими взаимодействие с Sandbox, предоставляет администратор платформы OSMP или Kaspersky Anti Targeted Attack Platform.

Если в общих параметрах приложения Kaspersky Endpoint Security настроено использование прокси-сервера, то для подключения к серверам, обеспечивающими взаимодействие с Sandbox, используется прокси-сервер.

Отправка файлов и директорий на проверку в Sandbox может выполняться в одном из следующих режимов:

- *Вручную*. При этом режиме вы можете отправить объекты на проверку в Sandbox вручную с помощью команды или из графического интерфейса.
- *Только автоматический*. Приложение автоматически отправляет объекты на проверку, при этом отправить объекты на проверку в Sandbox вручную невозможно.
- *Автоматический и ручной*. Приложение автоматически отправляет объекты на проверку, при этом вы можете отправить объекты на проверку в Sandbox вручную с помощью команды или из графического интерфейса.

По умолчанию интеграция с Sandbox выключена. Вы можете включать и выключать компонент Sandbox, а также настраивать следующие параметры интеграции с помощью Web Console и командной строки:

- Выбирать режим отправки объектов на проверку (вручную, только автоматический, автоматический и ручной).
- Выбирать действия, которые приложение будет выполнять при обнаружении угрозы (в асинхронном режиме отправки объекта в Sandbox):
  - Удалять файл с обнаруженным объектом и помещать копию файла на карантин.
  - Запускать задачу проверки важных областей. По умолчанию приложение проверяет память процессов, память ядра, загрузочные секторы, объекты автозапуска и путь к обнаруженному объекту.
  - Создавать задачу поиска IOC. Приложение автоматически создает задачу поиска IOC, вы можете настроить режим запуска задачи, область поиска и действие при обнаружении IOC (удалить обнаруженный объект, запустить задачу проверки важных областей).
- Настраивать общие параметры подключения к серверам Sandbox.
- Добавлять и удалять сертификаты серверов Sandbox.
- Настраивать двустороннюю аутентификацию при подключении к серверам Sandbox и добавлять сертификаты клиента.

Настройка интеграции с Sandbox в Web Console

В Web Console вы можете настраивать параметры интеграции приложения с Sandbox в свойствах политики (**Параметры приложения** → **Встроенные агенты** → **Sandbox**).

Настройка интеграции с Sandbox в командной строке

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.

Запуск задачи *Интеграция с Sandbox* невозможен, если не добавлен сертификат сервера.

Если задача *Интеграция с Sandbox* запущена, в командной строке вы можете отправлять файлы в Sandbox на проверку.

Чтобы отправить файлы в Sandbox на проверку, выполните следующую команду:

```
kesl-control [-X] --sandbox <путь>
```

где `<путь>` – 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*.

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`.

Параметр	Описание	Значение
`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.		
`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 <файл>
```

где `<файл>` – путь к файлу, содержащему сертификат сервера.

Чтобы добавить или заменить сертификат клиента:

1. Выполните команду:

   ```
   kesl-control [-X] --add-sandbox-client-certificate <файл>
   ```

   где `<файл>` – 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 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
```

Интеграция с Kaspersky 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.

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.

Приложение Kaspersky Endpoint Security 12.4 для Linux совместимо с решением Kaspersky Endpoint Detection and Response Optimum версии 3.1.

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.

Интеграцию приложения 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*).

Чтобы использовать функциональность Kaspersky Endpoint Detection and Response Optimum, вам нужно активировать компонент EDR Optimum. Если основная лицензия, по которой вы используете приложение Kaspersky Endpoint Security, не включает функциональность Kaspersky Endpoint Detection and Response Optimum, вам нужно приобрести отдельную лицензию для этой функциональности и добавить в приложение лицензионный ключ EDR Optimum.

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионных ключей на SVM.

Интеграция с Kaspersky Endpoint Detection and Response Optimum состоит из следующих этапов:

1. **Включение необходимых компонентов Kaspersky Endpoint Security**

   Убедитесь, что включены и работают следующие компоненты приложения Kaspersky Endpoint Security:

   - Защита от файловых угроз.
   - Защита от веб-угроз.
   - Анализ поведения.

   Вы также можете включить запрет запуска объектов.

2. **Включение средств анализа угроз**

   Убедитесь, что включен 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.

3. **Активация компонента EDR Optimum**

Убедитесь, что соблюдено одно из следующих условий:

- Вы используете приложение Kaspersky Endpoint Security по лицензии, которая включает в себя функциональность Kaspersky Endpoint Detection and Response Optimum.
- Вы приобрели отдельную лицензию на использование функциональности Kaspersky Endpoint Detection and Response Optimum и добавили в приложение лицензионный ключ EDR Optimum.

  Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, лицензионный ключ для активации дополнительной функциональности добавляется на SVM.

4. **Установка плагина 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.

5. **Включение компонента EDR Optimum**

   По умолчанию компонент EDR Optimum выключен. Вы можете включать и выключать компонент, а также настраивать параметры интеграции:

   - с помощью Web Console;
   - с помощью командной строки.

     Управление компонентом EDR Optimum с помощью Консоли администрирования Kaspersky Security Center не поддерживается.

   Вы можете проверить статус работы компонента EDR Optimum:

   - С помощью *Отчета о статусе компонентов приложения* в Web Console.

     В список компонентов Kaspersky Endpoint Security добавлен компонент **Endpoint Detection and Response Optimum**. Подробную информацию о работе с отчетами см. в справке Kaspersky Security Center.
   - В свойствах устройства в Web Console.
   - С помощью командной строки.

6. **Включение передачи 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.

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum

Вы можете включать и выключать компонент EDR Optimum:

- с помощью Web Console;
- с помощью командной строки.

Управление параметрами интеграции с Kaspersky Endpoint Detection and Response Optimum через Консоль администрирования не поддерживается.

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console

В Web Console вы можете включать и выключать компонент EDR Optimum и настраивать параметры интеграции с Kaspersky Endpoint Detection and Response Optimum:

- в свойствах политики (**Параметры приложения → Встроенные агенты → Endpoint Detection and Response**);
- в свойствах управляемого устройства (**Активы (Устройства) → Управляемые устройства** → ссылка <имя устройства> → закладка **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → закладка **Параметры приложения** → раздел **Detection and Response → Endpoint Detection and Response Optimum**).

  Включение и выключение компонента EDR Optimum в свойствах устройства недоступно, если на устройство распространяется действие политики.

  Параметры интеграции с Kaspersky Endpoint Detection and Response Optimum в свойствах устройства

Параметр	Описание
Endpoint Detection and Response Optimum включен/выключен	Включает или выключает компонент EDR Optimum, необходимый для интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Optimum. По умолчанию переключатель выключен.
Сетевая изоляция	По ссылке **Настроить разблокировку устройства** открывается окно **Настройка разблокировки устройства**, в котором вы можете настроить длительность блокировки устройства.
Исключения	По ссылке **Настроить исключения** открывается окно **Исключения**, в котором вы можете настроить исключения сетевой изоляции.

Включение и выключение интеграции с Kaspersky Endpoint Detection and Response Optimum в командной строке

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
```

Просмотр статуса интеграции с Kaspersky Endpoint Detection and Response Optimum

Просмотр статуса интеграции в Web Console

Вы можете посмотреть статус интеграции с Kaspersky Endpoint Detection and Response Optimum в Web Console, выбрав раздел **Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → закладка **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → закладка **Общие** → **Компоненты**.

Просмотр статуса интеграции в командной строке

Вы можете посмотреть статус интеграции с Kaspersky Endpoint Detection and Response Optimum с помощью командной строки, выполнив команду `kesl-control --app-info`.

Статусы интеграции

Для компонента EDR Optimum отображается один из следующих статусов:

- *Выполняется*.

Этот статус отображается при одновременном соблюдении следующих условий:

- добавлен лицензионный ключ, необходимый для работы EDR Optimum;
- текущая дата не превышает дату окончания срока действия лицензии;
- один или несколько компонентов Kaspersky Endpoint Security, необходимых для работы EDR Optimum, включены;
- на устройстве включена интеграция с Kaspersky Endpoint Detection and Response Optimum.

- *Остановлена*.

  Этот статус отображается в следующих случаях:

  - интеграция с Kaspersky Endpoint Detection and Response Optimum выключена;
  - приложение Kaspersky Endpoint Security остановлено.

- *Не поддерживается лицензией*.

  Этот статус отображается в следующих случаях:

  - текущая дата превышает дату окончания срока действия лицензии;
  - действующая лицензия не включает функциональность EDR Optimum.

- *Ошибка*.

  Этот статус отображается при одновременном соблюдении следующих условий:

  - текущая дата не превышает дату окончания срока действия лицензии;
  - в работе одного или нескольких компонентов Kaspersky Endpoint Security, необходимых для работы EDR Optimum, произошла ошибка.

Просмотр информации об обнаруженной угрозе и действиях по реагированию

Для просмотра всей информации об обнаруженной угрозе и выполнения действий по реагированию на эту угрозу вы можете воспользоваться окном с деталями алерта, которое содержит:

- граф цепочки развития угрозы;
- рекомендации по реагированию на угрозу с возможностью выполнения выбранного действия;
- общую информацию об обнаружении угрозы (например, о режиме обнаружения);
- информацию о защищаемом устройстве;
- информацию об обнаруженном объекте;
- историю появления файлов на устройстве;
- информацию о выполненных приложением действиях по реагированию на обнаруженную угрозу.

В окне с деталями алерта вы можете выполнить следующие действия по реагированию:

- изолировать устройство, на котором обнаружена угроза;
- поместить файл на карантин;
- создать задачу *Поиск IOC*.

Срок хранения деталей алерта составляет 30 дней. По истечении этого времени старые записи автоматически удаляются.

Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum.

Интеграция с Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response представляет собой решение для автоматического обнаружения и анализа инцидентов безопасности в вашей инфраструктуре с помощью телеметрии и передовых технологий машинного обучения. Информация об инциденте передается специалистам "Лаборатории Касперского", которые затем могут либо обработать инцидент самостоятельно, либо дать рекомендации по его устранению.

При взаимодействии с Kaspersky Managed Detection and Response приложение Kaspersky Endpoint Security может выполнять следующие функции:

- Отправлять данные телеметрии в Kaspersky Managed Detection and Response для обнаружения угроз.
- Выполнять действия по реагированию, направленные на обеспечение функций безопасности, по командам, полученным от Kaspersky Managed Detection and Response.

Интеграцию приложения Kaspersky Endpoint Security с решением Kaspersky Managed Detection and Response обеспечивает компонент приложения – Managed Detection and Response (далее также MDR).

Чтобы использовать функциональность Kaspersky Managed Detection and Response, вам нужно активировать компонент MDR одним из следующих способов:

- Путем добавления лицензионного ключа с помощью файла ключа или кода активации. Вы можете активировать приложение Kaspersky Endpoint Security по лицензии, которая включает функциональность Kaspersky Managed Detection and Response (подробнее см. в справке Kaspersky Managed Detection and Response). Если основная лицензия, по которой вы используете приложение, не включает функциональность Kaspersky Managed Detection and Response, вам нужно приобрести отдельную лицензию для этой функциональности и добавить в приложение лицензионный ключ MDR.

  Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионных ключей на SVM.

Лицензию, которая позволяет активировать функциональность Kaspersky Managed Detection and Response, требуется предварительно зарегистрировать на портале MDR.

- Путем загрузки на устройство *файла MDR BLOB*, который содержит информацию о лицензии Kaspersky Managed Detection and Response. Файл BLOB находится в ZIP-архиве конфигурационного файла MDR. Вы можете загрузить файл BLOB в Web Console, в Консоли администрирования или в командной строке.

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.

Интеграция с Kaspersky Managed Detection and Response состоит из следующих этапов:

1. **Включение необходимых компонентов Kaspersky Endpoint Security**

   Убедитесь, что включены и работают следующие компоненты приложения Kaspersky Endpoint Security:

   - Защита от файловых угроз.
   - Анализ поведения.

   Если эти компоненты выключены, устройство в Kaspersky Managed Detection and Response будет иметь красный статус.

   Рекомендуется также включить компоненты Защита от веб-угроз и Защита от сетевых угроз. Если эти компоненты выключены, устройство в Kaspersky Managed Detection and Response будет иметь желтый статус.

   Подробнее о статусах устройств см. в справке Kaspersky Managed Detection and Response.

2. **Включение использования Kaspersky Security Network в расширенном режиме**

   Функциональность Kaspersky Managed Detection and Response недоступна, если Kaspersky Security Network выключен или используется в стандартном режиме. Вы можете настроить использование Kaspersky Security Network в Web Console, в Консоли администрирования или в командной строке.

3. **Активация компонента MDR**

   Если вы используете компонент MDR по лицензии, убедитесь, что соблюдено одно из следующих условий:

   - Вы используете приложение Kaspersky Endpoint Security по лицензии, которая включает в себя функциональность Kaspersky Managed Detection and Response.
   - Вы приобрели отдельную лицензию на использование функциональности Kaspersky Managed Detection and Response и добавили в приложение лицензионный ключ MDR.

     Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, лицензионный ключ для активации дополнительной функциональности добавляется на SVM.

   Если вы активируете компонент MDR с помощью файла MDR BLOB, вам нужно загрузить файл BLOB в Web Console, в Консоли администрирования или в командной строке.

4. **Загрузка конфигурационного файла KPSN**

   Если ваша конфигурация не соответствует требованиям для работы без конфигурационных файлов KPSN, вам нужно загрузить на Сервер администрирования Kaspersky Security Center конфигурационный файл KPSN.

5. **Включение компонента MDR**

   По умолчанию компонент MDR выключен. Вы можете включать и выключать компонент:

   - с помощью Web Console;
   - с помощью Консоли администрирования;
   - с помощью командной строки.

   Вы можете проверить статус работы компонента MDR:

   - в свойствах устройства в Web Console или в Консоли администрирования;
   - с помощью командной строки.

Рекомендации по созданию эталонного образа для корректной интеграции с MDR

В эталонный образ не рекомендуется включать приложение Kaspersky Endpoint Security for Linux.

Если приложение Kaspersky Endpoint Security for 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 for Linux и установите его повторно.

Если не выполнить эти действия, устройства могут идентифицироваться некорректно.

Загрузка конфигурационного файла KPSN для интеграции с Kaspersky Managed Detection and Response

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.

Чтобы загрузить конфигурационный файла 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**.

Чтобы загрузить конфигурационный файла KPSN в Консоли администрирования:

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**.

Настройка интеграции с Kaspersky Managed Detection and Response в Web Console

В Web Console вы можете настраивать параметры интеграции с Kaspersky Managed Detection and Response в свойствах политики (**Параметры приложения** → **Встроенные агенты** → **Managed Detection and Response**).

Настройка интеграции с Kaspersky Managed Detection and Response в Консоли администрирования

В Консоли администрирования вы можете включать и выключать компонент MDR и загружать файл MDR BLOB в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Detection and Response** → **Managed Detection and Response**).

Если для активации компонента MDR вы используете лицензионный ключ, загружать файл MDR BLOB не требуется.

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.

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.

Настройка интеграции с Kaspersky Managed Detection and Response в командной строке

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.

- Изменять время запуска служебной задачи *Mdr_Autostart_Scan*, которая создается автоматически после интеграции Kaspersky Endpoint Security с Managed Detection and Response.

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 <путь к файлу 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. Если требуется, вы можете настроить время запуска этой задачи. Другие параметры задачи и другие параметры ее расписания недоступны для изменения.

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-premise) или с компонентом Kaspersky Endpoint Detection and Response (KATA) и активирован компонент EDR Expert (on-premise).
- 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-premise), 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-premise), 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-premise) 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 Агента Endpoint Detection and Response, 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. 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 закладку **Приложения**.

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

6. В открывшемся окне свойств приложения на закладке **Параметры приложения** выберите раздел **Detection and Response** и перейдите по ссылке **Endpoint Detection and Response Optimum**.

7. 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;

     При нажатии на эту кнопку приложение изолирует устройство на период, указанный в свойствах задачи *Включение сетевой изоляции (NetworkIsolationStart)*.

   - Нажмите на кнопку **Разблокировать изолированное устройство**, чтобы выключить сетевую изоляцию устройства.

8. 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-premise) 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 закладку **Приложения**.

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

6. В открывшемся окне свойств приложения на закладке **Параметры приложения** выберите раздел **Detection and Response**.

7. В блоке **Сетевая изоляция (EDR Expert (on-premise))** 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 закладку **Приложения**.

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

6. В открывшемся окне свойств приложения на закладке **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 закладку **Задачи**.

5. В списке задач нажмите на задачу *Включение сетевой изоляции*.

   Откроется окно со свойствами задачи.

6. Перейдите на закладку **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-premise), 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-premise), 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.

Настройка исключений из сетевой изоляции в автоматическом режиме

Вы можете настраивать исключения из сетевой изоляции для устройств, изолированных автоматически, в свойствах политики или в свойствах устройства. Параметры сетевой изоляции в свойствах политики в Web Console описаны в Приложении 5.

Вы можете настраивать исключения из сетевой изоляции только при интеграции с Kaspersky Endpoint Detection and Response Optimum.

Добавление и удаление исключений из сетевой изоляции в свойствах устройства недоступно, если на устройство распространяется действие политики.

Чтобы добавить или удалить исключение из сетевой изоляции в свойствах 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 выберите в открывшемся окне 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 закладку **Приложения**.

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

   Откроется окно свойств приложения.

6. В открывшемся окне свойств приложения на закладке **Параметры приложения** выберите раздел **Detection and Response** и перейдите по ссылке **Endpoint Detection and Response Optimum**.

7. В открывшемся окне в блоке параметров **Исключения** 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**, чтобы сохранить внесенные изменения.

Окно добавления исключения из сетевой изоляции

В этом окне вы можете ввести информацию о сетевом соединении, которое не нужно блокировать после включения сетевой изоляции.

Параметры сетевого соединения

Параметр	Описание
Название	Поле ввода названия сетевого соединения.
Направление	В раскрывающемся списке вы можете выбрать направление сетевого соединения: • **Исходящее**. • **Входящее**. • **Входящее/Исходящее**.
Протокол	В раскрывающемся списке вы можете выбрать протокол, используемый сетевым соединением: • **Любой**. • **Пользовательский**. • **ICMP**. • **IPv6_ICMP**. • **TCP**. • **UDP**. • **IGMP**. • **GRE**. • **IPv4**. • **IPv6**.
Номер	Поле ввода номера сетевого соединения. Поле доступно, если в раскрывающемся списке **Протокол** выбрано значение **Пользовательский**.
Локальные порты/ диапазоны	Флажок добавляет номера локальных портов или диапазоны локальных портов, перечисленные в поле ниже, в перечень исключений из сетевой изоляции.
Удаленные порты/ диапазоны	Флажок добавляет номера удаленных портов или диапазоны удаленных портов, перечисленные в поле ниже, в перечень исключений из сетевой изоляции.
Удаленный адрес	Флажок добавляет IP-адрес удаленного устройства, указанный в поле ниже, в перечень исключений из сетевой изоляции.
Приложения	Флажок добавляет приложения, перечисленные в таблице под флажком, в перечень исключений из сетевой изоляции. Вы можете добавить путь к приложению, сетевое соединение с которым не нужно блокировать, нажав на кнопку **Добавить**. В открывшемся окне введите путь к приложению в поле **Путь к приложению** и сохраните изменения. Вы можете удалить приложение из таблицы, установив флажок напротив удаляемого приложения, а затем нажав на кнопку **Удалить**. Эти параметры применимы на устройствах с версией ядра от 4.18 с поддержкой eBPF с BTF и с включенными функциями tracepoints и kprobes для трассировки ядра.

Окно Словарь сетевых профилей

В этом окне вы можете выбрать один или несколько профилей исключаемого сетевого соединения.

Профили сетевых соединений

Профиль сетевого соединения	Описание
DNS-сервер	Служба, обеспечивающая разрешение DNS-имен, отвечая на запросы получения IP-адресов и запросы обновления DNS-записей.
DNS-клиент	Служба, обеспечивающая разрешение DNS-имен, выполняя запросы DNS-имен.

Профиль сетевого соединения	Описание
Службы сертификатов Active Directory	Службы, используемые для создания, проверки и отзыва сертификатов открытых ключей для внутреннего пользования в организации.
Службы федерации Active Directory	Службы, используемые для предоставления пользователям доступа к нескольким веб-службам или сетевым ресурсам при помощи единых наборов учетных данных, хранящихся централизованно.
Службы Active Directory облегченного доступа к каталогам	Службы, предоставляющие те же функции, что и доменные службы Active Directory, но не требующие создания доменов или контроллеров домена.
Службы управления правами Active Directory	Службы, используемые для управления доступом пользователей к документам.
DHCP	Служба, использующая протокол динамической конфигурации узлов (DHCP) для автоматического распределения IP-адресов.
Протокол передачи файлов (FTP)	Стандартный сетевой протокол, используемый для передачи файлов между клиентом и сервером в сети.
Центр распространения ключей Kerberos	Сетевая служба, используемая для предоставления тикетов (TGS) и временных ключей сеанса пользователям и устройствам в домене Active Directory.
Безопасная оболочка (SSH)	Протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений.
Системные компоненты Linux	Системные сетевые службы Linux, например, NetworkManager.

Управление сетевой изоляцией устройства в командной строке

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*.

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).

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 на карантин критически важных системных объектов (англ. System Critical Object, SCO) невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Endpoint Security.

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-premise) или с компонентом Kaspersky Endpoint Detection and Response (KATA) и активирован компонент EDR Expert (on-premise).
- 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-premise) 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-premise) или в справке Kaspersky Anti Targeted Attack Platform.
- В результате выполнения задачи YARA-проверки 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.

Помещение файла на карантин с помощью Web Console

При интеграции с Kaspersky Endpoint Detection and Response Optimum вы можете помещать файлы на карантин с помощью задачи *Помещение файла на карантин* в Web Console.

Вы можете создавать и запускать задачу помещения файла на карантин для всех управляемых устройств или для конкретного устройства.

Задача выполняется для файлов, указанных в свойствах задачи на закладке **Параметры приложения** в таблице **Помещение файла на карантин**. Таблица содержит следующую информацию о файлах, которые требуется поместить на карантин:

- **Путь** – путь к директории на устройстве, где находится файл.
- **Тип контрольной суммы** – тип проверки контрольной суммы файла.

С помощью кнопок над таблицей вы можете добавлять или удалять информацию о файлах, которые требуется поместить на карантин.

Чтобы добавить информацию о файле, который требуется поместить на карантин, вам нужно нажать на кнопку **Добавить** и указать параметры задачи в открывшемся окне.

Параметры задачи Помещение файла на карантин

Параметр	Описание
Укажите файл, который требуется поместить на карантин	В раскрывающемся списке вы можете выбрать способ указания пути к файлу, помещаемому на карантин: • **Задать файл по полному пути**. • **Задать файл по пути к директории и контрольной сумме**.
Полный путь к файлу	Поле ввода полного пути к файлу, помещаемому на карантин. Это поле отображается, если в раскрывающемся списке **Укажите файл, который требуется поместить на карантин** вы выбрали значение **Задать файл по полному пути**. Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `//`. Например, вы можете ввести путь `//server_ip/shared_folder`.

Параметр	Описание
Тип контрольной суммы	В раскрывающемся списке вы можете выбрать тип контрольной суммы файла, помещаемого на карантин: • **MD5**. • **SHA256**. Этот раскрывающийся список отображается, если в раскрывающемся списке **Укажите файл, который требуется поместить на карантин** вы выбрали значение **Задать файл по пути к директории и контрольной сумме**.
Контрольная сумма файла	Поле ввода контрольной суммы файла, помещаемого на карантин. Это поле отображается, если в раскрывающемся списке **Укажите файл, который требуется поместить на карантин** вы выбрали значение **Задать файл по пути к директории и контрольной сумме**.
Путь к файлу	Поле ввода пути к директории файла, помещаемого на карантин. Это поле отображается, если в раскрывающемся списке **Укажите файл, который требуется поместить на карантин** вы выбрали значение **Задать файл по пути к директории и контрольной сумме**. Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `//`. Например, вы можете ввести путь `//server_ip/shared_folder`.

Задача *Помещение файла на карантин* может завершиться с ошибкой *Недостаточно места в хранилище карантина*, если вы пытаетесь поместить на карантин большой файл. В этом случае вы можете очистить карантин или увеличить размер карантина и затем повторить попытку.

Вы можете посмотреть результат выполнения задачи в свойствах задачи в Web Console в разделе **Результаты**.

Настройка параметров карантина в Web Console

В Web Console вы можете настраивать параметры карантина в свойствах политики (**Параметры приложения** → **Общие настройки** → **Отчеты и хранилище**) и в свойствах управляемого устройства (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → закладка **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → закладка **Параметры приложения** → раздел **Параметры хранилищ**).

Параметры карантина в свойствах управляемого устройства описаны в таблице ниже.

Параметры карантина в свойствах устройства

Параметр	Описание
Ограничить размер карантина до (МБ)	Поле ввода для указания максимального размера карантина (в мегабайтах). Если флажок снят, размер карантина не ограничен. Значение по умолчанию: 200.
Уведомлять при заполнении карантина на (%)	Поле ввода для указания процента 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.

Настройка параметров карантина в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры карантина в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры хранилищ**) и в свойствах управляемого устройства (**Управляемые устройства** → закладка **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 Агента Endpoint Detection and Response, 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.

Настройка параметров карантина в командной строке

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.

Параметр	Описание	Значение
`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 – 999999 0 – размер карантина не ограничен. Значение по умолчанию: 200, если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response, 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 <путь к файлу> [--md5] [--sha256] [--save-original-file]
```

где:

- `<путь к файлу>` – 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 ["<условия фильтра>"] [-n <количество>] [--json]
```

где:

- `<условия фильтра>` – 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.
- `<количество>` – 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 <идентификатор объекта>
```

где `<идентификатор объекта>` – 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 <идентификатор объекта> --file <путь к файлу>
```

где `--file <путь к файлу>` – 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.

Удаление файлов из карантина

Чтобы удалить выбранные файлы из карантина, выполните следующую команду:

```
kesl-control -Q --mass-remove --query "<условия фильтра>"
```

где `условия фильтра` – одно или несколько логических выражений в формате `<поле> <операция сравнения> '<значение>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.

Примеры:
Чтобы удалить файлы, 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
```

Запуск процесса

При интеграции Kaspersky Endpoint Security с решениями Detection and Response можно удаленно запускать процессы и исполняемые файлы на защищаемом устройстве с помощью задачи запуска процесса (*Run process*).

Вы можете создавать и выполнять задачи запуска процессов в Web Console только при интеграции с Kaspersky Endpoint Detection and Response Optimum. При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise), с Kaspersky Endpoint Detection and Response (KATA) или Kaspersky Managed Detection and Response задачи создаются и запускаются на стороне соответствующего решения Detection and Response.

С помощью задачи *Запуск процесса* вы можете запускать:

- Процессы, остановленные в результате вредоносной активности на устройстве.
- Процессы, остановленные вами. Например, вы можете удаленно запустить процесс, который был завершен вами с помощью задачи *Завершение процесса*.
- Скрипты. Например, вы можете запустить скрипт, чтобы собрать с устройства данные, необходимые для расследования возникновения угрозы.
- Утилиты. Например, вы можете запустить утилиту, которая сохраняет информацию о конфигурации устройства в файл.
- Приложения.

Если в вашей операционной системе установлена система SELinux в режиме `Enforcing`, то для запуска задачи *Запуск процесса* вам нужно дополнительно настроить систему SELinux.

Вы можете создавать и запускать задачу *Запуск процесса*, а также изменять ее параметры в Web Console. Управление задачей *Запуск процесса* с помощью командной строки не поддерживается.

Параметры задачи Запуск процесса

Параметр	Описание
Исполняемая команда	Поле ввода команды запуска процесса. Например, если вы хотите запустить утилиту `klnagchk`, которая предназначена для проверки подключения к Серверу администрирования, вам нужно ввести `/< абсолютный путь к директории с утилитой >/klnagchk`, а затем, если необходимо, заполнить остальные поля, описанные в этой таблице ниже.
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. Например, вы можете ввести аргументы `-logfile /tmp/klnagchk.log -savecert /home/user/certificate.cer`. Эти аргументы указывают утилите, что нужно сохранить результат работы в файл с именем `klnagchk.log` в директории `/tmp`, а также сохранить сертификат, используемый для проверки доступа к Серверу администрирования, в файле `certificate.cer` в директории `/home/user/`.
Путь к рабочей директории (необязательно)	Поле ввода пути к рабочей директории, в которой выполняется команда из поля **Исполняемая команда**. 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`.

Вы можете посмотреть результат выполнения задачи *Запуск процесса* в свойствах задачи в Web Console в разделе **Параметры приложения** → **Результаты выполнения**.

В таблице отображается список устройств, на которых выполнена задача *Запуск процесса*, а также результаты выполнения задачи. В раскрывающемся списке **Устройство** вы можете выбрать отображение результатов задачи для всех управляемых устройств, на которых запускалась задача, или для конкретного устройства.

Таблица содержит следующие сведения:

- **Статус** – статус выполнения задачи.
- **Устройство** – имя устройства, на котором запускалась задача.
- **Время** – дата и время выполнения задачи.

- **Результаты** – результат выполнения задачи в виде кода возврата. По ссылке с кодом возврата открывается окно **Результаты запуска задачи**, в котором отображается следующая информация:
  - статус выполнения задачи;
  - время запуска процесса;
  - время завершения процесса;
  - имя устройства, на котором был запущен процесс;
  - исполняемая команда;
  - аргументы командной строки;
  - путь к рабочей директории;
  - код возврата.

По ссылке **Скачать данные потока STDOUT** в окне **Результаты запуска задачи** вы можете скачать отчет об успешном выполнении задачи в формате TXT. Если задача *Запуск процесса* завершилась с ошибкой, то при попытке скачивания этого отчета отобразится сообщение об ошибке.

По ссылке **Скачать данные потока STDERR** в окне **Результаты запуска задачи** вы можете скачать отчет об ошибках, возникших в процессе выполнения задачи, в формате TXT. Если задача *Запуск процесса* завершилась успешно, то при попытке скачивания этого отчета отобразится сообщение об ошибке.

Завершение процесса

При интеграции Kaspersky Endpoint Security с решениями Detection and Response можно удаленно завершать процессы на защищаемом устройстве с помощью задачи завершения процесса (*Terminate process*).

Вы можете создавать и выполнять задачи завершения процессов в Web Console только при интеграции с Kaspersky Endpoint Detection and Response Optimum. При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise), с Kaspersky Endpoint Detection and Response (KATA) или Kaspersky Managed Detection and Response задачи создаются и запускаются на стороне соответствующего решения Detection and Response.

С помощью задачи *Завершение процесса* вы можете завершать:

- Процессы, запущенные на устройстве в результате вредоносной активности.
- Процессы, запущенные вами. Например, вы можете удаленно завершить процесс, который был запущен вами с помощью задачи *Запуск процесса*.
- Скрипты. Например, вы можете удаленно завершить работу скрипта, который был запущен вами с помощью задачи *Запуск процесса*.

- Утилиты. Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена вами с помощью задачи *Запуск процесса*.

- Приложения.

Невозможно завершить процессы критически важных системных объектов (англ. System Critical Object, SCO). К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Endpoint Security.

Вы можете создавать и запускать задачу *Завершение процесса*, а также изменять ее параметры в Web Console. Управление задачей *Завершение процесса* с помощью командной строки не поддерживается.

Параметры задачи Завершение процесса

Параметр	Описание
Укажите файл, процессы которого требуется завершить	В раскрывающемся списке вы можете выбрать способ указания пути к файлу: • **По пути к директории и контрольной сумме**. • **По полному пути**. • **По PID**. Значение **По PID** отображается в раскрывающемся списке только для задач, создаваемых в свойствах устройства.
Полный путь к файлу	Поле ввода полного пути к файлу. Это поле отображается, только если в раскрывающемся списке **Укажите файл, процессы которого требуется завершить** вы выбрали значение **По полному пути**.
Тип контрольной суммы	В раскрывающемся списке вы можете выбрать тип контрольной суммы файла: • **MD5**. • **SHA256**. Этот раскрывающийся список отображается, если в раскрывающемся списке **Укажите файл, процессы которого требуется завершить** вы выбрали значение **По пути к директории и контрольной сумме**.
Контрольная сумма файла	Поле ввода контрольной суммы файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, процессы которого требуется завершить** вы выбрали значение **По пути к директории и контрольной сумме**, а в раскрывающемся списке **Тип контрольной суммы** значение **MD5**.
Путь к директории	Поле ввода пути к директории файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, процессы которого требуется завершить** вы выбрали значение **По пути к директории и контрольной сумме**.
Идентификатор процесса	Поле ввода идентификатора процесса (PID). Это поле отображается, если в раскрывающемся списке **Укажите файл, процессы которого требуется завершить** вы выбрали значение **По PID**.

Вы можете посмотреть результат выполнения задачи *Завершение процесса* в свойствах задачи в Web Console в разделе **Результаты**.

Получение файла с устройства

При интеграции Kaspersky Endpoint Security с решениями Detection and Response можно получать файлы с защищаемого устройства с помощью задачи получения файла (*Get file*).

Вы можете создавать и выполнять задачи получения файла с устройства в Web Console только при интеграции с Kaspersky Endpoint Detection and Response Optimum. При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise), с Kaspersky Endpoint Detection and Response (KATA) или Kaspersky Managed Detection and Response задачи создаются и запускаются на стороне соответствующего решения Detection and Response.

Например, вы можете получить файл журнала событий, который создало стороннее приложение.

Вы можете создавать и запускать задачу *Получение файла с устройства*, а также изменять ее параметры в Web Console. Управление задачей *Получение файла с устройства* с помощью командной строки не поддерживается.

Задача *Получение файла с устройства* выполняется для файлов, указанных в свойствах задачи на закладке **Параметры приложения** в таблице **Получение файла**.

Таблица содержит следующую информацию о файлах, которые требуется получить в результате выполнения задачи:

- **Путь к директории** – путь к директории на устройстве, где находится файл.
- **Тип проверки контрольной суммы** – тип проверки контрольной суммы файла.

С помощью кнопок над таблицей вы можете добавлять, изменять или удалять информацию о файлах, которые требуется получить с устройства.

Чтобы добавить информацию о файле, который требуется получить, вам нужно нажать на кнопку **Добавить** и указать параметры задачи в открывшемся окне **Получение файла**.

Параметры задачи Получение файла с устройства

Параметр	Описание
Укажите файл, который требуется получить	В раскрывающемся списке вы можете выбрать способ указания пути к файлу: • **По пути к директории и контрольной сумме**. • **По полному пути**.
Полный путь к файлу	Поле ввода полного пути к файлу. Это поле отображается, если в раскрывающемся списке **Укажите файл, который требуется получить** вы выбрали значение **По полному пути**.
Тип контрольной суммы	В раскрывающемся списке вы можете выбрать тип контрольной суммы файла: • **MD5**. • **SHA256**. Этот раскрывающийся список отображается, если в раскрывающемся списке **Укажите файл, который требуется получить** вы выбрали значение **По пути к директории и контрольной сумме**.

Параметр	Описание
Контрольная сумма файла	Поле ввода контрольной суммы файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, который требуется получить** вы выбрали значение **По пути к директории и контрольной сумме**.
Путь к директории с файлом	Поле ввода пути к директории файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, который требуется получить** вы выбрали значение **По пути к директории и контрольной сумме**.

В результате выполнения задачи *Получение файла с устройства* копия файла помещается на карантин на устройстве. Вы можете загрузить эту копию из карантина через Web Console на то устройство, с которого вы инициировали загрузку

Размер файла не должен превышать 100 МБ.

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 с устройства*, будут иметь статус *Заражен* независимо от результатов проверки файла.

Задача *Получение файла с устройства* 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).

Вы можете посмотреть результат выполнения задачи в свойствах задачи в Web Console в разделе **Результаты**.

Удаление файла с устройства

При интеграции Kaspersky Endpoint Security с решениями Detection and Response можно удалять файлы с защищаемого устройства с помощью задачи удаления файла (*Delete file*).

Вы можете создавать и выполнять задачи удаления файла в Web Console только при интеграции с Kaspersky Endpoint Detection and Response Optimum. При интеграции с Kaspersky Endpoint Detection and Response (KATA) задачи создаются и запускаются на стороне Kaspersky Endpoint Detection and Response (KATA).

Критически важные системные объекты (англ. System Critical Object, SCO) удалить невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Endpoint Security.

Вы можете создавать и запускать задачу *Удаление файла с устройства*, а также изменять ее параметры в Web Console. Управление задачей *Удаление файла с устройства* с помощью командной строки не поддерживается.

Параметры задачи Удаление файла с устройства

Параметр	Описание
Укажите файл, который нужно удалить	В раскрывающемся списке вы можете выбрать способ указания пути к удаляемому файлу: • **По пути и контрольной сумме**. • **По полному пути**.
Полный путь к файлу	Поле ввода полного пути к удаляемому файлу. Это поле отображается, если в раскрывающемся списке **Укажите файл, который нужно удалить** вы выбрали значение **По полному пути**.
Тип контрольной суммы	В раскрывающемся списке вы можете выбрать тип контрольной суммы удаляемого файла: • **MD5**. • **SHA256**. Этот раскрывающийся список отображается, если в раскрывающемся списке **Укажите файл, который нужно удалить** вы выбрали значение **По пути и контрольной сумме**.
Контрольная сумма файла	Поле ввода контрольной суммы удаляемого файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, который нужно удалить** вы выбрали значение **По пути и контрольной сумме**.
Путь к директории	Поле ввода пути к директории удаляемого файла. Это поле отображается, если в раскрывающемся списке **Укажите файл, который нужно удалить** вы выбрали значение **По пути и контрольной сумме**.
Включать вложенные директории	Флажок включает или выключает вложенные директории.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки устройства. После перезагрузки устройства убедитесь, что файл удален.

Задача *Удаление файла с устройства* может завершиться с ошибкой *Доступ запрещен*, если вы пытаетесь удалить запущенный исполняемый файл. В этом случае вам нужно создать и выполнить задачу *Завершение процесса* для этого файла, а затем повторить попытку удаления.

Вы можете посмотреть результат выполнения задачи в свойствах задачи в Web Console в разделе **Результаты**.

Поиск индикаторов компрометации

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. При интеграции Kaspersky Endpoint Security с решениями Detection and Response вы можете обнаруживать на защищаемых устройствах индикаторы компрометации 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.
- Включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (on-premise) или с компонентом Kaspersky Endpoint Detection and Response (KATA) и активирован компонент EDR Expert (on-premise).

При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) или с Kaspersky Endpoint Detection and Response (KATA) поиск IOC выполняется на стороне соответствующего решения.

При интеграции с Kaspersky Endpoint Detection and Response Optimum поиск IOC выполняется с помощью задачи *Поиск IOC* (*IOC Scan*). Вы можете создавать задачи поиска IOC:

- в Web Console;
- из окна с деталями алерта;
- в командной строке.

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.

Поиск индикаторов компрометации в Web Console

Вы можете выполнять поиск индикаторов компрометации с помощью задачи поиска IOC в Web Console только при интеграции с Kaspersky Endpoint Detection and Response Optimum. При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) или с Kaspersky Endpoint Detection and Response (KATA) поиск IOC выполняется на стороне соответствующего решения Detection and Response.

Вы можете создавать и запускать задачу *Поиск IOC*, а также изменять ее параметры в Web Console.

Для задачи *Поиск IOC* функция Wake-on-LAN в параметрах расписания недоступна. Убедитесь, что устройство включено для выполнения задачи.

Вы можете изменять основные параметры задачи *Поиск IOC* в свойствах задачи на закладке **Параметры приложения** → **Параметры поиска IOC**.

Параметры задачи *Поиск IOC*

Параметр	Описание
Переопределить IOC-файлы	При нажатии на кнопку открывается панель **Переопределить IOC-файлы**. При нажатии на кнопку **Добавить IOC-файлы**, расположенную в панели **Переопределить IOC-файлы**, открывается окно, с помощью которого вы можете выбрать на устройстве и загрузить IOC-файлы, необходимые для поиска индикаторов компрометации. После загрузки IOC-файлов вы можете просмотреть список индикаторов из IOC-файлов.
Экспортировать IOC-коллекцию	При нажатии на кнопку выполняется скачивание IOC-файлов на устройство.

Параметр	Описание
Применять действия по реагированию при обнаружении IOC	Флажок включает или выключает применение действий по реагированию при обнаружении индикаторов компрометации. Если флажок установлен, то при обнаружении индикаторов компрометации приложение выполняет выбранные вами действия: • **Запускать проверку важных областей**. Если флажок установлен, то при обнаружении индикаторов компрометации приложение запускает задачу *Проверка важных областей*. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы, загрузочные секторы и другие **важные области**. ◦ /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 • **Поместить копию на карантин, объект удалить**. Если флажок установлен, то при обнаружении индикаторов компрометации приложение помещает копию объекта на карантин и удаляет исходный объект.

Параметр	Описание
	• **Изолировать устройство от сети**. Если флажок установлен, то при обнаружении индикаторов компрометации приложение изолирует устройство от сети для предотвращения распространения угрозы. Вы можете настроить время изоляции. Если на изолируемое устройство распространяется действие политики, то применяются параметры автоматического отключения изоляции через указанный период, а также параметры исключений из сетевой изоляции, заданные в свойствах политики. Если на изолируемое устройство действие политики не распространяется, то применяются параметры, заданные в свойствах устройства. Если флажок снят, то при обнаружении индикаторов компрометации приложение не выполняет действия по реагированию. Информация об обнаружении индикаторов компрометации отображается в окне с деталями алерта и в свойствах задачи.

Вы можете изменять дополнительные параметры задачи *Поиск IOC* в свойствах задачи на закладке **Параметры приложения → Дополнительно**.

Раздел **Дополнительно** доступен для редактирования если вы загрузили IOC-файл в панели **Переопределить IOC-файлы**.

Дополнительные параметры задачи *Поиск IOC*

Параметр	Описание
Типы данных (IOC-документы) для анализа во время поиска IOC	Флажки в разделе **Дополнительно** добавляют следующие типы данных (IOC-документы) для анализа во время поиска IOC: • **Процессы - ProcessItem**. • **Файлы - FileItem**. • **IOC-документы**. Ссылка **IOC-документы** доступна если вы загрузили IOC-файл в панели **Переопределить IOC-файлы**. По этой ссылке вы можете перейти в окно **Параметры проверки файлов – FileItem**, в котором вы можете добавить области проверки. • **ARP-таблицы - ArpEntryItem**. • **Сетевые порты - PortItem**. • **Учетные записи пользователей - UserItem**. • **Системные объекты - SystemItem**.
Искать IOC в следующих областях	Флажок включает или выключает проверку следующих областей: • **Файлы на всех дисках устройства**. • **Файлы на системных дисках устройства**. • **Важные области на устройстве**. Этот вариант выбран по умолчанию. • **Не проверять предопределенные области**.
Проверять указанные области	Флажок добавляет области, перечисленные в таблице под флажком, в перечень областей проверки. Вы можете добавить путь к области, которую нужно проверять, нажав на кнопку **Добавить**. В открывшемся окне введите путь к области в поле **Область** и сохраните изменения. Вы можете удалить область из таблицы, установив флажок напротив удаляемой области, а затем нажав на кнопку **Удалить**. Вы не можете снять флажок, если в списке **Искать IOC в следующих областях** выбран вариант **Не проверять предопределенные области**.

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 создавать новые задачи.

Вы можете посмотреть результат выполнения задачи *Поиск IOC* в свойствах задачи в Web Console в разделе **Параметры приложения → Результаты поиска IOC**. В таблице отображается список устройств, на которых выполнена задача *Поиск IOC*, а также результаты выполнения задачи. В раскрывающемся списке **Устройство** вы можете выбрать отображение результатов задачи для всех управляемых устройств, на которых запускалась задача, или для конкретного устройства.

Таблица содержит следующие сведения:

- **Статус** – статус обнаружения индикаторов компрометации, отображающийся в виде значка.
- **Устройство** – имя устройства, на котором запускалась задача.
- **Время** – дата и время выполнения задачи.
- **Результаты** – информация о результате выполнения задачи *Поиск IOC*. Может отображаться один из следующих статусов:
  - *обнаружены IOC* – отображается в виде ссылки, при переходе по которой открывается окно с деталями алерта;
  - *IOC не обнаружены*.

Срок хранения результатов поиска IOC составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет старые записи.

Поиск индикаторов компрометации в командной строке

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-premise) 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 <путь к директории или файлу> [--process on|off]
[--hint <регулярное выражение>] [--arpentry on|off] [--ports on|off] [--system on|off]
[--files on|off] [--drives all|system|critical|custom] [--excludes <список исключений>]
[--scope <список директорий>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

где:

- `--path <путь к директории или файлу>` – 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 <регулярное выражение>` – 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 <список исключений>` – 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 <список директорий>` – 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**.
  - /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.

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.

СКАЧАТЬ 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`.

Запрет запуска объектов

При интеграции с решениями Detection and Response в рамках действия по реагированию на угрозы приложение Kaspersky Endpoint Security может контролировать 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.

Запрет запуска объектов работает на основании правил запрета запуска. *Правило запрета запуска* – это набор критериев, которые приложение Kaspersky Endpoint Security учитывает при реагировании на запуск объекта. Объект должен соответствовать всем критериям правила запрета запуска, чтобы приложение заблокировало его запуск. Приложение идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.

Функциональность запрета запуска объектов 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.
- Включена интеграция приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (on-premise) или с компонентом Kaspersky Endpoint Detection and Response (KATA) и активирован компонент EDR Expert (on-premise).

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.

Включение запрета запуска объектов может повлиять на скорость запуска приложений в операционной системе.

Для работы запрета запуска объектов вам нужно включить применение правил запрета запуска объектов.

Особенности работы запрета запуска объектов при интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) или Kaspersky Endpoint Detection and Response (KATA)

При интеграции приложения Kaspersky Endpoint Security с решением Kaspersky Endpoint Detection and Response Expert (on-premise) или с компонентом Kaspersky Endpoint Detection and Response (KATA) приложение использует *правила запрета запуска объектов компонента EDR Expert (on-premise)*. Эти правила приложение получает от Kaspersky Endpoint Detection and Response Expert (on-premise) или Kaspersky Endpoint Detection and Response (KATA).

При интеграции с Kaspersky Endpoint Detection and Response Expert (on-premise) или Kaspersky Endpoint Detection and Response (KATA) вы можете:

- Включать и выключать применение правил запрета запуска объектов компонента EDR Expert (on-premise) в Web Console, в Консоли администрирования или в командной строке.

  При срабатывании правил запрета запуска приложение Kaspersky Endpoint Security отправляет отчет в Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise).

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 или в командной строке.

- 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.

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.

Настройка запрета запуска объектов в Web Console

Настройка запрета запуска объектов EDR Expert (on-premise)

Если включена интеграция с решением Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise)**).

Переключатель **Запрет запуска** включает или выключает применение правил запрета запуска объектов компонента EDR Expert (on-premise).

Настройка запрета запуска объектов EDR Optimum

Если включена интеграция с Kaspersky Endpoint Detection and Response Optimum, вы можете включать и выключать запрет запуска объектов и настраивать правила запрета запуска объектов компонента EDR Optimum:

- в свойствах политики (**Параметры приложения** → **Встроенные агенты** → **Endpoint Detection and Response**);
- в свойствах управляемого устройства (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → закладка **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → закладка **Параметры приложения** → раздел **Detection and Response** → **Endpoint Detection and Response Optimum**).

Включение и выключение запрета запуска объектов в свойствах устройства недоступно, если на устройство распространяется действие политики.

Параметры запрета запуска объектов EDR Optimum в свойствах устройства

Параметр	Описание
Запрет запуска объектов включен/ выключен	Включает или выключает применение правил запрета запуска объектов компонента EDR Optimum. По умолчанию применение правил выключено.
Действие при запуске или открытии объекта	Вы можете выбрать режим работы запрета запуска объектов: • **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.
Список правил запрета запуска объектов	По ссылке **Добавить** открывается окно, в котором вы можете настроить правило запрета запуска объектов компонента EDR Optimum. При необходимости вы можете удалить правило из списка с помощью кнопки **Удалить**.

Чтобы добавить в список правило запрета запуска объектов компонента EDR Optimum в свойствах устройства:

1. Нажмите на кнопку **Добавить**, расположенную над списком правил запрета запуска объектов.
2. В открывшемся окне введите название правила запрета запуска.
3. Укажите статус работы правила запрета запуска, установив переключатель в соответствующее положение:
   - **Включено** – правило включено, приложение применяет это правило во время работы.
   - **Выключено** – правило выключено и не используется во время работы приложения.

Вы можете включать или выключать созданное правило в любое время.

4. 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.

5. Для добавления объекта укажите путь к объекту и/или контрольную сумму объекта.

   Чтобы указать путь к объекту, выберите вариант **Использовать путь** и введите путь к объекту.

   Чтобы указать контрольную сумму объекта, выберите вариант **SHA256** или **MD5** и введите контрольную сумму объекта.

6. Нажмите на кнопку **OK**.

   Созданное правило добавлено в перечень правил в блоке параметров **Запрет запуска объектов**.

Настройка запрета запуска объектов в Консоли администрирования

Вы можете включать и выключать запрет запуска объектов в Консоли администрирования только если включена интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise) или с Kaspersky Endpoint Detection and Response (KATA).

Вы можете включать и выключать запрет запуска объектов в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Параметры приложения → Detection and Response → EDR Expert (on-premise)**).

Флажок **Включить запрет запуска объектов** в блоке параметров **Запрет запуска объектов** включает или выключает применение правил запрета запуска объектов компонента EDR Expert (on-premise).

Управление запретом запуска объектов в командной строке

В командной строке вы можете запускать и останавливать применение правил запрета запуска объектов с помощью следующих предустановленных задач:

- *Запрет запуска объектов (EDR Expert (on-premise))* (*KATAEDR_Prevention*).
- *Запрет запуска объектов (EDR Optimum)* (*EDRO_Prevention*).

По умолчанию задачи *Запрет запуска объектов (EDR Expert (on-premise))* и *Запрет запуска объектов (EDR Optimum)* не запущены. Вы можете запускать и останавливать эти задачи вручную.

Вы можете запустить задачу *Запрет запуска объектов (EDR Expert (on-premise))*, только если включена интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise) или с Kaspersky Endpoint Detection and Response (KATA).

Вы можете запустить задачу *Запрет запуска объектов (EDR Optimum)*, только если включена интеграция с Kaspersky Endpoint Detection and Response Optimum.

С помощью команд управления правилами запрета запуска объектов вы можете просматривать список правил запрета запуска объектов компонента EDR Expert (on-premise) и правила запрета запуска объектов компонента EDR Optimum.

Чтобы просмотреть список правил запрета запуска объектов компонента EDR Expert (on-premise), выполните следующую команду:

```
kesl-control [-T] --get-prevention-state --kata
```

Чтобы просмотреть список правил запрета запуска объектов компонента EDR Optimum, выполните следующую команду:

```
kesl-control [-T] --get-prevention-state --edro
```

Cloud Sandbox

Cloud Sandbox – технология, 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. Далее данные об этих файлах попадают в Kaspersky Security Network. Таким образом, если Cloud Sandbox обнаружит вредоносный файл, приложение Kaspersky Endpoint Security выполнит действие для устранения угрозы на всех устройствах, на которых обнаружит этот файл.

Для работы Cloud Sandbox требуется 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, по которой вы используете приложение.

Если у вас развернуто решение Kaspersky Endpoint Detection and Response Optimum, вы можете включить в Web Console отдельный счетчик для угроз, обнаруженных с помощью Cloud Sandbox:

- в свойствах политики (**Параметры приложения** → **Встроенные агенты** → **Endpoint Detection and Response**);
- в свойствах управляемого устройства (**Активы (Устройства)** → **Управляемые устройства** → ссылка <имя устройства> → закладка **Приложения** → ссылка <название приложения Kaspersky Endpoint Security> → закладка **Параметры приложения** → раздел **Detection and Response** → **Endpoint Detection and Response Optimum**).

Также счетчик угроз, обнаруженных с помощью Cloud Sandbox, отображается в отчетах графического пользовательского интерфейса. Вы можете использовать этот счетчик для составления статистики при анализе обнаруженных угроз.

Чтобы включить счетчик Cloud Sandbox в Web Console в свойствах устройства:

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

   Откроется список политик.

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 закладку **Приложения**.

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

6. В открывшемся окне свойств приложения на закладке **Параметры приложения** выберите раздел **Detection and Response** и перейдите по ссылке **Endpoint Detection and Response Optimum**.

7. В открывшемся окне в блоке параметров **Cloud Sandbox** включите переключатель **Cloud Sandbox**.

8. Нажмите на кнопку **OK**.

Интеграция с Kaspersky Unified Monitoring and Analysis Platform

Приложение Kaspersky Endpoint Security совместимо с решением Kaspersky Unified Monitoring and Analysis Platform (далее также KUMA).

Kaspersky Unified Monitoring and Analysis Platform – это комплексное программное решение, сочетающее в себе следующие функциональные возможности:

- получение, обработка и хранение событий информационной безопасности (телеметрии);
- анализ и корреляция поступающих данных;

- поиск по полученным событиям;
- создание уведомлений о выявлении признаков угроз информационной безопасности.

Подробнее о решении см. в справке Kaspersky Unified Monitoring and Analysis Platform.

Во время интеграции с Kaspersky Unified Monitoring and Analysis Platform устройства с Kaspersky Endpoint Security устанавливают защищенные соединения с сервером KUMA. Для обеспечения безопасности соединения используются следующие сертификаты, выданные сервером KUMA:

- Сертификат сервера KUMA. Соединение шифруется с помощью TLS-сертификата сервера. Вы можете повысить уровень безопасности соединения, включив проверку сертификата сервера на стороне Kaspersky Endpoint Security. Для этого вам нужно добавить сертификат сервера KUMA перед включением интеграции с Kaspersky Unified Monitoring and Analysis Platform.
- Сертификат клиента. Этот сертификат используется для дополнительной защиты подключения с помощью двусторонней аутентификации (проверки устройств с Kaspersky Endpoint Security сервером KUMA). Один и тот же сертификат клиента может использоваться несколькими устройствами. По умолчанию сервер KUMA не выполняет проверку сертификатов клиентов, но двусторонняя аутентификация может быть включена на стороне Kaspersky Unified Monitoring and Analysis Platform. В этом случае вам нужно включить двустороннюю аутентификацию в параметрах интеграции с Kaspersky Unified Monitoring and Analysis Platform и добавить сертификат клиента (криптоконтейнер с сертификатом и закрытым ключом).

Сертификаты для защиты соединения с сервером KUMA предоставляет администратор Kaspersky Unified Monitoring and Analysis Platform.

Для подключения к серверу KUMA используется прокси-сервер, если использование прокси-сервера настроено в общих параметрах приложения Kaspersky Endpoint Security.

По умолчанию интеграция с Kaspersky Unified Monitoring and Analysis Platform выключена. Вы можете включать и выключать интеграцию, а также настраивать следующие параметры интеграции с помощью командной строки, Web Console и Консоли администрирования:

- Настраивать общие параметры подключения к серверам KUMA.
- Добавлять и удалять сертификаты серверов KUMA.
- Настраивать двустороннюю аутентификацию при подключении к серверам KUMA и добавлять сертификаты клиента.
- Настраивать параметры передачи событий.

Перед включением интеграции с Kaspersky Unified Monitoring and Analysis Platform убедитесь, что соблюдено одно из следующих условий:

- Вы используете приложение Kaspersky Endpoint Security по лицензии, которая включает функциональность Kaspersky Unified Monitoring and Analysis Platform.
- Вы приобрели отдельную лицензию на использование функциональности Kaspersky Unified Monitoring and Analysis Platform и добавили в приложение лицензионный ключ для дополнительной функциональности (ключ KUMA).

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, активация выполняется на стороне Сервера защиты (компонента решения Kaspersky Security для виртуальных сред Легкий агент) путем добавления лицензионных ключей на SVM.

Настройка интеграции с KUMA в Web Console

В Web Console вы можете настраивать параметры интеграции приложения с Kaspersky Unified Monitoring and Analysis Platform в свойствах политики (**Параметры приложения** → **Встроенные агенты** → **Интеграция с KUMA**).

Настройка интеграции с KUMA в Консоли администрирования

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 (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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 или UDP. 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.
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.
Использовать двустороннюю аутентификацию	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.

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. Если архив защищен паролем, введите пароль в поле **Пароль криптоконтейнера**.

Настройка интеграции с KUMA в командной строке

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.

Параметры задачи 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*.

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. `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 **[SiemTransferSettings]** 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 <путь к файлу>
```

где `<путь к файлу>` – 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 <путь к файлу>
   ```

   где `<путь к файлу>` – 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 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
```

Настройка параметров использования приложения в режиме Легкого агента

Параметры, описанные в этом разделе, применяются, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Для работы приложения Kaspersky Endpoint Security в режиме Легкого агента требуется постоянное взаимодействие между Легким агентом и Сервером защиты, установленным на SVM. Если соединение с Сервером защиты отсутствует, Легкий агент не может передавать фрагменты файлов на проверку Серверу защиты, проверка не выполняется.

Для взаимодействия с Сервером защиты Легкий агент устанавливает и поддерживает подключение к SVM, на которой установлен этот Сервер защиты.

Вы можете настраивать параметры подключения Легкого агента к SVM в Web Console или в Консоли администрирования. В командной строке настройка параметров недоступна, вы можете только просматривать информацию об использовании приложения в режиме Легкого агента.

Вы можете настраивать следующие параметры подключения Легкого агента к SVM:

- Способ обнаружения SVM. Вы можете выбрать способ, который будут использовать Легкие агенты для обнаружения доступных для подключения SVM. Легкий агент может обнаруживать SVM, работающие в сети, одним из следующих способов:
  - С помощью Сервера интеграции. SVM передают информацию о себе на Сервер интеграции. Сервер интеграции формирует список доступных для подключения SVM и предоставляет его Легким агентам.

    Для использования этого способа обнаружения SVM требуется подключение SVM и Легких агентов 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.
  - С использованием списка адресов SVM. Вы можете задать список адресов SVM, к которым могут подключаться Легкие агенты.
- Алгоритм выбора SVM для подключения. После получения информации о доступных SVM Легкий агент выбирает оптимальную для подключения SVM в соответствии с алгоритмом выбора SVM. Вы можете указать, какой алгоритм должны использовать Легкие агенты при выборе SVM для подключения.
- Теги для подключения. Вы можете регулировать подключение Легких агентов к SVM с помощью тегов для подключения. Если вы используете теги для подключения, Легкий агент может подключаться только к тем SVM, на которых настроено использование этого тега для подключения.
- Защита соединения между Легким агентом и Сервером защиты. Вы можете защищать соединение между Легкими агентами и Серверами защиты с помощью шифрования.

Подробнее о параметрах подключения Легкого агента к SVM см. в справке решения Kaspersky Security для виртуальных сред Легкий агент.

Настройка параметров Легкого агента в Web Console

В Web Console вы можете настраивать параметры подключения Легкого агента к SVM в свойствах политики (**Параметры приложения** → **Режим Легкого агента**).

Настройка параметров Легкого агента в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры подключения Легкого агента к SVM в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**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 **ОК**.

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, Скала-Р, 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, Облачной платформы VK Cloud (Private Cloud от VK) или Облачной платформы ТИОНИКС).
	  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, Скала-Р, 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, Облачной платформы VK Cloud (Private Cloud от VK) или Облачной платформы ТИОНИКС).
	  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, Скала-Р, 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, Облачной платформы VK Cloud (Private Cloud от VK) или Облачной платформы ТИОНИКС).
	  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.

Просмотр в командной строке информации об использовании приложения в режиме Легкого агента

В командной строке вы можете посмотреть следующую информацию об использовании приложения в режиме Легкого агента для защиты виртуальных сред:

- о параметрах использования приложения в режиме Легкого агента;
- о подключении Легкого агента к Серверу интеграции;
- о подключении Легкого агента к SVM.

Чтобы посмотреть информацию о параметрах использования приложения в режиме Легкого агента, выполните следующую команду:

```
kesl-control [-V] --ksvla-info
```

В результате выполнения команды в консоль выводится следующая информация:

- Режим Легкого агента для защиты виртуальных сред: включен/выключен.

  Если режим Легкого агента включен, приложение используется в качестве Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент.

- Режим защиты инфраструктуры VDI: включен/выключен.

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

- Тип защищенной виртуальной машины: временная или постоянная.
- Роль защищенной виртуальной машины в виртуальной инфраструктуре: сервер или рабочая станция.
- Идентификатор (UUID) защищенной виртуальной машины.

Чтобы посмотреть информацию о подключении Легкого агента к Серверу интеграции, выполните следующую команду:

```
kesl-control [-V] --viis-info
```

В результате выполнения команды в консоль выводится следующая информация:

- Адрес и порт Сервера интеграции, к которому подключается Легкий агент.

  Если в вашей инфраструктуре развернут отказоустойчивый кластер Серверов интеграции на базе Linux, выводится адрес и порт балансировщика нагрузки. См. подробнее в справке Kaspersky Security для виртуальных сред Легкий агент.

- Статус подключения к Серверу интеграции.
- Дата и время последнего соединения Легкого агента с Сервером интеграции.

Чтобы посмотреть информацию о подключении Легкого агента к SVM, выполните следующую команду:

```
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.

Просмотр событий и отчетов

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 базе данных /var/opt/kaspersky/kesl/private/storage/events.db. 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 (Просмотр событий в командной строке, Просмотр событий в Kaspersky Security Center).

- 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. Вы можете включать и выключать запись событий в этот журнал с помощью Web Console, Консоли администрирования или командной строки.

Если для управления приложением вы используете командную строку, по умолчанию запись событий в журнал операционной системы выключена.

Если приложение Kaspersky Endpoint Security используется в стандартном режиме или в режиме Агента Endpoint Detection and Response и для управления приложением вы используете Kaspersky Security Center, в журнал операционной системы по умолчанию 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.

Настройка в Web Console

В Web Console вы можете включать и выключать запись событий в журнал операционной системы в свойствах политики (**Параметры приложения** → **Общие настройки** → **Настройки уведомлений**).

По нажатию на кнопку **Настройки** в блоке с названием уровня важности события (критические события, отказы функционирования, предупреждения, информационные сообщения) открывается окно, содержащее список событий этого уровня важности. Для каждого события вы можете настроить сохранение в журнал операционной системы.

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать запись событий в журнал операционной системы в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры приложения**).

По ссылке **Настроить** в блоке **Уведомления** открывается окно **Параметры уведомлений**. В этом окне вы можете с помощью флажков выбрать события, которые приложение будет записывать в журнал операционной системы.

Вы можете выбирать отдельные типы событий или все типы событий определенного уровня важности (критические события, отказы функционирования, предупреждения, информационные сообщения).

Настройка 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.

Параметр `UseSyslog` может принимать следующие значения:

- `Yes` – включить запись 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 изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

Просмотр событий в Kaspersky Security Center

Список всех событий в работе приложения Kaspersky Endpoint Security отображается в Web Console и в Консоли администрирования.

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.

Вы можете настроить уведомления о событиях. *Уведомление* – это сообщение с информацией о событии, которое произошло на защищенном устройстве. 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 командной строке

С помощью командной строки вы можете просматривать:

- текущие события приложения;

- события из журнала событий приложения.

Вывод текущих событий

Вы можете выводить в консоль информацию обо всех текущих событиях приложения или о текущих событиях, связанных с запуском или остановкой указанной задачи. С помощью фильтра вы так же можете выводить определенные текущие события, например, события указанного типа.

Чтобы вывести в консоль информацию обо всех текущих событиях приложения, выполните следующую команду:

```
kesl-control -W
```

Команда возвращает название события и дополнительную информацию о событии.

Чтобы вывести в консоль информацию только о текущих событиях, связанных с запущенной задачей, выполните следующую команду:

```
kesl-control --start-task <идентификатор/имя задачи> -W
```

Пример:
Включить вывод текущих событий запущенной задачи с ID=1:

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

Чтобы вывести в консоль информацию о текущих событиях, соответствующих условиям фильтра, выполните следующую команду:

```
kesl-control -W --query "<условия фильтра>"
```

Условия фильтра задаются с помощью одного или нескольких логических выражений в формате `<поле> <операция сравнения> '<значение>'`, скомбинированных с помощью логического оператора `and`.

Пример:
Вывести события TaskStateChanged:

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

Вывести события TaskSettingsChanged, инициированных пользователем User:

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

Вывод событий из журнала событий

Вы можете выводить в консоль или в файл информацию о событиях из журнала событий приложения. Вы можете использовать фильтр для вывода определенных событий.

Чтобы вывести в консоль информацию обо всех событиях в журнале событий приложения, выполните следующую команду:

```
kesl-control -E --query [--db <файл базы данных>]
```

где `<файл базы данных>` – 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, вы можете выводить в консоль информацию обо всех событиях с помощью команды `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`.

Чтобы вывести в консоль информацию о событиях в журнале событий приложения, соответствующих определенным условиям, выполните следующую команду:

```
kesl-control -E --query "<условия фильтра>" [--db <файл базы данных>] [-n
<количество>] [--json] [--reverse]
```

где:

- `<условия фильтра>` – одно или несколько логических выражений в формате `<поле> <операция сравнения> '<значение>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.
- `<количество>` – 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).

Чтобы вывести в файл информацию о событиях в журнале событий приложения, соответствующих определенным условиям, выполните следующую команду:

```
kesl-control -E --query "<условия фильтра>" [--db <файл базы данных>] [-n
<количество>] --file <путь к файлу> [--json]
```

где `--file <путь к файлу>` – полный путь к файлу, в который вы хотите вывести события.

Настройка всплывающих уведомлений в графическом интерфейсе

В графическом интерфейсе приложения информация о событиях по умолчанию отображается во всплывающих уведомлениях. Вы можете включать и выключать отображение всплывающих уведомлений с помощью Консоли администрирования или командной строки.

Настройка в Консоли администрирования

В Консоли администрирования вы можете включать и выключать отображение всплывающих уведомлений графическом интерфейсе в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры приложения**).

Флажок **Показывать всплывающие уведомления в графическом пользовательском интерфейсе** включает отображение всплывающих уведомлений в графическом пользовательском интерфейсе.

По умолчанию флажок установлен.

Настройка 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.

Параметр `ShowPopUpNotifications` может принимать следующие значения:

- `Yes` (значение по умолчанию) – показывать всплывающие уведомления в графическом пользовательском интерфейсе.
- `No` – не показывать всплывающие уведомления в графическом пользовательском интерфейсе.

Управление приложением через графический интерфейс

Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, графический интерфейс не поддерживается.

С помощью графического интерфейса приложения Kaspersky Endpoint Security вы можете:

- Просматривать информацию о состоянии защиты устройства.
- Включать и выключать 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.
- Запускать и останавливать задачи проверки:
  - Поиск вредоносного ПО.
  - Проверка важных областей.
  - Проверка контейнеров.
- Запускать выборочную проверку файлов и директорий.

- Запускать и останавливать задачи обновления и отката обновления баз.
- Отправлять файл или директорию на проверку в Sandbox.
- Включать и выключать использование Kaspersky Security Network.
- Управлять лицензионными ключами приложения и просматривать информацию о лицензии, по которой используется приложение, и о связанном с лицензией ключе.
- Запрашивать и получать временный доступ к заблокированному устройству у администратора локальной сети организации.
- Просматривать статистику работы и отчеты приложения.
- Просматривать информацию об объектах, помещенных в резервное хранилище.
- Создавать файлы трассировки приложения.

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.

Если компонент или задача приложения работает в информирующем режиме, то в графическом интерфейсе приложения для этого компонента или задачи отображается предупреждение *Выбран информирующий режим работы*.

Графический интерфейс

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 12.4 для Linux**. Открывает главное окно графического интерфейса приложения, в котором отображается состояние защиты устройства и находятся элементы интерфейса, предоставляющие доступ к функциям приложения.
- **Выход**. Выполняет выход из графического интерфейса приложения.

Главное окно графического интерфейса приложения

Вы можете открыть главное окно графического интерфейса приложения одним из следующих способов:

- Выбрав название приложения в меню приложений оконного менеджера операционной системы.
- С помощью правой кнопки мыши или двойным щелчком мыши по значку приложения в области уведомлений панели задач.

Главное окно графического интерфейса приложения разделено на несколько частей:

- В верхней части главного окна отображается статус защиты устройства. При нажатии на кнопку **Посмотреть** открывается окно **Центр защиты**. В этом окне отображается информация о состоянии защиты устройства и рекомендации о действиях, которые вам нужно выполнить для устранения проблем в защите (при их наличии).
- В блоке **Проверка** отображается состояние задачи поиска вредоносного ПО и количество обнаруженных угроз. При нажатии кнопкой мыши на этом блоке открывается окно **Проверка**. В этом окне вы можете запустить и остановить задачи *Поиск вредоносного ПО*, *Проверка важных областей* и *Проверка контейнеров*. Вы также можете просмотреть отчеты для этих задач.
- В блоке **Обновление** отображается состояние задачи *Обновление*. При нажатии кнопкой мыши на этом блоке открывается окно **Обновление**. В этом окне вы можете запустить задачи *Обновление* и *Откат обновления баз*. Вы также можете просмотреть отчеты для этих задач.
- В нижней части главного окна расположены следующие элементы:
  - Кнопка **Отчеты**. При нажатии на эту кнопку открывается окно **Отчеты**, в котором вы можете просмотреть статистику работы компонентов и задач и различные отчеты.
  - Кнопка **Резервное хранилище**. При нажатии на эту кнопку открывается окно **Резервное хранилище**, в котором содержится информация об объектах в резервном хранилище.
  - Кнопка **Настройка**. При нажатии на эту кнопку открывается окно **Настройка**, в котором вы можете включить или выключить компоненты приложения, а также настроить использование Kaspersky Security Network.
  - Кнопка **Временный доступ**. При нажатии на эту кнопку открывается окно **Временный доступ**, в котором вы можете запросить и получить временный доступ к заблокированному устройству.
  - Кнопка **Поддержка**. При нажатии на эту кнопку открывается окно **Поддержка**, в котором вы можете просмотреть информацию о приложении, а также создать файл трассировки приложения.
- В самой нижней части главного окна приложения отображается информация о лицензии и о ключе, а также о проблемах лицензирования (при их наличии). При нажатии кнопкой мыши на этой области окна открывается окно **Лицензии**, в котором отображается подробная информация о лицензии. По кнопке **Приобрести лицензию** в этом окне вы можете открыть веб-сайт интернет-магазина "Лаборатории Касперского", где вы можете приобрести лицензию. После приобретения лицензии вы получите код активации или файл ключа, с помощью которых вам нужно активировать приложение.

Для настройки графического интерфейса требуются права пользователя с ролью Администратор (admin). Некоторые элементы графического интерфейса могут быть недоступны пользователям с другими ролями.

Включение и выключение компонентов приложения

Вы можете включать и выключать компоненты приложения в графическом интерфейсе с помощью переключателя.

По умолчанию включены компоненты Защита от файловых угроз, Контроль устройств и Анализ поведения. Компонент Защита от веб-угроз может включаться автоматически, если на устройстве разрешено локальное управление параметрами защиты от веб-угроз (политика не применяется или "замок" в свойствах политики не установлен) и в системе обнаружен один из поддерживаемых браузеров.

Чтобы включить или выключить компонент приложения:

1. Откройте главное окно графического интерфейса приложения.
2. В нижней части главного окна нажмите на кнопку **Настройка**.

   Откроется окно **Настройка**.
3. Включите или выключите переключатель для нужного компонента.

Запуск и остановка задач проверки

Чтобы запустить или остановить задачу проверки:

1. Откройте главное окно графического интерфейса приложения.
2. В главном окне нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.
3. Выполните одно из следующих действий:

   - Если вы хотите запустить задачу проверки, нажмите на кнопку **Запустить**, расположенную под той задачей проверки, которую вы хотите запустить.

     Отобразится ход выполнения задачи проверки.

   - Если вы хотите остановить задачу проверки, нажмите на кнопку **Остановить**, расположенную под той задачей проверки, которую вы хотите остановить.

     Задача проверки остановится, отобразится информация о проверенных объектах и обнаруженных угрозах.
4. Если вы хотите просмотреть отчет по задаче проверки, нажмите на кнопку **Показать отчет**.

При обнаружении зараженного объекта или при завершении задачи проверки отображается всплывающее окно в области уведомлений рядом со значком приложения в правой части панели задач.

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}*). Вы можете скрыть информацию о выполненных временных задачах, нажав на крестик или закрыв окно **Проверка** (при переходе в главное окно или при выходе из приложения).

Запуск выборочной проверки и проверки в Sandbox

Вы можете запускать выборочную проверку файлов и директорий с помощью графического интерфейса.

Чтобы запустить выборочную проверку файла или директории:

1. Нажатием на правую кнопку мыши на файле/директории, проверку которого/которой вы хотите запустить, откройте контекстное меню.
2. Выберите приложение **Kaspersky Endpoint Security 12.4 для Linux** в качестве приложения для проверки файла или директории.

   В зависимости от среды рабочего стола названия пунктов контекстного меню могут отличаться.

Задача выборочной проверки и ход ее выполнения отобразятся в графическом интерфейсе.

Если включена интеграция приложения Kaspersky Endpoint Security с Sandbox, вы можете с помощью графического интерфейса отправить файл или директорию в Sandbox на проверку.

Чтобы отправить файл или директорию в Sandbox на проверку:

1. Нажатием на правую кнопку мыши на файле/директории, который/которую вы хотите отправить на проверку, откройте контекстное меню.
2. Выберите приложение **Kaspersky Endpoint Security 12.4 для Linux** в качестве приложения для проверки файла или директории.

   В зависимости от среды рабочего стола названия пунктов контекстного меню могут отличаться.
3. В открывшемся окне выберите вариант **Отправить на проверку в Sandbox**.

Запуск и остановка задачи обновления

Чтобы запустить или остановить задачу обновления:

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.

     При успешном завершении задачи обновления становится доступна ссылка **Откатить обновление**, с помощью которой вы можете откатить последнее успешное обновление баз.

- 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**.

Чтобы запустить задачу отката обновления:

1. Откройте главное окно графического интерфейса приложения.
2. В главном окне приложения нажмите на раздел **Обновление**.

   Откроется окно **Обновление**.
3. Запустите задачу отката обновления баз по ссылке **Откатить обновление**.

Настройка использования Kaspersky Security Network

Вы можете включать или выключать использование Kaspersky Security Network с помощью графического интерфейса.

Чтобы включить использование Kaspersky Security Network:

1. Откройте главное окно графического интерфейса приложения.
2. В нижней части главного окна нажмите на кнопку **Настройка**.

   Откроется окно **Настройка**.
3. В окне **Настройка** 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**.

   Откроется окно **Использование Kaspersky Security Network**.
5. В окне **Использование Kaspersky Security Network** внимательно прочитайте Положение о Kaspersky Security Network и выберите вариант **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Положения о Kaspersky Security Network**.
6. Нажмите **ОК**.

   Кнопка **ОК** недоступна, если в окне **Использование Kaspersky Security Network** не выбран ни один из вариантов.

Чтобы выключить использование Kaspersky Security Network:

1. Откройте главное окно графического интерфейса приложения.
2. В нижней части главного окна приложения нажмите на кнопку **Настройка**.

   Откроется окно **Настройка**.
3. Нажмите на кнопку **Выключить**.
4. В открывшемся окне нажмите на кнопку **Да**, чтобы отказаться от использования Kaspersky Security Network.

Просмотр отчетов

Вы можете просматривать отчеты о работе компонентов и задач приложения с помощью графического интерфейса. Отчеты отображаются в окне, которое открывается по кнопке **Отчеты**, расположенной в нижней части главного окна графического интерфейса приложения.

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.

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**. Этот отчет содержит статистические данные о работе компонента Защита от файловых угроз и о задачах проверки. Вы можете обновить отображаемый отчет, нажав на кнопку **Обновить**.
- **Системный аудит**. Этот отчет содержит информацию о событиях, которые произошли во время работы приложения и во время взаимодействия пользователя с приложением.
- **Защита от угроз**. Этот отчет содержит информацию 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-premise) и EDR Optimum.

Чтобы просмотреть отчет:

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, содержащий список событий.

   По умолчанию события в отчете отсортированы по возрастанию значений столбца **Дата**.
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.

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;
- просматривать выбранное событие в отдельном блоке.

Просмотр объектов резервного хранилища

Вы можете выполнять следующие действия с объектами резервного хранилища с помощью графического интерфейса:

- Просматривать информацию об объектах, помещенных в резервное хранилище на устройстве.
- Восстанавливать объекты из резервного хранилища в их исходные директории.
- Удалять объекты из резервного хранилища. Удаленные объекты восстановить невозможно.

Информация о восстановлении и удалении объектов записывается в журнал событий.

Чтобы просмотреть объекты в резервном хранилище:

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.

Управление лицензионными ключами

С помощью графического интерфейса вы можете добавлять и удалять лицензионные ключи приложения, а также просматривать информацию о лицензии, по которой используется приложение, и о связанном с лицензией ключе.

Для активации приложения Kaspersky Endpoint Security на защищенном устройстве требуется добавить основной лицензионный ключ в приложение.

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

Если основная лицензия, по которой вы используете приложение, не включает в себя нужную вам дополнительную функциональность приложения Kaspersky Endpoint Security, вам также требуется добавить в приложение лицензионный ключ для дополнительной функциональности:

- отдельный лицензионный ключ "Kaspersky Endpoint Detection and Response Optimum Add-on" (далее также "ключ EDR Optimum") – для активации компонента EDR Optimum;
- отдельный лицензионный ключ "Kaspersky Unified Monitoring and Analysis Platform Add-on" (далее также "ключ KUMA") – для активации функциональности Kaspersky Unified Monitoring and Analysis Platform;
- отдельный лицензионный ключ "Kaspersky Managed Detection and Response Optimum/Expert Add-on" (далее также "ключ MDR") – для активации функциональности компонента MDR.

Вы также можете добавить в приложение резервный ключ для основной функциональности и резервный ключ для дополнительной функциональности. Резервный ключ становится активным либо по истечении срока действия лицензии, связанной с активным ключом, либо при удалении активного ключа. Наличие резервного ключа позволяет избежать ограничения функциональности приложения в момент окончания срока действия лицензии.

Резервный ключ может быть добавлен только после добавления активного лицензионного ключа.

Добавление лицензионного ключа

Если приложение еще не активировано (не добавлен активный основной лицензионный ключ) вы можете активировать приложение по коммерческой лицензии или по пробной лицензии.

Чтобы активировать приложение:

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.

> Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

После активации приложения вы можете добавить резервный основной лицензионный ключ и, если требуется, активный и резервный ключи для дополнительной функциональности приложения. Процедуры добавления резервного основного ключа и ключей для дополнительной функциональности не отличаются.

Чтобы добавить в приложение резервный основной ключ или ключи для дополнительной функциональности:

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**.

Если вы добавляете основной лицензионный ключ, а приложение уже активировано, то новый ключ добавляется как резервный основной ключ.

Если вы добавляете отдельный ключ для дополнительной функциональности, то он добавляется как активный, если ранее в приложение не был добавлен ключ для этой дополнительной функциональности. Новый ключ для дополнительной функциональности добавляется как резервный, если в приложение уже добавлен ключ для этой дополнительной функциональности.

> Если в приложение ранее были добавлены и активный ключ, и резервный ключ, то новый ключ заменяет ранее добавленный резервный ключ.

Ключ для пробной лицензии и ключ по подписке не могут быть добавлены в качестве резервного ключа.

Удаление лицензионного ключа

Чтобы удалить лицензионный ключ, добавленный в приложение:

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**.
3. Нажмите на кнопку **Удалить**, расположенную справа от информации о ключе, который вы хотите удалить.
4. Подтвердите удаление в открывшемся окне.

Просмотр информации о лицензии

Чтобы просмотреть информацию о лицензии:

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 (активном основном ключе и активном ключе для дополнительной функциональности) 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 (резервном основном ключе и резервном ключе для дополнительной функциональности) 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.

Получение временного доступа к устройству

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**.

Просмотр информации о приложении

Вы можете просматривать информацию об установленном приложении и устройстве с установленным приложением в окне **Поддержка**, которое открывается по кнопке **Поддержка**, расположенной в нижней части главного окна графического интерфейса приложения.

В окне **Поддержка** отображается следующая информация:

- 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).

В нижней части окна **Поддержка** отображаются следующие ссылки:

- **Лицензии**, по которой открывается окно **Лицензии**, в котором отображается подробная информация о лицензии.
- **База знаний**, по которой открывается страница Базы знаний.
- **Поддержка**, по которой открывается страница Kaspersky CompanyAccount.
- **Трассировка**, по которой открывается окно **Трассировка**. В этом окне вы можете создавать файлы трассировки приложения и настраивать уровень детализации файлов трассировки.

  Для перехода по ссылке **Трассировка** требуются права пользователя с ролью Администратор (admin).

Создание файла трассировки

Вы можете создавать файлы трассировки приложения и настраивать уровень детализации файлов трассировки с помощью графического интерфейса.

Для создания и настройки уровня детализации файла трассировки требуются права пользователя с ролью Администратор (admin).

Чтобы создать файл трассировки:

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.

   Рекомендуется уточнить требуемый уровень детализации у специалистов Службы технической поддержки "Лаборатории Касперского". По умолчанию установлено значение **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/.

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. Имя файла манифеста для каждого компонента одно и тоже, но содержимое файлов манифестов различается. 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. Для запуска утилиты проверки целостности на устройствах с операционными системами Windows требуется учетная запись администратора.

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.
- Для проверки директории веб-плагина управления Kaspersky Endpoint Security:
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\server\plugins\kesl_<номер версии>\integrity_check.xml – на устройствах с операционными системами Windows;
  - /var/opt/kaspersky/ksc-web-console/server/plugins/kesl_<номер версии>/integrity_check.xml – на устройствах с операционными системами Linux.

Чтобы проверить целостность компонента решения, вам нужно запустить утилиту из папки расположения утилиты для этого компонента.

Чтобы запустить утилиту проверки целостности, выполните одну из следующих команд:

- для проверки целостности пакета приложения:

  ```
  integrity_checker [<путь к файлу манифеста>] --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
  ```

- для проверки целостности пакета графического пользовательского интерфейса:

  ```
  integrity_checker <путь к файлу манифеста> --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
  ```

- для проверки целостности MMC-плагина управления Kaspersky Endpoint Security:

  ```
  integrity_checker.exe [<путь к файлу манифеста>]
  ```

- для проверки целостности Агента администрирования:

  ```
  integrity_checker <путь к файлу манифеста>
  ```

- для проверки целостности директории веб-плагина управления Kaspersky Endpoint Security:

  ```
  integrity_checker <путь к файлу манифеста> --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds
  ```

  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 <директория>` – 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 <имя файла>`, где `<имя файла>` – имя файла, в который будут записываться события с уровнем детализации DEBUG, произошедшие во время проверки.
- `--signature-type kds` – тип проверяемой сигнатуры (этот параметр является обязательным для проверки директории веб-плагина управления Kaspersky Endpoint Security).
- `--signature-type kds-with-filename` – тип проверяемой сигнатуры (этот параметр является обязательным для проверки пакета приложения, пакета графического пользовательского интерфейса).
- `--single-file <файл>` – проверить только один файл, входящий в состав манифеста, остальные объекты манифеста игнорировать.
- `--version` – отобразить версию утилиты и не выполнять проверку целостности.

Вы можете просмотреть описание всех доступных параметров утилиты проверки целостности в справке параметров утилиты, выполнив команду `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.

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 Kaspersky Endpoint Security в течение жизненного цикла (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в 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.

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.

О файлах трассировки приложения

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 включили создание файлов трассировки приложения, по умолчанию файлы трассировки хранятся в директории /var/log/kaspersky/kesl/. Для доступа к этой директории требуются root-права.

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".

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.

Настройка параметров трассировки приложения

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.

Если вы управляете приложением через командную строку, вы можете настраивать параметры трассировки приложения в общих параметрах приложения.

Настройка параметров трассировки в Web Console

В Web Console вы можете настраивать параметры трассировки приложения в свойствах политики (**Параметры приложения** → **Общие настройки** → **Служба технической поддержки**).

Для применения параметров трассировки требуется перезапустить приложение.

Настройка параметров трассировки в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры трассировки приложения в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры приложения**).

В блоке **Параметры трассировки и записи дампов** по ссылке **Настроить** открывается окно, в котором вы можете настроить параметры трассировки (см. таблицу ниже).

Параметры трассировки приложения

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.

Параметр	Описание
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.

Для применения параметров трассировки требуется перезапустить приложение.

Настройка параметров трассировки в командной строке

В командной строке вы можете настраивать параметры трассировки приложения с помощью параметров `TraceLevel`, `TraceFolder`, `TraceMaxFileCount` и `TraceMaxFileSize` в общих параметрах приложения.

Параметр `TraceLevel` позволяет включить или выключить создание файлов трассировки приложения и указать уровень детализации файлов трассировки. Параметр может принимать следующие значения:

- `Detailed` – создавать детализированный файл трассировки.
- `MediumDetailed` – создавать файл трассировки, содержащий информационные сообщения и сообщения об ошибках.
- `NotDetailed` – создавать файл трассировки, содержащий сообщения об ошибках.
- `None` (значение по умолчанию) – не создавать файл трассировки.

Параметр `TraceFolder` позволяет указать директорию, в которой хранятся файлы трассировки приложения. Значение по умолчанию: /var/log/kaspersky/kesl. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись только для учетной записи, под которой работает Kaspersky Endpoint Security (права rwx-------- 700). Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права.

Параметр `TraceMaxFileCount` позволяет указать максимальное количество файлов трассировки приложения. Параметр может принимать значения от 1 до 10000. Значение по умолчанию: 10.

Параметр `TraceMaxFileSize` позволяет указать максимальный размер файла трассировки приложения (в мегабайтах). Параметр может принимать значения от 1 до 1000. Значение по умолчанию: 500.

Вы можете изменять значение параметров с помощью ключей командной строки или с помощью конфигурационного файла, который содержит все общие параметры приложения.

После изменения значений параметров `TraceFolder`, `TraceMaxFileCount`, `TraceMaxFileSize` требуется перезапустить приложение.

О файлах трассировки плагинов управления приложением

Автоматическая отправка файлов трассировки плагинов управления 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 плагинов управления

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.

Помимо общих данных файлы трассировки 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.

О файлах 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 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.

Настройка параметров записи дампов

Если вы управляете приложением Kaspersky Endpoint Security через Kaspersky Security Center, вы можете 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 конфигурационного файла kesl.ini.

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`.

Настройка параметров записи дампов в Web Console

В Web Console вы можете настраивать параметры записи дампов в свойствах политики (**Параметры приложения** → **Общие настройки** → **Служба технической поддержки**).

Параметры записи дампов в свойствах политики в Web Console описаны в Приложении 5.

Для применения параметров записи дампов требуется перезапустить приложение.

Настройка параметров записи дампов в Консоли администрирования

В Консоли администрирования вы можете настраивать параметры записи дампов в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры приложения**).

В блоке **Параметры трассировки и записи дампов** по ссылке **Настроить** открывается окно, в котором вы можете настроить параметры записи дампов (см. таблицу ниже).

Параметры записи дампов

Параметр	Описание
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.

Для применения параметров записи дампов требуется перезапустить приложение.

Настройка записи дампов в командной строке

Чтобы настроить запись дампов с помощью конфигурационного файла kesl.ini:

1. Остановите Kaspersky Endpoint Security.
2. Откройте файл /var/opt/kaspersky/kesl/common/kesl.ini на редактирование.
3. В секции **[General]** установите значение параметра:
   - `CoreDumps=yes` – включить запись дампов при сбое в работе приложения.
   - `CoreDumps=no` – выключить запись дампов.
4. Если вы хотите изменить директорию, в которой сохраняются файлы дампа по умолчанию, укажите путь к директории в параметре `CoreDumpsPath`.
5. Запустите Kaspersky Endpoint Security.

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 закладке **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 закладке **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 закладку **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. 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 <префикс группы команд>
```

где <префикс группы команд> может принимать следующие значения:

- -A – команды управления контролем приложений.
- -B – команды управления резервным хранилищем.
- -C – команды управления общими параметрами проверки контейнеров (Проверка контейнеров, Мониторинг контейнеров).
- -D – команды управления контролем устройств.
- -E – команды управления событиями приложения (Просмотр событий в командной строке, Просмотр событий в Kaspersky Security Center).
- -F – команды управления сетевым экраном.
- -H – команды управления заблокированными устройствами.
- -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 сетевого трафика.
- -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 (on-premise) и 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 для защиты виртуальных сред.
- -W – команды вывода событий (Просмотр событий в командной строке, Просмотр событий в Kaspersky Security Center).
- -X – команды управления параметрами интеграции приложения Kaspersky Endpoint Security с Sandbox.

Команды управления параметрами и задачами приложения

-T – префикс, указывающий, что команда принадлежит к группе команд управления параметрами и задачами приложения.

-C – префикс, указывающий, что команда принадлежит к группе команд управления общими параметрами проверки контейнеров (Проверка контейнеров, Мониторинг контейнеров).

-N – префикс, указывающий, что команда принадлежит к группе команд управления параметрами проверки сетевого трафика.

Команда 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).

Синтаксис команды

```
kesl-control [-T] --export-settings [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, в который будут сохранены параметры приложения.

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

Команда kesl-control --import-settings

Команда позволяет импортировать из конфигурационного файла все параметры приложения (включая общие параметры проверки контейнеров, параметры проверки защищенных соединений, общие параметры приложения и параметры задач).

Синтаксис команды

```
kesl-control [-T] --import-settings --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – 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.

Команда kesl-control --update-application

Команда позволяет установить загруженное обновление модулей приложения.

> Команда не может быть выполнена, если приложение используется в режиме Легкого агента.

Синтаксис команды

```
kesl-control [-T] --update-application
```

Команды управления общими параметрами приложения

Команда kesl-control --get-app-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения общих параметров приложения.

Синтаксис команды

```
kesl-control [-T] --get-app-settings [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – 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. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kesl-control --set-app-settings

Команда позволяет устанавливать значения общих параметров приложения с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kesl-control [-T] --set-app-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kesl-control [-T] --set-app-settings --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`<имя параметра>=<значение параметра>` – имя и значение одного из общих параметров приложения.

`--file <путь к конфигурационному файлу>` – 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

Команда kesl-control --get-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения параметров указанной задачи.

Синтаксис команды

```
kesl-control [-T] --get-settings <идентификатор/имя задачи> [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`--file <путь к конфигурационному файлу>` – 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. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kesl-control --set-settings

Команда позволяет устанавливать значения параметров указанной задачи с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kesl-control [-T] --set-settings <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>] [--add-path <путь>] [--del-path <путь>] [--add-exclusion <путь>] [--del-exclusion <путь>]
```

Задать параметры с помощью конфигурационного файла:

```
kesl-control [-T] --set-settings <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`<имя параметра>=<значение параметра>` – имя и значение одного из параметров задачи.

`--add-path <путь>` – добавить путь к директории с проверяемыми объектами.

`--del-path <путь>` – удалить путь к директории с проверяемыми объектами.

`--add-exclusion <путь>` – добавить путь к директории с объектами, которые нужно исключить из проверки.

`--del-exclusion <путь>` – удалить путь к директории с исключаемыми объектами.

`--file <путь к конфигурационному файлу>` – 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.

Команда kesl-control --set-to-default

Команда позволяет восстановить значения по умолчанию для параметров указанной задачи.

Синтаксис команды

```
kesl-control [-T] --set-settings <идентификатор/имя задачи> --set-to-default
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда kesl-control --get-schedule

Команда позволяет вывести в консоль или в конфигурационный файл текущее расписание запуска указанной задачи.

Синтаксис команды

```
kesl-control [-T] --get-schedule <идентификатор/имя задачи> [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`--file <путь к конфигурационному файлу>` – 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. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда kesl-control --set-schedule

Команда позволяет устанавливать расписание указанной задачи с помощью ключей команды или путем импорта параметров из указанного конфигурационного файла.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kesl-control [-T] --set-schedule <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kesl-control [-T] --set-schedule <идентификатор/имя задачи> --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

<идентификатор/имя задачи> – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

<имя параметра>=<значение параметра> – имя и значение одного из параметров расписания задач.

--file <путь к конфигурационному файлу> – 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

Команда kesl-control --get-task-list

Команда позволяет вывести список существующих задач приложения.

Синтаксис команды

```
kesl-control [-T] --get-task-list [--json]
```

Аргументы и ключи

--json – выводить параметры в формате JSON.

Команда kesl-control --get-task-state

Команда позволяет вывести состояние указанной задачи.

Синтаксис команды

```
kesl-control [-T] --get-task-state <идентификатор/имя задачи> [--json]
```

Аргументы и ключи

<идентификатор/имя задачи> – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`--json` – выводить параметры в формате JSON.

Команда kesl-control --create-task

Команда позволяет создать задачу указанного типа с параметрами по умолчанию или с параметрами, указанными в конфигурационном файле.

Синтаксис команды

Создать задачу с параметрами по умолчанию:

```
kesl-control [-T] --create-task <имя задачи> --type <тип задачи>
```

Создать задачу с параметрами из конфигурационного файла:

```
kesl-control [-T] --create-task <имя задачи> --type <тип задачи> [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`<имя задачи>` – имя, которое вы задаете для новой задачи.

`<тип задачи>` – обозначение типа создаваемой задачи.

`--file <путь к конфигурационному файлу>` – 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.

Команда kesl-control --delete-task

Команда позволяет удалить задачу.

Синтаксис команды

```
kesl-control [-T] --delete-task <идентификатор/имя задачи>
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда kesl-control --start-task

Команда позволяет запустить задачу.

Синтаксис команды

```
kesl-control [-T] --start-task <идентификатор/имя задачи> [-W] [--progress]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`[-W]` – включить вывод текущих событий.

`[--progress]` – отображать ход выполнения задачи.

Команда kesl-control --stop-task

Команда позволяет остановить задачу.

Синтаксис команды

```
kesl-control [-T] --stop-task <идентификатор/имя задачи> [-W]
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

`[-W]` – включить вывод текущих событий.

Команда kesl-control --suspend-task

Команда позволяет приостановить задачу.

Синтаксис команды

```
kesl-control [-T] --suspend-task <идентификатор/имя задачи>
```

Аргументы и ключи

`<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда kesl-control --resume-task

Команда позволяет возобновить выполнение задачи.

Синтаксис команды

```
kesl-control [-T] --resume-task <идентификатор/имя задачи>
```

Аргументы и ключи

<идентификатор/имя задачи> – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.

Команда kesl-control --scan-file

Команда позволяет создать и запустить задачу выборочной проверки.

Синтаксис команды

```
kesl-control [-T] --scan-file <путь> [--action <действие>]
```

Аргументы и ключи

<путь> – путь к файлу или директории, которые нужно проверить. Вы можете указать несколько путей, разделяя их пробелами.

`--action <действие>` – действие, которое приложение будет выполнять над зараженными объектами. Если вы не укажете ключ `--action`, приложение будет выполнять рекомендуемое действие.

Команда kesl-control --scan-container

Команда позволяет создать и запустить задачу выборочной проверки контейнера или образа.

Синтаксис команды

```
kesl-control [-T] --scan-container <идентификатор/имя[:тег]>
```

Аргументы и ключи

<идентификатор/имя[:тег]> – имя или идентификатор контейнера или образа. Для проверки нескольких объектов можно использовать **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 запретом запуска объектов

Команда kesl-control --get-prevention-state

Команда позволяет вывести в консоль правила запрета запуска объектов указанного компонента.

Синтаксис команды

```
kesl-control [-T] --get-prevention-state [--kata|--edro]
```

Аргументы и ключи

`--kata` – правила запрета запуска объектов компонента EDR Expert (on-premise).

`--edro` – правила запрета запуска объектов компонента EDR Optimum.

Команды управления общими параметрами проверки контейнеров

Команда kesl-control --get-container-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения общих параметров проверки контейнеров.

Синтаксис команды

```
kesl-control [-C] --get-container-settings [--file <путь к конфигурационному файлу>] [--
json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – 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. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда 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.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kesl-control [-C] --set-container-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kesl-control [-C] --set-container-settings --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`<имя параметра>=<значение параметра>` – имя и значение одного из общих параметров проверки контейнеров.

`--file <путь к конфигурационному файлу>` – 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, указывающий, что команда принадлежит к группе команд управления параметрами проверки сетевого трафика.

Команда 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.

Синтаксис команды

```
kesl-control -N --query user

kesl-control -N --query auto
```

```
kesl-control -N --query kl
```

Команда kesl-control --clear-web-auto-excluded

Команда позволяет очистить список доменов, которые приложение автоматически исключило из проверки.

Синтаксис команды

```
kesl-control -N --clear-web-auto-excluded
```

Команда kesl-control --get-net-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения параметров проверки сетевого трафика.

Синтаксис команды

```
kesl-control [-N] --get-net-settings [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – 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. Если вы не укажете ключ `--json`, параметры будут выведены в формате INI.

Команда 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.

Синтаксис команды

Задать параметры с помощью ключей команды:

```
kesl-control [-N] --set-net-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kesl-control [-N] --set-net-settings --file <путь к конфигурационному файлу> [--json]
```

Аргументы и ключи

`<имя параметра>=<значение параметра>` – имя и значение одного из параметров проверки сетевого трафика.

`--file <путь к конфигурационному файлу>` – 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.

Команда kesl-control --list-certificates

Команда позволяет вывести список доверенных корневых сертификатов.

Синтаксис команды

```
kesl-control [-N] --list-certificates
```

Команда kesl-control --add-certificate

Команда позволяет добавить сертификат в список доверенных корневых сертификатов.

Синтаксис команды

```
kesl-control [-N] --add-certificate <путь к сертификату>
```

Аргументы и ключи

`<путь к сертификату>` – путь к файлу сертификата, который вы хотите добавить, в формате PEM или DER.

Команда kesl-control --remove-certificate

Команда позволяет удалить сертификат из списка доверенных корневых сертификатов.

Синтаксис команды

```
kesl-control [-N] --remove-certificate <субъект сертификата>
```

Команда kesl-control --add-bypass-endpoints

Команда позволяет добавить исключение из перехвата трафика.

Синтаксис команды

```
kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip <удаленный IP-адрес> --dst-port <порт назначения>
```

Аргументы и ключи

`<in|out>` – направление трафика в исключаемом соединении: входящий или исходящий.

`<удаленный IP-адрес>` – 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.

`<порт назначения>` – порт на защищенном устройстве (исключение для входящего трафика) или порт на удаленном устройстве (исключение для исходящего трафика). Трафик на этот порт исключается из перехвата.

Команда kesl-control --list-bypass-endpoints

Команда позволяет просмотреть список настроенных исключений из перехвата трафика.

Синтаксис команды

```
kesl-control [-N] --list-bypass-endpoints
```

Команда kesl-control --remove-bypass-endpoints

Команда позволяет удалить исключение из перехвата трафика.

Синтаксис команды

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <удаленный IP-адрес> --dst-port <порт назначения>
```

Аргументы и ключи

`<in|out>` – направление трафика в исключаемом соединении: входящий или исходящий.

`<удаленный IP-адрес>` – адрес удаленного устройства в формате IPv4 или IPv6, трафик на который или с которого исключается из перехвата (в зависимости от направления трафика).

`<порт назначения>` – порт на защищенном устройстве (исключение для входящего трафика) или порт на удаленном устройстве (исключение для исходящего трафика).

Команды статистики

-S – префикс указывающий, что команда принадлежит к группе команд статистики.

Команда kesl-control --app-info

Команда позволяет вывести информацию о приложении.

Синтаксис команды

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

Аргументы и ключи

`--json` – выводить параметры в формате JSON.

Команда 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.

Синтаксис команды

```
kesl-control [-S] --supported-tech-info [--json]
```

Аргументы и ключи

`--json` – выводить функции в формате JSON.

Команда kesl-control --get-statistic

Команда позволяет вывести статистику о работе приложения и список точек монтирования, обнаруженных на устройстве.

Синтаксис команды

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

Аргументы и ключи

`[--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.

Команда kesl-control --omsinfo

Команда позволяет создать файл формата JSON для интеграции с Microsoft Operations Management Suite.

Синтаксис команды

```
kesl-control [-S] --omsinfo --file <путь к файлу>
```

Команды вывода событий

Команда 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.

Синтаксис команды

```
kesl-control -W [--query "<условия фильтра>"]
```

Аргументы и ключи

`<условия фильтра>` – одно или несколько логических выражений в формате `<поле> <операция сравнения> '<значение>'`, скомбинированных с помощью логического оператора `and`, для вывода определенных текущих событий.

Команды управления событиями приложения

-E – префикс, указывающий, что команда принадлежит к группе команд управления событиями приложения (Просмотр событий в командной строке, Просмотр событий в Kaspersky Security Center).

Команда 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.

Синтаксис команды

```
kesl-control -E
```

Команда 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.

Синтаксис команды

```
kesl-control -E --query "<условия фильтра>" [--db <файл базы данных>] [-n <количество>]
[--file <путь к файлу>] [--json] [--reverse]
```

Аргументы и ключи

`<файл базы данных>` – 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`.

`<условия фильтра>` – одно или несколько логических выражений в формате `<поле> <операция сравнения> '<значение>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.

`<количество>` – количество последних событий из выборки (то есть количество записей от конца выборки), которые нужно вывести.

`--file <путь к файлу>` – 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).

Команды управления лицензионными ключами

-L – префикс, указывающий, что команда принадлежит к группе команд управления лицензионными ключами.

Команды добавления и удаления лицензионных ключей могут быть выполнены, только если приложение используется в стандартном режиме или в режиме Агента Endpoint Detection and Response. Если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред, команды управления лицензионными ключами завершаются с ошибкой. Вы активируете приложение в составе решения Kaspersky Security для виртуальных сред Легкий агент, отдельно активировать приложение не требуется.

Команда 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 как основные лицензионные ключи приложения, так и лицензионные ключи для дополнительной функциональности. Указывать тип ключа в команде не требуется.

Синтаксис команды

```
kesl-control [-L] --add-active-key <путь к файлу ключа>

kesl-control [-L] --add-active-key <код активации>
```

Аргументы и ключи

<путь к файлу ключа> – путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.

<код активации> – код активации.

Пример:
Добавить ключ с помощью файла /home/test/00000001.key в качестве активного ключа:

```
kesl-control --add-active-key /home/test/00000001.key
```

Команда 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 как основные лицензионные ключи приложения, так и лицензионные ключи для дополнительной функциональности. Указывать тип ключа в команде не требуется.

Если активный ключ еще не добавлен в приложение на устройстве, команда завершается с ошибкой.

Синтаксис команды

```
kesl-control [-L] --add-reserve-key <путь к файлу ключа>

kesl-control [-L] --add-reserve-key <код активации>
```

Аргументы и ключи

<путь к файлу ключа> – путь к файлу ключа. Если файл ключа находится в текущей директории, достаточно указать только имя файла.

<код активации> – код активации.

Пример:
Добавить резервный ключ с помощью файла /home/test/00000002.key:

```
kesl-control --add-reserve-key /home/test/00000002.key
```

Команда kesl-control --remove-active-key

Команда позволяет удалить активный лицензионный ключ.

Синтаксис команды

```
kesl-control [-L] --remove-active-key [--edr-optimum]

kesl-control [-L] --remove-active-key [--kuma]

kesl-control [-L] --remove-active-key [--mdr]

kesl-control [-L] --remove-active-key [--edr-kata]
```

Аргументы и ключи

`--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-premise).

Если в команде вы не укажете ключ `--edr-optimum`, `--kuma`, `--mdr` или `--edr-kata`, в результате выполнения команды из приложения будет удален основной активный ключ.

Команда kesl-control --remove-reserve-key

Команда позволяет удалить резервный лицензионный ключ.

Синтаксис команды

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]

kesl-control [-L] --remove-reserve-key [--kuma]

kesl-control [-L] --remove-reserve-key [--mdr]

kesl-control [-L] --remove-reserve-key [--edr-kata]
```

Аргументы и ключи

`--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-premise).

Если в команде вы не укажете ключ `--edr-optimum`, `--kuma`, `--mdr` или `--edr-kata`, в результате выполнения команды из приложения будет удален основной резервный ключ.

Команда kesl-control -L --query

Команда `-L --query` позволяет вывести информацию о лицензии, по которой активировано приложение, и об используемых лицензионных ключах.

Синтаксис команды

```
kesl-control -L --query [--json]
```

Аргументы и ключи

`--json` – выводить данные в формате JSON.

Команда kesl-control --load-mdr-blob

Команда `--load-mdr-blob` 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.

Синтаксис команды

```
kesl-control [-L] --load-mdr-blob <путь к файлу MDR BLOB>
```

Команда kesl-control --remove-mdr-blob

Команда `--remove-mdr-blob` позволяет удалить с устройства файл BLOB, который может использоваться при интеграции с Kaspersky Managed Detection and Response.

Синтаксис команды

```
kesl-control [-L] --remove-mdr-blob
```

Команды управления сетевым экраном

-F – префикс, указывающий, что команда принадлежит к группе команд управления сетевым экраном.

Команда kesl-control --add-rule

Команда позволяет добавить новое сетевое пакетное правило.

Синтаксис команды

```
kesl-control [-F] --add-rule [--name <название правила>] [--action <действие>] [--protocol <протокол>] [--direction <направление>] [--remote <удаленный адрес>[:<диапазон портов>]] [--local <локальный адрес>[:<диапазон портов>]] [--at <индекс>]
```

Аргументы и ключи

`--name <название правила>` – название сетевого пакетного правила.

`--action <действие>` – действие, применяемое к соединениям, указанным в сетевом пакетном правиле.

`--protocol <протокол>` – тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность.

`--direction <направление>` – направление отслеживаемой сетевой активности.

`--remote <удаленный адрес>[:<диапазон портов>]` – сетевой адрес удаленного устройства.

`--local <локальный адрес>[:<диапазон портов>]` – сетевой адрес устройства с установленным приложением Kaspersky Endpoint Security.

`--at <индекс>` – 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.

Команда kesl-control --del-rule

Команда позволяет удалить сетевое пакетное правило с указанным названием или с указанным индексом в списке правил.

Синтаксис команды

```
kesl-control [-F] --del-rule --name <название правила>

kesl-control [-F] --del-rule --index <индекс>
```

Аргументы и ключи

`--name <название правила>` – название сетевого пакетного правила.

`--index <индекс>` – порядковый номер правила в списке сетевых пакетных правил.

Команда kesl-control --move-rule

Команда позволяет изменить приоритет выполнения сетевого пакетного правила.

Синтаксис команды

```
kesl-control [-F] --move-rule --name <название правила> --at <индекс>

kesl-control [-F] --move-rule --index <индекс> --at <индекс>
```

Аргументы и ключи

`--name <название правила>` – название сетевого пакетного правила.

`--index <индекс>` – текущий порядковый номер правила в списке сетевых пакетных правил.

`--at <индекс>` – новый порядковый номер правила в списке сетевых пакетных правил.

Команда kesl-control --add-zone

Команда позволяет добавить адрес в сетевую зону.

Синтаксис команды

```
kesl-control [-F] --add-zone --zone <зона> --address <адрес>
```

Аргументы и ключи

`--zone <зона>` – предустановленное имя сетевой зоны.

`--address <адрес>` – сетевой адрес или подсеть.

Команда kesl-control --del-zone

Команда позволяет удалить адрес из сетевой зоны.

Синтаксис команды

```
kesl-control [-F] --del-zone --zone <зона> --address <адрес>

kesl-control [-F] --del-zone --zone <зона> --index <индекс адреса>
```

Аргументы и ключи

`--zone <зона>` – предустановленное имя сетевой зоны.

`--address <адрес>` – сетевой адрес или подсеть.

`--index <индекс адреса>` – порядковый номер адреса в сетевой зоне.

Команда kesl-control -F --query

Команда позволяет посмотреть правила сетевого экрана, созданные с помощью приложения Kaspersky Endpoint Security.

Синтаксис команды

```
kesl-control -F --query
```

Команды управления заблокированными устройствами

-H –префикс, указывающий, что команда принадлежит к группе команд управления устройствами, заблокированными Защитой от шифрования и Защитой от сетевых угроз.

Команда kesl-control --get-blocked-hosts

Команда позволяет вывести в консоль список заблокированных устройств.

Синтаксис команды

```
kesl-control [-H] --get-blocked-hosts
```

Команда kesl-control --allow-hosts

Команда позволяет разблокировать заблокированные устройства.

Синтаксис команды

```
kesl-control [-H] --allow-hosts <адрес>
```

Аргументы и ключи

<адрес> – 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 Контролем устройств

-D – префикс, указывающий, что команда принадлежит к группе команд управления контролем устройств.

Команда kesl-control --get-device-list

Команда позволяет вывести в консоль список устройств, которые установлены на клиентском устройстве или подключены к нему, и экспортировать список подключенных устройств в файл в формате JSON.

Синтаксис команды

```
kesl-control [-D] --get-device-list [--all] [--json] [--export <файл>]
```

Аргументы и ключи

`--all` – выводить список всех подключенных устройств.

`--json` – выводить список подключенных устройств в формате JSON.

`--export <файл>` – экспортировать список подключенных устройств в файл в формате списка доверенных устройств. Вам нужно указать полный путь к файлу в формате JSON.

Команда kesl-control --trusted-devices

Команда позволяет просматривать список доверенных устройств, добавлять в него устройства и удалять из него устройства, а также импортировать список доверенных устройств из файла.

Синтаксис команды

```
kesl-control [-D] --trusted-devices [--list] [--add <идентификатор>] [--delete
<идентификатор>] [--merge|--add|--replace --file <файл>]
```

Аргументы и ключи

`--list` – вывести список доверенных устройств.

`--add <идентификатор>` – добавить устройство в список доверенных устройств по идентификатору или маске идентификатора устройства.

`--delete <идентификатор>` – удалить устройство из списка доверенных устройств по идентификатору или маске идентификатора устройства.

`--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 <файл>` – импортировать список доверенных устройств из указанного файла. Вам нужно указать полный путь к файлу в формате JSON.

Команда kesl-control --request-temporary-device-access

Команда позволяет создать файл запроса доступа, чтобы запросить временный доступ к заблокированному устройству.

Синтаксис команды

```
kesl-control [-D] --request-temporary-device-access --device-id <идентификатор устройства> --access-duration <длительность доступа> --path <путь к файлу запроса доступа>
```

Аргументы и ключи

`--device-id <идентификатор устройства>` – идентификатор заблокированного устройства, к которому вы хотите получить доступ.

`--access-duration <длительность доступа>` – период времени, на который вы хотите получить доступ к устройству (в часах). Возможные значения: 1–100.

`--path <путь к файлу запроса доступа>` – путь к директории, в которой вы хотите сохранить файл запроса доступа с расширением .akey.

Команда kesl-control --upload-temporary-device-access-key

Команда позволяет загрузить ключ доступа, чтобы получить временный доступ к заблокированному устройству.

Синтаксис команды

```
kesl-control [-D] --upload-temporary-device-access-key --path <путь к файлу с ключом доступа>
```

Аргументы и ключи

`--path <путь к файлу с ключом доступа>` – путь к файлу с ключом доступа к устройству (файлу с расширением .acode).

Команды управления Контролем приложений

-A – префикс, указывающий, что команда принадлежит к группе команд управления контролем приложений.

Команда kesl-control --get-app-list

Команда позволяет вывести список приложений, обнаруженных на клиентском устройстве во время выполнения задачи Инвентаризация.

Синтаксис команды

```
kesl-control [-A] --get-app-list [--json]
```

Аргументы и ключи

`--json` – выводить данные в формате JSON.

Команда kesl-control --get-categories

Команда позволяет вывести список созданных категорий контроля приложений.

Синтаксис команды

```
kesl-control [-A] --get-categories [--names <название категории 1> <название категории 2> ... <название категории N>] [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`<название категории 1> <название категории 2> ... <название категории N>` – названия категорий, информацию о которых вы хотите просмотреть. Если вы хотите просмотреть информацию о нескольких категориях, укажите названия категорий через пробел.

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу формата JSON, в который будут выведены параметры.

`--json` – выводить данные в формате JSON.

Команда kesl-control --set-categories

Команда позволяет создать или изменить список созданных категорий контроля приложений.

Синтаксис команды

```
kesl-control [-A] --set-categories [--names <название категории 1> <название категории 2> ... <название категории N>] --file <путь к конфигурационному файлу>
```

Аргументы и ключи

`<название категории 1> <название категории 2> ... <название категории 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 укажите название категории, она будет удалена из списка.

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу с параметрами категорий.

Команда kesl-control --get-settings 21

Команда позволяет вывести список созданных правил контроля приложений.

Синтаксис команды

```
kesl-control --get-settings 21 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, в который будут выведены параметры.

`--json` – выводить данные в формате JSON.

Команда kesl-control --set-settings 21

Команда позволяет изменить список созданных категорий приложений и правил контроля приложений.

Синтаксис команды

```
kesl-control --set-settings 21 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры.

`--json` – импорт данных из файла в формате JSON.

Команда kesl-control --set-to-default 21

Команда позволяет удалить список категорий приложений и правил контроля приложений.

Синтаксис команды

```
kesl-control --set-settings 21 --set-to-default
```

Команды управления Веб-Контролем

Команда kesl-control --get-settings 26

Команда позволяет вывести список настроенных параметров Веб-Контроля.

Синтаксис команды

```
kesl-control --get-settings 26 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, в который будут выведены параметры.

`--json` – выводить данные в формате JSON.

Команда kesl-control --set-settings 26

Команда позволяет изменить список настроенных параметров Веб-Контроля.

Синтаксис команды

```
kesl-control --set-settings 26 [--file <путь к конфигурационному файлу>] [--json]
```

Аргументы и ключи

`--file <путь к конфигурационному файлу>` – полный путь к конфигурационному файлу, из которого будут импортированы параметры.

`--json` – импорт данных из файла в формате JSON.

Команда kesl-control --set-to-default 26

Команда позволяет удалить настроенные параметры и восстановить значения параметров Веб-Контроля до правила по умолчанию.

Синтаксис команды

```
kesl-control --set-settings 26 --set-to-default
```

Команды управления резервным хранилищем

-B – префикс, указывающий, что команда принадлежит к группе команд управления резервным хранилищем.

Команда kesl-control -B --mass-remove

Команда позволяет удалить из резервного хранилища все или только указанные объекты.

Синтаксис команды

Удалить все объекты:

```
kesl-control -B --mass-remove
```

Удалить объекты, соответствующие условиям фильтра:

```
kesl-control -B --mass-remove --query "< условия фильтра >"
```

Аргументы и ключи

`< условия фильтра >` – одно или несколько логических выражений в формате `< поле > < операция сравнения > '< значение >'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.

Команда kesl-control -B --query

Команда позволяет вывести информацию об объектах резервного хранилища.

Синтаксис команды

Вывести информацию обо всех объектах резервного хранилища:

```
kesl-control -B --query [-n < количество >] [--json] [--reverse]
```

Вывести информацию об объектах резервного хранилища, соответствующих условиям фильтра:

```
kesl-control -B --query ["<условия фильтра>"] [-n <количество>] [--json] [--reverse]
```

Аргументы и ключи

`<условия фильтра>` – 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 объектах резервного хранилища.

`<количество>` – количество последних объектов из хранилища, которые нужно вывести. Если вы не укажете ключ `-n`, будут выведены последние 30 объектов. Для отображения всех объектов укажите значение 0.

`--json` – выводить данные в формате JSON.

`--reverse` – выводить объекты в обратном порядке (от самого нового объекта наверху к более старым внизу).

Команда kesl-control -B --restore

Команда позволяет восстановить объект из резервного хранилища.

Синтаксис команды

```
kesl-control -B --restore <идентификатор объекта> [--file <путь к файлу>]
```

Аргументы и ключи

`<идентификатор объекта>` – идентификатор объекта в резервном хранилище.

`--file <путь к файлу>` – новое имя файла и путь к директории, в которой его требуется сохранить. Если вы не укажете ключ `--file`, объект будет восстановлен с исходным именем в исходное местоположение.

Команды управления карантином

-Q – префикс, указывающий, что команда принадлежит к группе команд управления карантином.

Команда kesl-control -Q --mass-remove

Команда позволяет удалить из карантина все или только указанные файлы.

Синтаксис команды

Удалить все файлы:

```
kesl-control -Q --mass-remove
```

Удалить файлы, соответствующие условиям фильтра:

```
kesl-control -Q --mass-remove --query "<условия фильтра>"
```

Аргументы и ключи

`<условия фильтра>` – одно или несколько логических выражений в формате `<поле> <операция сравнения> '<значение>'`, скомбинированных с помощью логического оператора `and`, для ограничения результатов запроса.

Команда 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.

Синтаксис команды

```
kesl-control [-Q] --put <путь к файлу> [--md5] [--sha256] [--save-original-file]
```

Аргументы и ключи

`<путь к файлу>` – 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.

Команда kesl-control -Q --query

Команда позволяет вывести информацию о файлах на карантине.

Синтаксис команды

Вывести информацию обо всех файлах на карантине:

```
kesl-control -Q --query [-n <количество>] [--json]
```

Вывести информацию о файлах на карантине, соответствующих условиям фильтра:

```
kesl-control -Q --query ["<условия фильтра>"] [-n <количество>]
```

Аргументы и ключи

< условия фильтра > – 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.

< количество > – 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.

Команда kesl-control -Q --restore

Команда позволяет восстановить файл из карантина.

Синтаксис команды

```
kesl-control -Q --restore < идентификатор файла > [--file < путь к файлу >]
```

Аргументы и ключи

< идентификатор файла > – идентификатор файла на карантине.

--file < путь к файлу > – 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 пользователями и ролями

-U – префикс, указывающий, что команда принадлежит к группе команд управления пользователями и ролями.

Команда kesl-control --get-user-list

Команда позволяет вывести список пользователей и ролей.

Синтаксис команды

```
kesl-control [-U] --get-user-list
```

Команда kesl-control --grant-role

Команда позволяет назначить роль определенному пользователю.

Синтаксис команды

```
kesl-control [-U] --grant-role <роль> <пользователь>
```

Команда kesl-control --revoke-role

Команда позволяет отозвать роль у определенного пользователя.

Синтаксис команды

```
kesl-control [-U] --revoke-role <роль> <пользователь>
```

Команды управления компонентом EDR Expert (on-premise)

-R – префикс, указывающий, что команда принадлежит к группе команд управления параметрами интеграции с Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (on-premise) и Kaspersky Endpoint Detection and Response Optimum.

Команда 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).

Синтаксис команды

```
kesl-control [-R] --add-kataedr-server-certificate <файл> [--server-type
<response|telemetry>]
```

Аргументы и ключи

<файл> – путь к файлу, содержащему сертификат сервера.

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (OSMP) 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`.

Команда 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).

Синтаксис команды

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type
<response|telemetry>]
```

Аргументы и ключи

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (OSMP) 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`.

Команда 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).

Синтаксис команды

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

Аргументы и ключи

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (OSMP) 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`.

Команда 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).

Синтаксис команды

```
kesl-control [-R] --add-kataedr-client-certificate <файл> [--server-type
<response|telemetry>]
```

Аргументы и ключи

< файл > – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (OSMP) 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`.

Команда 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).

Синтаксис команды

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type
<response|telemetry>]
```

Аргументы и ключи

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (OSMP) 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`.

Команда 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).

Синтаксис команды

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

Аргументы и ключи

`--server-type <response|telemetry>` – при интеграции в режиме EDR Expert (OSMP) 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 NDR (KATA)

-R – префикс, указывающий, что команда принадлежит к группе команд управления параметрами интеграции с Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (on-premise) и Kaspersky Endpoint Detection and Response Optimum.

Команда kesl-control --add-katandr-server-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат сервера NDR.

Синтаксис команды

```
kesl-control [-R] --add-katandr-server-certificate <файл>
```

Аргументы и ключи

< файл > – путь к файлу, содержащему сертификат сервера.

Команда kesl-control --remove-katandr-server-certificate

Команда позволяет удалить сертификат сервера NDR.

Синтаксис команды

```
kesl-control [-R] --remove-katandr-server-certificate
```

Команда kesl-control --query-katandr-server-certificate

Команда позволяет вывести информацию о сертификате сервера NDR.

Синтаксис команд

```
kesl-control [-R] --query-katandr-server-certificate
```

Команда kesl-control --add-katandr-client-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат клиента, используемый для защиты подключения к серверу NDR.

Синтаксис команды

```
kesl-control [-R] --add-katandr-client-certificate <файл>
```

Аргументы и ключи

<файл> – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

Команда kesl-control --remove-katandr-client-certificate

Команда позволяет удалить сертификат клиента, используемый для защиты подключения к серверу NDR.

Синтаксис команды

```
kesl-control [-R] --remove-katandr-client-certificate
```

Команда kesl-control --query-katandr-client-certificate

Команда позволяет вывести информацию о сертификате клиента.

Синтаксис команды

```
kesl-control [-R] --query-katandr-client-certificate
```

Команды управления сетевой изоляцией устройства

-R – префикс, указывающий, что команда принадлежит к группе команд управления параметрами интеграции с Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (on-premise) и Kaspersky Endpoint Detection and Response Optimum. Сетевая изоляция устройств применяется как действие по реагированию на обнаружение угрозы при интеграции с указанными решениями Detection and Response.

Команда kesl-control --isolation-stat

Команда позволяет вывести в консоль текущее состояние сетевой изоляции: включена или выключена.

Синтаксис команды

```
kesl-control [-R] --isolation-stat
```

Команда kesl-control --isolation-off

Команда позволяет временно выключить сетевую изоляцию устройства.

Синтаксис команды

```
kesl-control [-R] --isolation-off
```

Команды управления параметрами интеграции с KUMA

-M – префикс, указывающий, что команда принадлежит к группе команд управления параметрами интеграции с Kaspersky Unified Monitoring and Analysis Platform.

Команда kesl-control --add-kuma-server-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат сервера KUMA.

Синтаксис команды

```
kesl-control [-M] --add-kuma-server-certificate <путь к файлу>
```

Аргументы и ключи

`<путь к файлу>` – путь к файлу, содержащему сертификат сервера.

Команда kesl-control --remove-kuma-server-certificate

Команда позволяет удалить сертификат сервера KUMA.

Синтаксис команды

```
kesl-control [-M] --remove-kuma-server-certificate
```

Команда kesl-control --query-kuma-server-certificate

Команда позволяет вывести информацию о сертификате сервера KUMA.

Синтаксис команды

```
kesl-control [-M] --query-kuma-server-certificate
```

Команда kesl-control --add-kuma-client-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат клиента, используемый для защиты подключения к серверу KUMA.

Синтаксис команды

```
kesl-control [-M] --add-kuma-client-certificate <путь к файлу>
```

Аргументы и ключи

<путь к файлу> – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

Команда kesl-control --remove-kuma-client-certificate

Команда позволяет удалить сертификат клиента, используемый для защиты подключения к серверу KUMA.

Синтаксис команды

```
kesl-control [-M] --remove-kuma-client-certificate
```

Команда kesl-control --query-kuma-client-certificate

Команда позволяет вывести информацию о сертификате клиента.

Синтаксис команды

```
kesl-control [-M] --query-kuma-client-certificate
```

Команды управления параметрами интеграции с Sandbox

-X – префикс, указывающий, что команда принадлежит к группе команд управления параметрами интеграции с Sandbox.

Команда kesl-control --add-sandbox-server-certificate

Команда позволяет добавить или заменить ранее добавленный сертификат сервера, обеспечивающего взаимодействие с Sandbox.

Синтаксис команды

```
kesl-control [-X] --add-sandbox-server-certificate <файл>
```

Аргументы и ключи

< файл > – путь к файлу, содержащему сертификат сервера.

Команда kesl-control --remove-sandbox-server-certificate

Команда позволяет удалить сертификат сервера, обеспечивающего взаимодействие с Sandbox.

Синтаксис команды

```
kesl-control [-X] --remove-sandbox-server-certificate
```

Команда kesl-control --query-sandbox-server-certificate

Команда позволяет вывести информацию о сертификате сервера, обеспечивающего взаимодействие с Sandbox.

Синтаксис команды

```
kesl-control [-X] --query-sandbox-server-certificate
```

Команда 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.

Синтаксис команды

```
kesl-control [-X] --add-sandbox-client-certificate < файл >
```

Аргументы и ключи

< файл > – путь к криптоконтейнеру (архиву формата PFX), содержащему сертификат клиента и закрытый ключ.

Команда kesl-control --remove-sandbox-client-certificate

Команда позволяет удалить сертификат клиента, используемый для защиты подключения к серверу, обеспечивающего взаимодействие с Sandbox.

Синтаксис команды

```
kesl-control [-X] --remove-sandbox-client-certificate
```

Команда kesl-control --query-sandbox-client-certificate

Команда позволяет вывести информацию о сертификате клиента.

Синтаксис команды

```
kesl-control [-X] --query-sandbox-client-certificate
```

Команда kesl-control --sandbox

Команда позволяет отправить файлы в Sandbox на проверку.

Синтаксис команды

```
kesl-control [-X] --sandbox <путь 1> <путь 2>
```

Аргументы и ключи

< путь > – путь к файлу или директории, которые вы хотите проверить. Вы можете указать несколько путей, разделяя их пробелами.

Команды управления поиском IOC

-T – префикс, указывающий, что команда принадлежит к группе команд управления параметрами и задачами приложения.

Команда kesl-control --scan-ioc

Команда запускает поиск индикаторов компрометации на устройстве (IOC).

Синтаксис команды

```
kesl-control [-T] --scan-ioc --path <путь к директории или файлу> [--process on|off] [--hint <регулярное выражение>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--excludes <список исключений>] [--scope <список директорий>] [--action Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

Аргументы и ключи

`--path <путь к директории или файлу>` – 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 <регулярное выражение>` – 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 <список исключений>` – 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 <список директорий>` – 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**.
  - /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.

Команды приложения в режиме Легкого агента для защиты виртуальных сред

-V – префикс, указывающий, что команда принадлежит к группе команд приложения Kaspersky Endpoint Security, используемого в режиме Легкого агента для защиты виртуальных сред (в составе решения Kaspersky Security для виртуальных сред Легкий агент).

Команды могут быть выполнены, только если приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред.

Команда kesl-control --ksvla-info

Команда позволяет вывести информацию об использовании приложения в режиме Легкого агента для защиты виртуальных сред.

Синтаксис команды

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

Команда kesl-control --viis-info

Команда позволяет вывести информацию о подключении Легкого агента (приложения Kaspersky Endpoint Security, используемого в качестве Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент), к Серверу интеграции.

Синтаксис команды

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

Команда kesl-control --svm-info

Команда позволяет вывести информацию о подключении Легкого агента (приложения Kaspersky Endpoint Security, используемого в качестве Легкого агента в составе решения Kaspersky Security для виртуальных сред Легкий агент), к SVM.

Синтаксис команды

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

Команды управления сбором метрик о состоянии системы

Команда kesl-control --export-metrics

Команда позволяет настроить сбор метрик о состоянии операционной системы.

Синтаксис команды

```
kesl-control [-J] --export-metrics [--period <интервал времени между выводами в секундах>|--interactive]
```

Аргументы и ключи

`--period` – периодический вывод результатов в командную строку;

`<интервал времени между выводами в секундах>` – интервал времени между выводами результатов команды в командную строку (в секундах);

`--interactive` – интерактивный вывод (по нажатию клавиши **Enter**).

Приложение 2. 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:
  - конфигурационный файл autoinstall.ini, который используется при установке приложения с помощью Kaspersky Security Center;
  - конфигурационный файл, который используется при установке приложения с помощью командной строки.
- 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.

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 этих файлах.

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.	`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.	`true/yes` – приложение используется в режиме Легкого агента для защиты виртуальных сред. `false/no` – приложение используется в стандартном режиме.
`EndpointAgentMode`	Использование Kaspersky Endpoint Security в режиме Агента Endpoint Detection and Response.	`true/yes` – приложение используется в режиме Агента Endpoint Detection and Response. `false/no` – приложение используется в стандартном режиме.
`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.	`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 Агента Endpoint Detection and Response или в режиме Легкого агента для защиты виртуальных сред).
`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.

Параметр	Описание	Значения
`CoreDumps`	Включение создания файла дампа при сбое в работе приложения.	`true/yes` – создавать файл дампа при сбое в работе приложения. `false/no` (значение по умолчанию) – не создавать файл дампа при 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 дампов, заданной по умолчанию, требуются root-права.
`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.
`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: 2047.
`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.

Параметр	Описание	Значения
`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.	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`.	`true/yes` – включен "безопасный" режим работы приложения. `false/no` (значение по умолчанию) – "безопасный" режим работы приложения выключен, приложение работает в штатном режиме.
`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.	`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.
Секция **[Network]** содержит следующие параметры:		

Параметр	Описание	Значения
`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).
`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, которой маркируются пакеты, созданные или проверенные приложением, чтобы запись о них не попадала в журнал утилиты iptable.	Значение задается десятеричным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 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.

Параметр	Описание	Значения
`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:		
`ServerMode`	Роль защищенной виртуальной машины, на которой приложение Kaspersky Endpoint Security используется в режиме Легкого агента для защиты виртуальных сред: сервер или рабочая станция. Не рекомендуется изменять значение этого параметра вручную. Параметр настраивается во время первоначальной настройки приложения.	`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 для защиты виртуальных сред. Не рекомендуется изменять значение этого параметра вручную. Параметр настраивается во время первоначальной настройки приложения.	`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.

Параметр	Описание	Значения
`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.
`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. `< значение >%` – значение от 1 до 100 в процентах от объема памяти. `< значение >MB` – значение в мегабайтах. `lowest/< значение >%/< значение >MB` – наименьшее значение между значением в процентах и значением в мегабайтах. `highest/< значение >%/< значение >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. `< значение >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. `< значение >%` – значение от 0 до 100 в процентах от объема памяти. `< значение >MB` – значение в мегабайтах. `lowest/< значение >%/< значение >MB` – наименьшее значение между значением в процентах и значением в мегабайтах. `highest/< значение >%/< значение >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.

Параметр	Описание	Значения
`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.
`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.
Секция **[Environment]** по умолчанию отсутствует в конфигурационном файле.		
`ExperimentalContainerdSupport`	Включение поддержки среды containerd при работе компонента Мониторинг контейнеров (Проверка контейнеров, 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`.	`true/yes` – включить поддержку среды containerd в работе компонента Мониторинг контейнеров. `false/no` – не включать поддержку среды containerd в работе компонента Мониторинг контейнеров.

Параметр	Описание	Значения
`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

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

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

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
```

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
```

Общие параметры приложения

Общие параметры приложения 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.
`TraceLevel`	Включение трассировки приложения и уровень детализации файлов трассировки.	`Detailed` – создавать детализированный файл трассировки. `MediumDetailed` – создавать файл трассировки, содержащий информационные сообщения и сообщения об ошибках. `NotDetailed` – создавать файл трассировки, содержащий сообщения об ошибках. `None` (значение по умолчанию) – не создавать файл трассировки.
`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 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--------`).
`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
`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 приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным. `No` (значение по умолчанию) – выключить обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.
`NamespaceMonitoring`	Включение проверки пространств имен и контейнеров (Проверка контейнеров, Мониторинг 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 проверку пространств имен и контейнеров. `No` – выключить проверку пространств имен и контейнеров.
`FileBlockDuringScan`	Включение режима перехвата файловых операций с блокированием доступа к файлам на время проверки. Режим перехвата файловых операций влияет на работу компонентов Защита от файловых угроз и Контроль устройств.	`Yes` (значение по умолчанию) – блокировать доступ к файлам на время проверки. `No` – не блокировать доступ к файлам на время проверки. Обращение к любому файлу разрешается, проверка выполняется 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, если во время проверки этот файл сможет, например, изменить свое имя до принятия приложением решения о статусе этого файла. При этом компоненты Защита от файловых угроз, Контроль устройств и запрет запуска объектов работают в режиме информирования, независимо от установленного режима работы.
`UseKSN`	Настройка использования Kaspersky Security Network в работе приложения.	`Basic` – включить использование Kaspersky Security Network в стандартном режиме. `Extended` – включить использование Kaspersky Security Network в расширенном режиме. `No` (значение по умолчанию) – не использовать Kaspersky 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` – включить режим работы, при котором приложение Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО. `No` (значение по умолчанию) – использовать полную версию баз вредоносного ПО. Облачный режим выключается автоматически, если 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.	`Yes` – включить компонент Managed Detection and Response. `No` (значение по умолчанию) – выключить компонент Managed Detection and Response.
`UseEdrOptimum`	Включение компонента EDR Optimum для интеграции с Kaspersky Endpoint Detection and Response Optimum.	`Yes` – включить компонент EDR Optimum. `No` (значение по умолчанию) – выключить компонент EDR 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 использование 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 форматов: • `[<connection protocol>://]<IP address of the proxy server>:<port>`, если для подключения к прокси-серверу не требуется аутентификация; • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>`, если для подключения к прокси-серверу требуется аутентификация. Подключение к прокси-серверу по протоколу HTTPS не поддерживается.
`ProxyBypass`	Список адресов, для подключения к которым прокси-сервер не используется.	Адрес задается в формате `< адрес >[:< номер порта >]`. Для указания адресов вы можете использовать маски (символы `*`) и комментарии (после символа \).
`ProxyBypassEdr`	Использование прокси-сервера при подключении к серверам, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise).	`Yes` – не использовать прокси-сервер при подключении к серверам, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise). `No` (значение по умолчанию) – использовать прокси-сервер при подключении к серверам, обеспечивающим интеграцию с Kaspersky Endpoint Detection and Response Expert (on-premise).
`ProxyBypassNdr`	Использование прокси-сервера при подключении к серверам, обеспечивающим интеграцию с Kaspersky Network Detection and Response (KATA).	`Yes` – не использовать прокси-сервер при подключении к серверам, обеспечивающим интеграцию с Kaspersky Network Detection and Response (KATA). `No` (значение по умолчанию) – использовать прокси-сервер при подключении к серверам, обеспечивающим интеграцию с Kaspersky Network Detection and Response (KATA).
`ProxyBypassSandbox`	Использование прокси-сервера при подключении к серверам, обеспечивающим взаимодействие с Sandbox.	`Yes` – не использовать прокси-сервер при подключении к серверам, обеспечивающим взаимодействие с Sandbox. `No` (значение по умолчанию) – использовать прокси-сервер 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 сохраняются, 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.	0–100000 0 – непривилегированный пользователь не может запускать задачи выборочной проверки. Значение по умолчанию: 5.
`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 событий в 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/events.db.
`ExcludedMountPoint.item_#`	Точка монтирования, которую требуется исключить из области проверки. Исключение применяется в работе компонентов Защита от файловых угроз, Защита от шифрования, Мониторинг контейнеров (Проверка контейнеров, 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 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:<тип файловой системы>` – 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. `<путь, содержащий маску /mnt/user* или /mnt/**/user_share>` – исключать из перехвата объекты, находящиеся в точках монтирования, имена которых содержат указанную **маску**. 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. Для исключения точки монтирования `/dir` требуется указывать именно `/dir` (без звездочек). Маска `/dir/*` исключает все точки монтирования на уровень ниже от `/dir`, но не саму точку монтирования `/dir`. Маска `/dir/**` исключает все точки монтирования на любом уровне вложенности под `/dir`, но не саму точку монтирования `/dir`. Вы можете использовать символ `?` вместо любого одного символа в имени файла или директории.

Параметр	Описание	Значения
`MemScanExcludedProgramPath.item_#`	Исключение памяти процесса из проверки. Приложение не будет проверять память указанного процесса.	`< полный путь к процессу >` – исключать из проверки процесс в указанной локальной директории. Для указания пути вы можете использовать **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.
`UseOnDemandCPULimit`	Включение ограничения на использование ресурсов процессора для задач типа *ODS*, *ContainerScan* и *InventoryScan*.	`Yes` – включить ограничение потребления ресурсов процессора для задач типа *ODS*, *ContainerScan* и *InventoryScan*. `No` (значение по умолчанию) – выключить ограничение 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.
`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 – 999999 0 – размер резервного хранилища не ограничен. Значение по умолчанию: 0.
`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.	Значение по умолчанию: /var/opt/kaspersky/kesl/common/objects-backup/ Для доступа к заданной по умолчанию директории требуются root-права.
`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.

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.	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 агента.
`ShowPopUpNotifications`	Включение отображения всплывающих уведомлений в графическом пользовательском интерфейсе.	`Yes` (значение по умолчанию) – показывать всплывающие уведомления в графическом пользовательском интерфейсе. `No` – не показывать всплывающие уведомления в графическом пользовательском интерфейсе.
`PowerSaveMode`	Отмена запуска запланированных задач на устройстве, работающем от аккумулятора.	`Yes` (значение по умолчанию) – пропускать запуск задач, для которых настроено расписание запуска, если устройство работает от аккумулятора. `No` – запускать задачи по расписанию независимо от источника питания, к которому подключено устройство (сеть или аккумулятор).
`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.	`UseFanotify` (значение по умолчанию) – использовать технологию fanotify для перехвата системных событий. `UseUpdatableKernelModule` – использовать обновляемый модуль ядра для перехвата системных событий.
`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) – 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.

Параметр	Описание	Значения
`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` (рекомендованное значение) – 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.
`SystemEventsTransmission`	Включение записи информации о событиях сторонних приложений в syslog. Для доступа к syslog требуются root-права.	`Yes` – включить запись информации о событиях сторонних приложений в syslog. `No` (значение по умолчанию) – выключить запись информации о событиях сторонних приложений в syslog.

Общие параметры проверки контейнеров

Общие параметры проверки контейнеров используются при проверке пространств имен и контейнеров в реальном времени (Проверка контейнеров, Мониторинг контейнеров).

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, выполнимое 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. Поддерживается интеграция с системой управления контейнерами Docker версии 28.5.2 и ниже.	`Yes` (значение по умолчанию) – использовать систему управления контейнерами Docker. `No` – не использовать систему управления контейнерами Docker.

Параметр	Описание	Значения
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.
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.

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.	`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.

Параметры расписания задач

В таблице ниже описаны параметры расписания запуска задач, которые вы можете настроить для всех задач приложения.

Параметры расписания запуска задач

Параметр	Описание	Значения
`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. Параметр `StartTime` является обязательным, если параметр `RuleType` принимает одно из следующих значений: Once, Monthly, Weekly, Daily, Hourly, Minutely.	`[< год >/< месяц >/< день месяца >] [ чч ]:[ мм ]:[ сс ]; [< день месяца >| < день недели >]; [< периодичность запуска >]`
`RandomInterval`	Интервал времени от 0 до указанного значения (в минутах), который будет добавлен ко времени запуска задачи, чтобы избежать одновременного запуска задач.	Значение по умолчанию: 99 минут.
`RunMissedStartRules`	Запуск пропущенной задачи после запуска приложения.	`Yes` (значение по умолчанию) – включать запуск пропущенной задачи после запуска приложения. `No` – не включать запуск пропущенной задачи после запуска 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.
`WorkingTimeout`	Максимальное время выполнения задачи (в минутах), при достижении которого приложение останавливает выполнение задачи, если значение параметра `UseWorkingTimeout=yes`.	Значение по умолчанию: 120 минут.

Приложение 3. Коды возврата командной строки

В приложении Kaspersky Endpoint Security предусмотрены следующие коды возврата командной строки:

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 2.0 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;

128 – неизвестная ошибка;

65 – все остальные ошибки.

Приложение 4. 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 5. Параметры приложения в политике в Web Console

В этом разделе приведены описания параметров политики в Web Console на закладке **Параметры приложения**.

Защита устройств от угроз

Защита от файловых угроз

для Windows, macOS и Linux

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. По умолчанию компонент Защита от файловых угроз постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы в режиме реального времени. Компонент проверяет файлы на всех дисках компьютера, а также на подключенных дисках. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Компонент проверяет файлы, к которым обращается пользователь или приложение. При обнаружении вредоносного файла Kaspersky Endpoint Security блокирует операцию с файлом. Далее приложение лечит или удаляет вредоносный файл, в зависимости от настройки компонента Защита от файловых угроз.

При обращении к файлу, содержимое которого расположено в облачном хранилище OneDrive, Kaspersky Endpoint Security загружает и проверяет содержимое этого файла.

`Linux` Для Linux-устройств на работу компонента влияет режим блокировки доступа к файлам во время проверки, который вы можете выбрать в общих настройках приложения. По умолчанию на время проверки доступ к файлу блокируется.

Настройка	ОС	Описание
Исключения из проверки	`Windows` `macOS` `Linux`	*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". Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
Действие при обнаружении угрозы	`Windows` `macOS` `Linux`	**Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл. **Лечить. Блокировать, если лечение невозможно (зависит от ОС)**. `Windows` `Linux` Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение блокирует этот файл. **Блокировать или запросить действие (зависит от ОС)**. `Windows` `Linux` Если выбран этот вариант действия, то приложение автоматически блокирует зараженный файл без попытки вылечить и удалить. `macOS` Kaspersky Endpoint Security выводит на экран окно уведомления с информацией о том, каким вредоносным объектом заражен файл, и предлагает выбрать, какое действие выполнит Kaspersky Endpoint Security. В зависимости от статуса объекта действия могут отличаться. Перед лечением или удалением зараженного файла приложение формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить.
Область защиты	`Windows` `macOS` `Linux`	Содержит объекты, которые проверяет компонент Защита от файловых угроз. Объектом проверки может быть жесткий, съемный или сетевой диск, папка, файл или несколько файлов, определенных по маске. По умолчанию компонент Защита от файловых угроз проверяет файлы, запускаемые со всех жестких, съемных и сетевых дисков. Область защиты этих объектов невозможно изменить или удалить. Вы можете только исключить объект (например, съемные диски) из проверки. `Linux` Для Linux-устройств вы можете изменять или удалять области проверки компонентом Защита от файловых угроз. Для работы компонента укажите хотя бы одну область защиты.
Типы файлов	`macOS`	**Проверять все файлы**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений). **Проверять программы и документы по содержимому**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла. **Проверять программы и документы по расширению**. Если выбран этот параметр, приложение проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
Оптимизация проверки	`Windows` `macOS`	В блоке **Оптимизация проверки** вы можете настроить параметры для большей производительности Kaspersky Endpoint Security при проверке файлов. • `Windows` `macOS` **Проверять только новые и измененные файлы**. Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы. • `Windows` **Останавливать контейнер, если лечение невозможно**. У приложения может не быть прав на чтение и запись обнаруженного объекта. В этом случае вылечить или удалить обнаруженный объект невозможно. Если флажок установлен, приложение блокирует обнаруженный объект и останавливает контейнер. Если флажок снят, приложение только блокирует обнаруженный объект. • `macOS` **Пропускать проверку системного тома "только для чтения"**. Если флажок установлен, приложение не проверяет системный том "только для чтения". Время выполнения проверки значительно уменьшается. • `Windows` **Не проверять файловые операции, исполняемые в контейнерах Windows**. Если флажок установлен, приложение проверяет контейнер только при запуске контейнера. Если флажок снят, приложение проверяет контейнер постоянно в режиме реального времени.

Настройка	ОС	Описание
Проверка составных файлов	`Windows` `macOS` `Linux`	Распространенной практикой сокрытия вирусов и других приложений, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие приложения, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить типы проверяемых составных файлов, таким образом увеличив скорость проверки. • **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). • **Дистрибутивы и самораспаковывающиеся архивы**. Проверка инсталляционных пакетов сторонних приложений и самораспаковывающихся архивов. Самораспаковывающиеся архивы имеют в своем составе исполняемый модуль-распаковщик. Для проверки самораспаковывающихся архивов должен быть установлен флажок **Проверять архивы**. • `Windows` `macOS` **Файлы офисных форматов и вложенные OLE-объекты**. Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других) и вложенных в файлы OLE-объектов (например, Excel-таблиц, макросов, вложений в сообщениях электронной почты). • `Windows` `Linux` **Проверять почтовые базы**. Проверка почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. • `Linux` **Проверять файлы почтовых форматов**. Проверка файлов сообщений электронной почты в текстовом формате.
Разрешать распаковку в фоновом режиме архивов размером более (МБ)	`Windows` `macOS`	Если флажок установлен, приложение предоставляет доступ к составным файлам, размер которых превышает заданное значение, до проверки этих файлов. При этом приложение Kaspersky Endpoint Security в фоновом режиме распаковывает и проверяет составные файлы. Приложение предоставляет доступ к составным файлам, размер которых меньше данного значения, только после распаковки и проверки этих файлов. Если флажок снят, приложение предоставляет доступ к составным файлам только после распаковки и проверки файлов любого размера.
Не проверять архивы размером более (МБ)	`Windows` `macOS` `Linux`	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.
Пропускать файл, если его проверка длится более (сек.)	`Linux`	Если флажок установлен, то приложение прекращает проверку составных файлов по истечению указанного времени. Если указано значение `0`, время проверки не ограничено.
Фоновая проверка	`Windows`	*Фоновая проверка* – это режим проверки Kaspersky Endpoint Security без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security проверяет объекты автозапуска, загрузочного сектора, системной памяти и системного раздела.
Проверка из контекстного меню	`Windows`	Kaspersky Endpoint Security позволяет проверять отдельные файлы на вирусы и другие приложения, представляющие угрозу, из контекстного меню. При выполнении проверки из контекстного меню Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.

Защита от атак BadUSB

для Windows и Linux

Некоторые вирусы изменяют встроенное программное обеспечение USB-устройств так, чтобы операционная система определяла USB-устройство как клавиатуру. В результате вирус может выполнять команды под вашей учетной записью, например, загрузить вредоносное приложение.

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

Когда к компьютеру подключается USB-устройство, определенное операционной системой как клавиатура, приложение предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) цифровой код, сформированный приложением (см. рис. ниже). Эта процедура называется авторизацией клавиатуры.

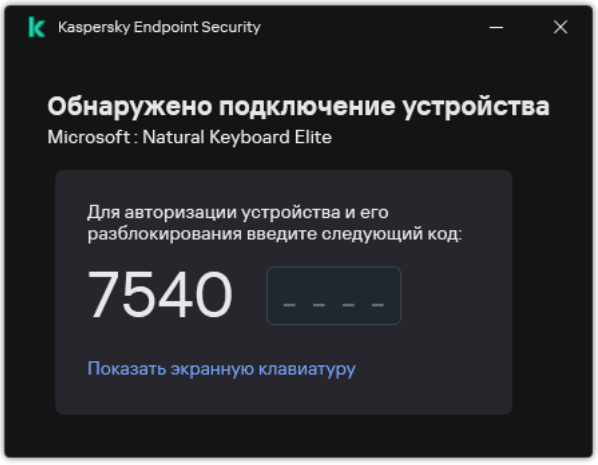
Если код введен правильно, приложение сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется.

При подключении авторизованной клавиатуры через другой USB-порт компьютера приложение снова запрашивает ее авторизацию.

Если цифровой код введен неправильно, приложение формирует новый. Вы можете настроить число попыток для ввода цифрового кода. Если цифровой код введен неправильно несколько раз или закрыто окно авторизации клавиатуры (см. рис. ниже), приложение блокирует ввод с этой клавиатуры. По истечении времени блокировки USB-устройства или перезагрузке операционной системы приложение снова предлагает пройти авторизацию клавиатуры.

Приложение разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.

Компонент Защита от атак BadUSB не устанавливается по умолчанию. Если вам нужен компонент Защита от атак BadUSB, вы можете добавить компонент в свойствах инсталляционного пакета перед установкой приложения или изменить состав компонентов приложения после установки приложения.



Авторизация клавиатуры

Настройки Защиты от атак BadUSB

Настройка	ОС	Описание
Максимальное количество попыток авторизации USB-устройства	`Windows` `Linux`	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)	`Windows` `Linux`	Время блокировки USB-устройства после заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).

Настройка	ОС	Описание
Запрет на использование экранной клавиатуры для авторизации USB-устройств	`Windows` `Linux`	Если переключатель включен, приложение запрещает использование экранной клавиатуры для авторизации USB-устройства, с которого невозможно ввести код авторизации.
Запрет на использование штрихкода для авторизации USB-устройств	`Windows` `Linux`	Если переключатель включен, Kaspersky Endpoint Security не показывает штрихкод в уведомлении для авторизации сканеров штрихкодов.

Проверка съемных дисков

для Windows, macOS и Linux

Kaspersky Endpoint Security проверяет все файлы, которые вы запускаете или копируете, даже если файл расположен на съемном диске (компонент Защита от файловых угроз). Для предотвращения распространения вирусов и других приложений, представляющих угрозу, вы можете настроить автоматическую проверку съемных дисков при подключении к компьютеру. При обнаружении угрозы Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет. Компонент обеспечивает защиту компьютера с помощью следующих методов проверки: машинное обучение, эвристический анализ (высокий уровень) и сигнатурный анализ. Также Kaspersky Endpoint Security использует технологии оптимизации проверки iSwift и iChecker. Технологии включены постоянно и выключить их невозможно.

Настройки Проверки съемных дисков

Настройка	ОС	Описание
Тип проверки	`Windows` `Linux`	**Быстрая проверка**. Если выбран этот вариант, то после подключения съемного диска Kaspersky Endpoint Security проверяет только файлы определенных форматов, наиболее подверженные заражению, а также не распаковывает составные объекты. **Подробная проверка**. Если выбран этот вариант, то после подключения съемного диска Kaspersky Endpoint Security проверяет все файлы, расположенные на съемном диске, в том числе вложенные файлы внутри составных объектов, архивы, дистрибутивы, файлы офисных форматов. Kaspersky Endpoint Security не проверяет файлы почтовых форматов и защищенные паролем архивы.
Запретить пользователям останавливать задачу проверки	`Windows`	Если флажок установлен, то в локальном интерфейсе Kaspersky Endpoint Security для задачи проверки съемных дисков недоступны кнопка **Стоп** в разделе **Задачи** и кнопка **Стоп** в окне проверки съемного диска.
Блокировать доступ к съемному диску во время проверки	`Linux`	Если флажок установлен, Kaspersky Endpoint Security блокирует доступ к файлам на подключенном диске во время выполнения проверки.
Скрыть индикатор выполнения задачи проверки	`Windows`	Если флажок установлен, Kaspersky Endpoint Security скрывает индикатор выполнения проверки съемных дисков. Приложение будет выполнять проверку в фоновом режиме. Если флажок снят, Kaspersky Endpoint Security отображает ход проверки съемных дисков в отдельном окне, а также в разделе **Задачи**.
Не проверять съемные диски размером более	`Windows`	Если флажок установлен, то Kaspersky Endpoint Security выполняет выбранное действие над съемными дисками, размер которых не превышает указанный максимальный размер. Если размер съемного диска превышает указанное значение, Kaspersky Endpoint Security пропускает проверку. Если флажок снят, то Kaspersky Endpoint Security выполняет выбранное действие над съемными дисками любого размера.

Анализ поведения

для Windows, macOS и Linux

Компонент Анализ поведения получает данные о действиях приложений на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы. Компонент Анализ поведения использует шаблоны опасного поведения приложений. Если активность приложения совпадает с одним из шаблонов опасного поведения, Kaspersky Endpoint Security выполняет выбранное ответное действие. Функциональность Kaspersky Endpoint Security, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

Компонент Анализ поведения дополнительно контролирует сетевые порты для процессов приложений, которые могут представлять угрозу безопасности компьютера. Приложение получает данные о таких процессах с антивирусными базами.

Для оптимальной работы компонента Анализ поведения рекомендуется включить компонент Защита от веб-угроз.

Настройки Анализа поведения

Настройка	ОС	Описание
Доверенные приложения	`Windows` `macOS` `Linux`	*Список доверенных приложений* – это список приложений, у которых Kaspersky Endpoint Security не контролирует файловую и сетевую активности (в том числе и вредоносную), а также обращения этих приложений к системному реестру. По умолчанию Kaspersky Endpoint Security контролирует объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех приложений и создаваемый ими сетевой трафик. После добавления приложения в список доверенных приложений Kaspersky Endpoint Security перестает контролировать активность приложения. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
Исключения из проверки	`Windows` `macOS` `Linux`	*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". Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
Действие при обнаружении угрозы	`Windows` `macOS` `Linux`	**Удалить файл или блокировать (зависит от ОС)**. `Windows` `macOS` Если выбран этот вариант, то при обнаружении вредоносной активности Kaspersky Endpoint Security удаляет исполняемый файл вредоносного приложения и создает копию файла в резервном хранилище. `Linux` При обнаружении вредоносной активности Kaspersky Endpoint Security блокирует приложение, осуществляющее вредоносную активность, и записывает в журнал событий информацию об обнаруженной вредоносной активности. **Информировать**. `Windows` `Linux` Если выбран этот вариант, то в случае обнаружения вредоносной активности приложения Kaspersky Endpoint Security не завершает работу этого приложения и добавляет информацию о вредоносной активности этого приложения в список активных угроз. `macOS` При обнаружении вредоносной активности Kaspersky Endpoint Security предлагает пользователю выбрать действие, которое требуется выполнить при обнаружении вредоносной активности. В зависимости от статуса объекта действия могут отличаться. **Блокировать**. Если выбран этот вариант, то, обнаружив вредоносную активность приложения, Kaspersky Endpoint Security завершает работу этого приложения.

Защита от шифрования

для Windows, macOS и Linux

`Windows` Для Windows-устройств компонент отслеживает операции только над файлами, которые находятся на уровне файловой системы NTFS и не зашифрованы системой EFS.

`Linux` Для Linux-устройств компонент анализирует файлы в локальных директориях с сетевым доступом по протоколам SMB/NFS.

`macOS` Для macOS-устройств компонент отслеживает папки с сетевым доступом по протоколу SMB.

Компонент Защита от шифрования обеспечивает защиту от удаленного шифрования, анализируя активность в общих сетевых папках. Если активность совпадает с одним из шаблонов поведения, характерного для внешнего шифрования, Kaspersky Endpoint Security выполняет выбранное действие.

`Linux` Перед включением компонента на Linux-устройствах внимательно изучите информацию о защите от шифрования.

Настройки Защиты от шифрования

Настройка	ОС	Описание
Исключения из проверки	`Windows` `Linux`	*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". Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
Исключения по имени или IP-адресу	`Windows`	**Исключения из Защиты от шифрования**. Список компьютеров, с которых не будут отслеживаться попытки шифрования папок общего доступа. **Исключения по маске**. Исключения из области защиты. Исключение папки из области защиты позволит сократить количество ложных срабатываний, если в вашей организации используется шифрование данных при обмене файлами с помощью папок общего доступа. Используйте **маски**. • Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках. • Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает. • Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Настройка	ОС	Описание
Действие при обнаружении угрозы	`Windows` `macOS` `Linux`	**Информировать**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security добавляет информацию об этой попытке изменения файлов в папках общего доступа в список активных угроз, добавляет запись в отчет. **Блокировать соединение на (мин)**. `Windows` Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security блокирует доступ на изменение файлов для сессии, которая инициировала вредоносную активность, и создает резервные копии измененных файлов. `macOS` `Linux` Обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security блокирует сетевой трафик от устройства, которое осуществляет вредоносную деятельность. Приложение создает событие *Обнаружено шифрование*, которое содержит информацию о скомпрометированном устройстве.
Область защиты	`Windows` `macOS` `Linux`	*Область защиты* – список путей к папкам общего доступа, в которых Kaspersky Endpoint Security отслеживает файловую активность. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. По умолчанию приложение автоматически определяет папки общего доступа и отслеживает файловую активность во всех папках. `macOS` Kaspersky Endpoint Security защищает все папки общего доступа для macOS-устройств. Изменить область защиты нельзя. `Windows` `Linux` Вы можете выбрать область защиты: **Все общие сетевые папки защищаемого устройства**. Приложение будет отслеживать файловую активность во всех папках общего доступа. **Только указанные общие папки**. Приложение будет отслеживать попытки шифрования только в указанных папках общего доступа.

Защита от эксплойтов

для Windows, macOS и Linux

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимое приложение. При обработке этих данных уязвимое приложение выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО. Если попытка запустить исполняемый файл из уязвимого приложения не была произведена пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла или информирует пользователя.

Компонент Защита от эксплойтов дополнительно контролирует сетевые порты для процессов приложений, которые могут представлять угрозу безопасности компьютера. Приложение получает данные о таких процессах с антивирусными базами.

Для работы компонента Защита от эксплойтов требуется включить компонент Анализ поведения. Для оптимальной работы компонента Защита от эксплойтов рекомендуется также включить компонент Защита от веб-угроз.

`Linux` Для Linux-устройств также требуется использовать обновляемый модуль ядра в качестве механизма перехвата системных событий.

Настройка	ОС	Описание
Действие при обнаружении угрозы	`Windows` `macOS` `Linux`	**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. **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.
Защита памяти системных процессов	`Windows`	Если переключатель включен, Kaspersky Endpoint Security блокирует сторонние процессы, осуществляющие попытки доступа к памяти системных процессов.

Защита сетевых соединений и средств коммуникации

Защита от почтовых угроз

для Windows, macOS и Linux

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других приложений, представляющих угрозу. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Защита от почтовых угроз может проверять и получаемые, и отправляемые сообщения. Приложение поддерживает протоколы POP3, SMTP, IMAP, NNTP.

`Linux` Приложение для Linux-устройств не поддерживает протокол NNTP.

Поддерживаемые почтовые клиенты

- `Windows`, `macOS` Microsoft Office Outlook;
- `Windows`, `macOS` Mozilla Thunderbird;
- `Windows` Windows Mail;
- `Windows`, `Linux` МойОфис Почта;
- `Windows`, `Linux` Органайзер Р7-Офис;
- `macOS` Apple Mail;
- `macOS` Canary Mail;
- `macOS` Spark;
- `macOS` Mimestream;
- `macOS` Airmail;
- `macOS` Post Box;

- macOS Boxy Suite 2;
- macOS Twobird;
- macOS Shift;
- macOS Clean Email;
- macOS eM Client;
- macOS Superhuman;
- macOS Polymail;
- macOS HEY;
- macOS Mail+ for Gmail;
- macOS Spike mail.

Windows Защита от почтовых угроз не всегда может получить доступ к сообщениям на уровне протокола (например, при использовании решения Microsoft Exchange). Поэтому дополнительно в состав Почтового Антивируса включено расширение Kaspersky ASAP Outlook Plugin для Microsoft Office Outlook. Расширение позволяет проверять сообщения на уровне почтового клиента. Kaspersky ASAP Outlook Plugin поддерживает работу с Outlook 2010, 2013, 2016, 2019, 2021.

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

При обнаружении вредоносного файла во вложении Kaspersky Endpoint Security добавляет информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*.

Настройки Почтового Антивируса

Настройка	ОС	Описание
Исключения из проверки	Windows macOS Linux	*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". Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.

Настройка	ОС	Описание
Действие при обнаружении угрозы	`Windows` `macOS` `Linux`	**Лечить. Удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение удаляет зараженный объект. Приложение добавит информацию о выполненном действии в тему сообщения, например, *[Сообщение было обработано] <тема сообщения>*. `Windows` `Linux` **Лечить. Блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении приложение пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение пытается вылечить обнаруженный объект. Если вылечить объект не удалось, приложение блокирует отправку сообщения, почтовый клиент показывает ошибку. **Блокировать**. При обнаружении зараженного объекта во входящем сообщении приложение добавит предупреждение к теме сообщения. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении приложение блокирует отправку сообщения, почтовый клиент показывает ошибку. `Linux` Для Linux-устройств компонент Защита от почтовых угроз не пытается лечить зараженный объект в исходящих сообщениях, а сразу блокирует отправку сообщения.
Проверять трафик POP3, SMTP, NNTP, IMAP	`Windows`	Проверка компонентом Защита от почтовых угроз почтового трафика, проходящего по протоколам POP3, SMTP, NNTP и IMAP.
Подключить расширение для Microsoft Outlook	`Windows`	Если флажок установлен, включена проверка сообщений электронной почты, передающихся по протоколам POP3, SMTP, NNTP, IMAP на стороне расширения, интегрированного в Microsoft Outlook. Приложение может проверять входящие и исходящие сообщения из Microsoft Outlook на разных этапах: • **Проверять при получении**. Если флажок установлен, приложение использует Защита от почтовых угроз при получении сообщений через Microsoft Outlook. • **Проверять при чтении**. • **Проверять при отправке**. В случае проверки почты с помощью расширения для Microsoft Outlook рекомендуется использовать режим кеширования Exchange (Cached Exchange Mode). Более подробную информацию о режиме кеширования Exchange и рекомендации по его использованию вы можете найти в базе знаний Microsoft.
Проверять вложенные архивы	`Windows` `Linux`	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	`Windows` `Linux`	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)	`Windows` `macOS` `Linux`	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.)	`Windows` `macOS` `Linux`	Если флажок установлен, то время проверки архивов, вложенных в сообщения электронной почты, ограничено указанным периодом.

Настройка	ОС	Описание
Фильтр вложений	`Windows` `Linux`	Фильтр вложений определяет какое действие применяет Защита от почтовых угроз по отношению к файлам, вложенным в сообщения электронной почты. Фильтр вложений не работает для исходящих сообщений электронной почты. • **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. Типы вложенных файлов, которые нужно переименовывать или удалять из сообщений электронной почты, вы можете указать в списке масок файлов.

Защита от веб-угроз

для Windows, macOS и Linux

Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует вредоносные и фишинговые веб-сайты. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.

Компонент Защита от веб-угроз проверяет входящий трафик, передаваемый по протоколам HTTP, HTTPS и FTP, веб-сайты и IP-адреса.

`Linux` Защита от веб-угроз по умолчанию выключена. Включение Веб-Антивируса может привести к снижению производительности установленных сторонних приложений и операционной системы. Подробнее о настройке приложения для работы Веб-Антивируса на Linux-устройствах см. в базе знаний Службы технической поддержки.

Настройки Веб-Антивируса

Настройки	ОС	Описание
Доверенные веб-адреса	`Windows` `macOS` `Linux`	Список веб-адресов, 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 Защита от веб-угроз препятствует загрузке файла с известного вам веб-сайта. Вы можете добавить в список доверенных веб-адресов как конкретный адрес веб-страницы / веб-сайта, так и маску адреса веб-страницы / веб-сайта. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.
Исключения из проверки	`Windows`	*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". Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.

Настройки	ОС	Описание
Действие при обнаружении угрозы	`Windows` `macOS` `Linux`	**Блокировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере. **Разрешить, информировать или запросить действие (в зависимости от ОС)**. `Windows` 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. `macOS` Kaspersky Endpoint Security выводит на экран уведомление с информацией о том, каким вредоносным приложением заражен объект веб-трафика, и предлагает выбрать, какое действие Kaspersky Endpoint Security выполнит над этим объектом. В зависимости от статуса объекта действия могут отличаться. `Linux` 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.

Защита от сетевых угроз

для Windows, macOS и Linux

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.

`Linux` Защита от сетевых угроз по умолчанию выключена. Включение Защиты от сетевых угроз может привести к снижению производительности установленных сторонних приложений и операционной системы. Подробнее о настройке приложения для работы Защиты от сетевых угроз для Linux-устройств см. в базе знаний Службы технической поддержки.

Настройки Защиты от сетевых угроз

Настройка	ОС	Описание
Доверенный IP-адрес	`Windows` `Linux`	Список IP-адресов доверенных устройств. Компонент Защита от сетевых угроз не блокирует сетевую активность с этих адресов. `Windows` Вы можете добавить IP-адрес с указанием используемого порта / диапазонов портов и протокола. `Linux` В список исключений можно добавить только IP-адрес. Приложение также не заносит в отчет информацию о сетевых атаках с IP-адресов, входящих в список исключений.
Действие при обнаружении угрозы	`Windows` `macOS` `Linux`	**Блокировать**. При обнаружении угрозы Защита от сетевых угроз блокирует атаку. **Блокировать атаку и атакующие устройства на (мин)**. Если функция включена, компонент Защита от сетевых угроз добавляет атакующий компьютер в список блокирования. Это означает, что компонент Защита от сетевых угроз блокирует сетевое соединение с атакующим компьютером после первой попытки сетевой атаки в течение заданного времени, чтобы автоматически защитить компьютер пользователя от возможных будущих сетевых атак с этого адреса. Минимальное время, на которое атакующий компьютер можно добавить в список блокирования, составляет одну минуту. Максимальное – 999 минут. Kaspersky Endpoint Security очищает список блокирования при перезапуске приложения и при изменении параметров Защиты от сетевых угроз.

Настройка	ОС	Описание
Считать атаками сканирование портов и интенсивные сетевые запросы	`Windows`	*Атака типа Сканирование портов* заключается в сканировании UDP- и TCP-портов, а также сетевых служб на компьютере. Атака позволяет определить степень уязвимости компьютера перед более опасными видами сетевых атак. Сканирование портов также позволяет злоумышленнику определить операционную систему на компьютере и выбрать подходящие для нее сетевые атаки. *Атака типа Интенсивные сетевые запросы (англ. Network Flooding)* – атака на сетевые ресурсы организации (например, веб-серверы). Атака заключается в отправке большого количества запросов для превышения пропускной способности сетевых ресурсов. Таким образом, пользователи не могут получить доступ к сетевым ресурсам организации. Если флажок установлен, Kaspersky Endpoint Security контролирует сетевой трафик на наличие этих атак. При обнаружении атаки приложение уведомляет пользователя и отправляет соответствующее событие в Kaspersky Security Center. Приложение предоставляет информацию об атакующем компьютере, необходимую для принятия своевременных действий по реагированию. Вы можете выключить обнаружение этих типов атак, так как некоторые разрешенные приложения выполняют действия, характерные для таких атак. Таким образом, вы можете избежать ложных срабатываний.
Защита от MAC-спуфинга	`Windows`	*Атака типа MAC-спуфинг* заключается в изменении MAC-адреса сетевого устройства (сетевой карты). В результате злоумышленник может перенаправить данные, отправленные на устройство, на другое устройство и получить доступ к этим данным. Kaspersky Endpoint Security позволяет блокировать атаки MAC-спуфинга и получать уведомления об атаках.

Сетевой экран

для Windows, macOS и Linux

Сетевой экран блокирует несанкционированные подключения к компьютеру во время работы в интернете или локальной сети. Также Сетевой экран контролирует сетевую активность приложений на компьютере. Это позволяет защитить локальную сеть организации от кражи персональных данных и других атак. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и предустановленных *сетевых правил*.

`Linux` Для Linux-устройств приложение использует компонент Управление сетевым экраном. Компонент управляет настройками и правилами сетевого экрана операционной системы.

Настройки Сетевого экрана

Настройка	ОС	Описание
Сетевые пакетные правила	`Windows` `macOS` `Linux`	Таблица сетевых пакетных правил. Сетевые пакетные правила используются для ввода ограничений на сетевые пакеты независимо от приложения. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных. В таблице представлены предустановленные сетевые пакетные правила, которые рекомендованы специалистами "Лаборатории Касперского" для оптимальной защиты сетевого трафика компьютеров под управлением операционных систем Microsoft Windows и Linux. Сетевой экран устанавливает приоритет выполнения для каждого сетевого пакетного правила. Сетевой экран обрабатывает сетевые пакетные правила в порядке их расположения в списке сетевых пакетных правил, сверху вниз. Сетевой экран находит первое по порядку подходящее для сетевого соединения сетевое пакетное правило и выполняет его действие: либо разрешает, либо блокирует сетевую активность. Далее Сетевой экран игнорирует все последующие сетевые пакетные правила для данного сетевого соединения. Сетевые пакетные правила имеют приоритет над сетевыми правилами приложений.

Настройка	ОС	Описание
Доступные сети	`Windows` `macOS` `Linux`	Таблица, содержащая информацию о сетевых соединениях, которые Сетевой экран обнаружил на компьютере пользователя. Сети Интернет по умолчанию присвоен тип **Публичная сеть**. Вы не можете изменить тип сети Интернет. Выделены следующие типы сетевого соединения: • **Публичная сеть**. Сеть не защищена антивирусными приложениями, сетевыми экранами, фильтрами (например, Wi-Fi в кафе). Пользователю компьютера, подключенного к такой сети, Сетевой экран закрывает доступ к файлам и принтерам этого компьютера. Сторонние пользователи также не могут получить доступ к информации через папки общего доступа и удаленный доступ к рабочему столу этого компьютера. Сетевой экран фильтрует сетевую активность каждого приложения в соответствии с сетевыми правилами этого приложения. • **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.
Всегда добавлять разрешающие правила для портов Агента администрирования	`macOS` `Linux`	Флажок включает или выключает автоматическое добавление разрешающих правил для портов Агента администрирования.
Права приложений и защищаемые ресурсы	`Windows`	**Приложение**. Таблица приложений, работу которых контролирует компонент Сетевой экран. Приложения распределены по группам доверия. Группа доверия определяет права, которые Kaspersky Endpoint Security использует для контроля сетевой активности приложений. Вы можете выбрать приложение из единого списка всех приложений, установленных на компьютерах под действием политики, и добавить приложение в группу доверия. **Сетевые правила**. Таблица сетевых правил приложений, входящих в группу доверия. В соответствии с этими правилами Сетевой экран регулирует сетевую активность для приложений. В таблице отображаются предустановленные сетевые правила, которые рекомендованы специалистами "Лаборатории Касперского". Эти сетевые правила добавлены для оптимальной защиты сетевого трафика компьютеров под управлением операционных систем Windows. Удалить предустановленные сетевые правила невозможно.

Контроль безопасности

Контроль устройств

для Windows, macOS и Linux

Контроль устройств управляет доступом пользователей к установленным или подключенным к компьютеру устройствам (например, жестким дискам, камере или модулю Wi-Fi). Это позволяет защитить компьютер от заражения при подключении этих устройств и предотвратить потерю или утечку данных.

Контроль устройств разрешает или запрещает доступ к устройствам на следующих уровнях:

- **Тип устройства**. Например, принтеры, съемные диски, CD/DVD-приводы.

- **Шина подключения**. *Шина подключения* – интерфейс, с помощью которого устройства подключаются к устройству (например, USB, FireWire). Если для типа устройств выбран режим **Зависит от шины**, приложение контролирует доступ к устройству в соответствии с режимом работы для шины, через которую подключается устройство (например, USB-порт).

- **Доверенные устройства**. *Доверенные устройства* – это устройства, полный доступ к которым разрешен в любое время для выбранных пользователей или группы пользователей.

  Вы можете добавить доверенные устройства по следующим данным:

  - `Windows` `macOS` **Модели**. Каждое устройство имеет идентификатор производителя (англ. Vendor ID, VID) и идентификатор продукта (англ. Product ID, PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы. Шаблон для ввода VID и PID: `VID_1234&PID_5678`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.

  - **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.

  - `Windows` `macOS` **Устройства по маске модели**. Если вы используете несколько устройств с похожими VID или PID (например, устройства одного производителя), вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Символ `?` заменяет один произвольный символ. Например, `VID_05AC&PID_*`.

  - **Устройства по маске идентификатора**. Если вы используете несколько устройств с похожими идентификаторами, вы можете добавить устройства в список доверенных с помощью масок. Символ `*` заменяет любой набор символов. Символ `?` заменяет один произвольный символ. Например, `WDC_C*`.

`Linux` Для Linux-устройств действие, выполняемое компонентом, зависит от режима перехвата файловых операций, выбранного в разделе "Общие настройки" в подразделе "Настройки обнаружения".

Настройки Контроля устройств

Настройка	ОС	Описание
Доверенные устройства	`Windows` `macOS` `Linux`	Список доверенных устройств и пользователей, которым разрешен доступ к этим устройствам. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски.
Шаблоны сообщений	`Windows` `Linux`	**Сообщение пользователю**. Шаблон сообщения, которое появляется при обращении пользователя к заблокированному устройству. Также сообщение появляется при попытке пользователя совершить операцию над содержимым устройства, которая запрещена для этого пользователя. **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к устройству или запрет операции над содержимым устройства, по мнению пользователя, произошли ошибочно.
Разрешить запрашивать временный доступ	`Windows` `Linux`	Если флажок установлен, то кнопка **Запросить доступ** в локальном интерфейсе Kaspersky Endpoint Security доступна. С помощью этой кнопки пользователь может запросить временный доступ к заблокированному устройству.
Режим работы	`Linux`	Kaspersky Endpoint Security выполнит выбранное действие 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**. При выборе этого варианта приложение Kaspersky Endpoint Security применяет режим доступа, заданный для устройства или шины.
Устройства и сети Wi-Fi	`Windows` `macOS` `Linux`	Список всех возможных типов устройств по классификации компонента Контроль устройств и статусом доступа к ним.
Шины подключения	`Windows` `Linux`	Список всех возможных шин подключения по классификации компонента Контроль устройств и статусом доступа к ним. Kaspersky Endpoint Security разрешает или запрещает доступ к устройствам по шине подключения, если выбран режим **Зависит от шины подключения**.

Настройка	ОС	Описание
Анти-Бриджинг	`Windows`	Анти-Бриджинг предотвращает создание сетевых мостов, исключая возможность одновременной установки нескольких сетевых соединений для компьютера. Это позволяет защитить корпоративную сеть от атак через незащищенные, несанкционированные сети. Анти-Бриджинг блокирует установку нескольких соединений в соответствии с приоритетами устройств. Чем выше находится устройство в списке, тем выше его приоритет. Если активное и новое соединения относятся к одному типу (например, Wi-Fi), Kaspersky Endpoint Security блокирует активное соединение и разрешает установку нового соединения. Если активное и новое соединения относятся к разным типам (например, сетевой адаптер и Wi-Fi), Kaspersky Endpoint Security блокирует соединение с более низким приоритетом и разрешает соединение с более высоким приоритетом. Анти-Бриджинг поддерживает работу со следующими типами устройств: сетевой адаптер, Wi-Fi и модем.

Веб-Контроль

для Windows, macOS и Linux

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.

Правила доступа к веб-сайтам

Веб-Контроль управляет доступом пользователей к веб-сайтам с помощью *правил доступа*. Вы можете настроить доступ к веб-сайтам по следующим областям проверки:

- **Категория веб-сайта**. Категоризацию веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз приложения). Вы можете ограничить доступ пользователей к отдельным категориям, например, к категории *Социальные сети,* или другим категориям.
- `Windows` **Тип данных**. Вы можете ограничить доступ пользователей к данным на веб-сайте и, например, скрыть графические изображения. Kaspersky Endpoint Security определяет тип данных по формату файла, а не по расширению.

  > Kaspersky Endpoint Security не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, Kaspersky Endpoint Security определит тип данных *Архивы*, а не *Графические файлы*.

- **Отдельный адрес**. Вы можете ввести веб-адрес или использовать маски.

Вы можете использовать одновременно несколько способов регулирования доступа к веб-сайтам. Например, вы можете ограничить доступ к типу данных *Файлы офисных приложений* только для категории веб-сайтов *Веб-почта*.

Веб-Контроль также позволяет настроить следующие дополнительные параметры правил доступа к веб-сайтам:

- **Пользователь или группа, на которых распространяется правило**.

  Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

- **Расписание доступа к устройствам**.

  Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Настройки Веб-Контроля

Настройка	ОС	Описание
Шаблоны сообщений	`Windows` `Linux`	**Предупреждение**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу. **Сообщение о блокировке**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу. **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации. Используется в случае, если доступ к веб-ресурсу, по мнению пользователя, заблокирован ошибочно. Для работы с шаблонами сообщений предусмотрены специальные переменные (например, `%USER_NAME%`). Переменные позволяют использовать единый шаблон сообщений для различных компьютеров.
Список правил	`Windows` `macOS` `Linux`	Список с правилами доступа к веб-ресурсам. Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом.
Действие по умолчанию	`Windows` `macOS` `Linux`	Правило доступа к веб-ресурсам, которые не входят ни в одно из правил. Возможны следующие варианты: • **Разрешать все, не указанное в списке правил**. • **Блокировать все, не указанное в списке правил**.
Завершать активные пользовательские сеансы браузера после применения правила	`Windows`	Если флажок установлен, Веб-Контроль разрывает подключение к запрещенным веб-ресурсам сразу после применения политики. Браузер немедленно прекращает загрузку данных на веб-странице. При обновлении веб-страницы или переходе на другую запрещенную веб-страницу приложение показывает предупреждение. Веб-Контроль позволяет немедленно разрывать соединения к веб-ресурсам только в браузерах. Для других приложений Веб-Контроль ограничивает только новые подключения. Если флажок снят, Веб-Контроль ограничивает только новые подключения к запрещенным веб-ресурсам. Активные подключения Веб-Контроль не разрывает.
Мониторинг веб-сессий	`Windows`	Kaspersky Endpoint Security записывает данные о посещении всех веб-сайтов, в том числе и разрешенных. Kaspersky Endpoint Security отправляет события в Kaspersky Security Center, журнал событий Windows и отчет. Для мониторинга активности пользователя в интернете нужно настроить параметры сохранения событий. Браузеры, которые поддерживают функцию мониторинга: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Яндекс.Браузер, Mozilla Firefox. Мониторинг активности пользователей не работает в других браузерах. Мониторинг активности пользователя в интернете может потребовать больше ресурсов компьютера при расшифровке HTTPS-трафика.

Контроль приложений

для Windows и Linux

Контроль приложений управляет запуском приложений на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании приложений. Также Контроль приложений снижает риск заражения компьютера, ограничивая доступ к приложениям.

Компонент Контроль приложений регулирует запуск приложений на защищаемых устройствах с помощью правил. Правило содержит условия и действия компонента Контроль приложений при срабатывании правила. Например, принадлежность приложения к категории приложений. *Категория приложений* – это группа приложений, обладающих общими признаками. Например, категория, в которую входят исполняемые файлы установленных приложений, или категория приложений, в которую входит стандартный набор приложений, используемых в организации. Вы можете использовать одну и ту же категорию только в одном правиле.

Администратор может создать множество правил. При этом одно приложение может соответствовать критериям нескольких правил. Приоритет запрещающего правила выше разрешающего. Kaspersky Endpoint Security проверяет приложение на принадлежность к правилу при каждом запуске. Kaspersky Endpoint Security последовательно проверяет приложение по всем правилам Контроля приложения.

Настройки Контроля приложений

Настройка	ОС	Описание
Шаблоны сообщений	`Windows`	**Сообщение пользователю**. Шаблон сообщения, которое появляется при срабатывании правила Контроля приложений, блокирующего запуск приложения. **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка приложения, по мнению пользователя, произошла ошибочно.
Режим работы	`Windows` `Linux`	Вы можете выбрать один из следующих вариантов: • **Разрешать все, не указанное в списке правил**. Если выбран этот вариант, Контроль приложений разрешает всем пользователям запуск любых приложений, кроме приложений, запрещенных правилами Контроля приложений. • **Блокировать все, не указанное в списке правил**. Если выбран этот вариант, Контроль приложений запрещает всем пользователям запуск любых приложений, кроме приложений, разрешенных правилами Контроля приложений.
Действие при запуске приложений	`Windows` `Linux`	• **Применять правила**. Kaspersky Endpoint Security управляет запуском приложений в соответствии с выбранным режимом. • **Информировать**. Kaspersky Endpoint Security информирует о попытке запуска приложения.
Добавить правила из политики к локальным правилам	`Linux`	При выборе этого элемента списка приложение применяет правила, заданные в политике, совместно с локальными правилами, настроенными на защищаемом устройстве.
Использовать строгую проверку цифровой подписи	`Windows`	Вы можете выбрать сертификат в качестве условия срабатывания правила Контроля приложений. Если флажок установлен, то Kaspersky Endpoint Security применяет правила к приложениям, подписанных сертификатом только из доверенного системного хранилища сертификатов приложения. Приложения, подписанные таким сертификатом, также являются доверенными для компонентов защиты, например, для задачи *Поиск вредоносного ПО*. При этом, если в правиле Контроля приложений указать сертификат из другого хранилища, Kaspersky Endpoint Security не применит такое правило. Если флажок снят, Kaspersky Endpoint Security применяет правила к приложениям, подписанных сертификатом из хранилища доверенных корневых центров Windows (англ. Trusted Root Certificate Store). Такие приложения не входит в доверенную зону. Компоненты защиты контролируют активность таких приложений.

Настройка	ОС	Описание
Контролировать загрузку DLL-модулей	`Windows`	Если флажок установлен, то Kaspersky Endpoint Security контролирует загрузку DLL-модулей при запуске пользователями приложений. Информация о DLL-модуле и приложении, загрузившей этот DLL-модуль, сохраняется в отчет. При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в параметрах Контроля приложений включено правило по умолчанию **Приложения ОС** или другое правило, которое содержит KL-категорию **Приложения ОС\Доверенные сертификаты** и обеспечивает загрузку доверенных DLL-модулей и драйверов до запуска Kaspersky Endpoint Security. Включение контроля загрузки DLL-модулей и драйверов при выключенном правиле **Приложения ОС** может привести к нестабильности операционной системы. Kaspersky Endpoint Security контролирует только DLL-модули и драйверы, загруженные с момента установки флажка. Рекомендуется перезагрузить компьютер после установки флажка, чтобы приложение контролировало все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security.
Правила	`Windows` `Linux`	Правила компонента Контроль приложений, с помощью которых Kaspersky Endpoint Security контролирует запуск приложений на защищаемых устройствах. Для каждого режима Контроля приложений можно добавить не более пяти правил.
Доверенные приложения обновления	`Windows`	Если флажок установлен, Kaspersky Endpoint Security будет считать приложения, входящие в правило, доверенными приложениями обновления. Kaspersky Endpoint Security разрешает таким приложениям создавать и запускать новые исполняемые файлы.

Контроль целостности системы

для Windows и Linux

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

Контроль целостности системы отслеживает изменения в операционной системе, которые могут указывать на нарушения безопасности компьютера. Обнаружив такие изменения, Kaspersky Endpoint Security формирует соответствующие события и предупреждает администратора. Контроль целостности системы может работать в режиме реального времени, а также выполнять проверку целостности системы по запросу.

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.

`Linux` Технические ограничения операционной системы Linux не позволяют приложению определять, какой пользователь или процесс внес изменение в файл.

Настройка	ОС	Описание
Контроль целостности системы в режиме реального времени	`Windows`	При работе в режиме реального времени Контроль целостности системы отслеживает изменения в объектах, которые вы включили в область действия компонента (*область мониторинга*). Также Контроль целостности системы позволяет блокировать несанкционированный доступ к этим объектам в режиме реального времени.
Действие при обнаружении изменений в системе	`Windows`	**Применять правила**. В этом режиме Контроль целостности системы блокирует действия с файлами и реестром в области мониторинга и формирует соответствующее событие. **Тестировать правила (Информировать)**. В этом режиме Контроль целостности системы разрешает действия с файлами и реестром в области мониторинга и формирует соответствующее событие.
Следить за файлами и реестром	`Windows`	Контроль целостности системы отслеживает изменения в файлах, папках и реестре.
Следить за устройствами	`Windows`	Контроль целостности системы отслеживает подключения и отключения внешних устройств.
Проверка целостности системы	`Windows`	Проверка целостности системы по запросу представляет собой задачу, которую вы можете запускать вручную или по расписанию. Для выполнения задачи *Проверка целостности системы* требуется настроить область действия компонента (*область мониторинга*) и создать снимок состояния системы. *Снимок состояния системы* – зафиксированное состояние объектов системы, с которым приложение сравнивает текущее состояние.
Области мониторинга	`Linux`	Таблица содержит области мониторинга компонента Контроль целостности системы. Приложение контролирует файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица содержит область мониторинга **Внутренние объекты "Лаборатории Касперского"**.
Области исключения	`Linux`	Таблица содержит области исключения из проверки. Приложение не проверяет файлы и директории, расположенные по указанным в таблице путям. По умолчанию таблица пуста.
Исключения по маске	`Linux`	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.

Доверенная зона

для Windows, macOS и Linux

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.

Kaspersky Endpoint Security поддерживает указание имени файла или папки через маску. Для формирования маски вы можете использовать следующие общие символы:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Настройка	ОС	Описание
Веб-адреса	`Windows` `macOS` `Linux`	Список веб-адресов, 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 Защита от веб-угроз препятствует загрузке файла с известного вам веб-сайта. Вы можете добавить в список доверенных веб-адресов как конкретный адрес веб-страницы / веб-сайта, так и маску адреса веб-страницы / веб-сайта.
IP-адреса	`Windows` `Linux`	Список IP-адресов доверенных устройств. Компонент Защита от сетевых угроз не блокирует сетевую активность с этих адресов. `Windows` Вы можете добавить IP-адрес с указанием используемого порта / диапазонов портов и протокола. `Linux` В список исключений можно добавить только IP-адрес. Приложение также не заносит в отчет информацию о сетевых атаках с IP-адресов, входящих в список исключений.
Сетевые порты	`Windows` `macOS` `Linux`	Список известных и зарегистрированных портов, по которым компоненты Веб-Контроль, Защита от файловых угроз, Защита от веб-угроз, Защита от почтовых угроз, Защита от эксплойтов и Анализ поведения контролируют потоки данных. Если переключатель включен, порт считается доверенным, и данные, передаваемые через такой порт на устройствах пользователей, не контролируются.
Корневые сертификаты	`Windows` `macOS` `Linux`	Список корневых сертификатов, которые приложение Kaspersky Endpoint Security будет считать доверенными. Список доверенных корневых сертификатов используется при проверке зашифрованных соединений.
Исключения из Защиты от шифрования	`Windows`	Список имен и IP-адресов компьютеров, которые компонент Анализ поведения будет считать доверенными. Kaspersky Endpoint Security не будет проверять указанные устройства на вирусы и другие приложения, представляющие угрозу.
Домены	`Windows` `Linux`	Список доверенных доменов. Компоненты Защита от веб-угроз, Веб-контроль и Cloud Discovery (доступно только для Windows-устройств) не контролируют зашифрованные соединения с этими доменами. Подключение к доменам из этого списка будет заблокировано на Windows-устройствах при использовании протоколов SSL/TLS, если включена настройка "Блокировать SSL/TLS-соединения".
Точки монтирования	`Linux`	Список доверенных точек монтирования. Они исключаются из проверки компонентами Защита от файловых угроз, Защита от шифрования, Контроль приложений и Анализ поведения. Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды `mount`.
Исключения из перехвата трафика	`Linux`	Список сетевых соединений, которые Kaspersky Endpoint Security исключает из перехвата трафика. Исключения из перехвата трафика влияют на работу компонентов Защита от веб-угроз, Защита от сетевых угроз и Веб-Контроль. Исключаемое соединение определяется следующими параметрами: • Направление трафика – входящий или исходящий; • IP-адрес удаленного устройства – 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). Исключения из перехвата трафика применяются только для соединений по протоколу TCP и не влияют на работу сетевых пакетных правил.
Сети Wi-Fi	`macOS`	Список доверенных сетей Wi-Fi. Вы можете указать следующие параметры: • Имя Wi-Fi сети; • Тип шифрования; • Тип аутентификации.

Настройка	ОС	Описание
Приложения	`Windows` `macOS` `Linux`	*Список доверенных приложений* – это список приложений, у которых Kaspersky Endpoint Security не контролирует файловую и сетевую активности (в том числе и вредоносную), а также обращения этих приложений к системному реестру. По умолчанию Kaspersky Endpoint Security контролирует объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех приложений и создаваемый ими сетевой трафик. После добавления приложения в список доверенных приложений Kaspersky Endpoint Security перестает контролировать активность приложения.
Исключения из Поиска вредоносного ПО	`Windows` `macOS` `Linux`	*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".
Устройства	`Windows` `Linux`	*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.

Общие настройки

Настройки обнаружения

для Windows, macOS и Linux

Этот раздел позволяет вам настроить параметры обнаружения в соответствии с вашими потребностями. Эффективность обнаружения и предотвращения угроз зависит от правильно выбранных настроек.

Настройки обнаружения

Настройка	ОС	Описание
Обнаружение других типов объектов	`Windows` `macOS` `Linux`	Вне зависимости от настроенных параметров приложения Kaspersky Endpoint Security всегда обнаруживает и блокирует вирусы, черви, трояны и вредоносные утилиты. Эти приложения могут нанести значительный вред компьютеру. Дополнительно можно включить обнаружение следующих типов объектов: • **Легальные приложения, 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". • `Windows` **Рекламные приложения**. Приложения, которые отображают в интерфейсе других программ рекламные баннеры и перенаправляют поисковые запросы на рекламные веб-страницы. • `Windows` **Приложения автодозвона**. Приложения автодозвона могут устанавливать телефонные соединения через модем в скрытом режиме. Такие приложения также являются легальными программами, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя. • `Windows` **Упаковщики**. Чтобы скрыть вредоносные программы от обнаружения антивирусом, злоумышленники упаковывают их с помощью специальных упаковщиков. Специалисты "Лаборатории Касперского" выделили упаковщики, которые злоумышленники используют чаще всего.

Настройка	ОС	Описание
Технология лечения активного заражения	`Windows`	Как правило, компоненты Kaspersky Endpoint Security при обнаружении вредоносной активности завершают работу вредоносного приложения до заражения компьютера. Технология лечения активного заражения обеспечивает защиту компьютера от уже действующих вредоносных приложений (активное заражение), минимизируя риски потери данных и распространения угрозы. Если технология включена, при обнаружении вредоносной активности Kaspersky Endpoint Security показывает всплывающее уведомление. В уведомлении приложение Kaspersky Endpoint Security предлагает провести процедуру лечения активного заражения компьютера. После подтверждения пользователем этой процедуры приложение Kaspersky Endpoint Security устраняет угрозу, затем выполняет перезагрузку компьютера. Применение технологии лечения активного заражения требует значительных ресурсов компьютера, что может замедлить работу других приложений. Во время обнаружения приложением активного заражения некоторые функции операционной системы могут быть недоступны. Доступность операционной системы восстановится после завершения лечения активного заражения и перезагрузки компьютера. Если приложение Kaspersky Endpoint Security установлено на компьютере под управлением операционной системы Windows для серверов, Kaspersky Endpoint Security не показывает уведомление. Таким образом, пользователь не может выбрать действие для лечения активного заражения. Для устранения угрозы вам необходимо включить технологию лечения активного заражения в параметрах приложения и включить немедленное лечение активного заражения в свойствах задачи *Поиск вредоносного ПО*. Далее вам нужно запустить задачу *Поиск вредоносного ПО*.
Блокировать доступ к файлам во время проверки	`Linux`	Если флажок установлен, приложение блокирует доступ к файлам на время проверки компонентами Защита от файловых угроз и Контроль устройств, действия Запрет запуска объектов и задачи Проверка съемных дисков. Если флажок снят, на время проверки обращение к любому файлу разрешается, проверка выполняется в асинхронном режиме.
Настройки записи событий в журнал	`Linux`	**Сообщать о незараженных объектах**. Если флажок установлен, приложение записывает в журнал событие *ObjectProcessed* для всех проверяемых объектов. **Сообщать о необработанных объектах**. Если флажок установлен, приложение записывает в журнал событие *ObjectNotProcessed*. **Сообщать об упакованных объектах**. Если флажок установлен, приложение записывает в журнал событие *PackedObjectDetected*.

Kaspersky Security Network

для Windows, macOS и Linux

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть Kaspersky Security Network.

Функциональность KSN может быть недоступна в приложении на территории США.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, приложение Kaspersky Endpoint Security получает от служб KSN сведения о репутации проверяемых веб-адресов, а также сведения о категории и репутации проверяемых файлов. Подробнее о настройке доступа к KSN см. в справке Kaspersky Security Center.

Использование Kaspersky Security Network является добровольным. Приложение предлагает использовать KSN во время первоначальной настройки приложения. Начать или прекратить использование KSN можно в любой момент.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского". Файл ksn_<ID языка>.txt с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения.

Инфраструктура репутационных баз "Лаборатории Касперского"

Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения для работы с репутационными базами "Лаборатории Касперского":

- *Kaspersky Security Network (KSN)* – это решение, которое используют большинство приложений "Лаборатории Касперского". Участники KSN получают информацию от "Лаборатории Касперского", а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.

- *Kaspersky Private Security Network (KPSN)* – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров. KPSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

  - отсутствие подключения локальных рабочих мест к сети Интернет;

  - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

Настройки Kaspersky Security Network

Настройка	ОС	Описание
Использовать расширенный режим KSN	`Windows` `macOS` `Linux`	*Расширенный режим KSN* – режим работы приложения, при котором Kaspersky Endpoint Security передает в "Лабораторию Касперского" дополнительные данные. Независимо от положения переключателя, Kaspersky Endpoint Security использует KSN для обнаружения угроз. `Linux` Для Linux-устройств настройка скрывается, если используется решение *Kaspersky Private Security Network (KPSN)*.
Использовать облачный режим	`Windows` `macOS` `Linux`	*Облачный режим* – режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию антивирусных баз. Работу приложения с облегченными антивирусными базами обеспечивает Kaspersky Security Network. Облегченная версия антивирусных баз позволяет снизить нагрузку на оперативную память компьютера примерно в два раза. Если вы не участвуете в Kaspersky Security Network или облачный режим выключен, Kaspersky Endpoint Security загружает полную версию антивирусных баз с серверов "Лаборатории Касперского". Если флажок установлен, то Kaspersky Endpoint Security использует облегченную версию антивирусных баз, за счет чего снижается нагрузка на ресурсы операционной системы. Kaspersky Endpoint Security загружает облегченную версию антивирусных баз в ходе ближайшего обновления после того, как флажок был установлен. Если флажок снят, то Kaspersky Endpoint Security использует полную версию антивирусных баз. Kaspersky Endpoint Security загружает полную версию антивирусных баз в ходе ближайшего обновления после того, как флажок был снят.

Настройка	ОС	Описание
Статус компьютера при недоступности серверов KSN	`Windows`	Раскрывающийся список, элементы которого определяют статус компьютера в Kaspersky Security Center при недоступности серверов KSN.
Использовать Сервер администрирования как прокси-сервер KSN	`Windows` `macOS` `Linux`	Если флажок установлен, то Kaspersky Endpoint Security использует службу KSN Proxy. Вы можете настроить параметры службы KSN Proxy в свойствах Сервера администрирования.
Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен	`Windows` `macOS` `Linux`	Если флажок установлен, Kaspersky Endpoint Security использует серверы KSN, когда служба KSN Proxy недоступна. Серверы KSN могут быть расположены как в "Лаборатории Касперского", так и на сторонних серверах, в случае использования Kaspersky Private Security Network.

Взаимодействие с пользователем

для Windows, macOS и Linux

Этот раздел позволяет вам настроить параметры интерфейса приложения, а также параметры взаимодействия приложения с пользователем.

Настройки интерфейса приложения

Настройка	ОС	Описание
Запускать Kaspersky Endpoint Security при включении компьютера (рекомендуется)	`Windows` `macOS`	Если функция включена, то приложение Kaspersky Endpoint Security запускается после загрузки операционной системы и защищает компьютер пользователя в течение всего сеанса работы. Если функция отключена, то приложение Kaspersky Endpoint Security не запускается после загрузки операционной системы до того момента, как пользователь запустит приложение вручную. Защита компьютера выключена и данные пользователя могут находиться под угрозой.
Показывать значок приложения	`Windows` `macOS`	На клиентском компьютере доступен значок приложения в области уведомлений. В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает уведомления над значком приложения.
Не отображать интерфейс приложения для пользователей	`Windows` `macOS`	Если флажок установлен, Kaspersky Endpoint Security запрещает пользователю открывать главное окно приложения и скрывает интерфейс приложения на удаленном компьютере. Если флажок снят, пользователь может открывать главное окно Kaspersky Endpoint Security и использовать интерфейс приложения на удаленном компьютере.
Скрыть раздел Мониторинг активности приложений	`Windows`	Если флажок установлен, на клиентском компьютере в главном окне Kaspersky Endpoint Security недоступна кнопка **Мониторинг активности приложений**. *Мониторинг активности приложений* – это инструмент, предназначенный для просмотра информации об активности приложений на компьютере пользователя в режиме реального времени.
Локально управлять обновлениями	`macOS`	Если флажок установлен, пользователь может локально управлять обновлениями Kaspersky Endpoint Security на удаленном компьютере. Если флажок снят, вы можете управлять обновлениями Kaspersky Endpoint Security на удаленном компьютере только с помощью плагина управления Kaspersky Endpoint Security в Kaspersky Security Center.
Локально управлять ключами	`macOS`	Если флажок установлен, пользователь может локально управлять ключами Kaspersky Endpoint Security на удаленном компьютере. Если флажок снят, вы можете управлять ключами Kaspersky Endpoint Security на удаленном компьютере только с помощью плагина управления Kaspersky Endpoint Security в Kaspersky Security Center.
Завершать работу приложения	`macOS`	Если флажок установлен, пункт **Выход** отображается в контекстном меню значка приложения. Пользователь удаленного компьютера может завершить работу Kaspersky Endpoint Security на удаленном компьютере. Если флажок снят, пункт **Выход** недоступен в контекстном меню значка приложения. Пользователь удаленного компьютера не может завершить работу Kaspersky Endpoint Security на удаленном компьютере.

Настройка	ОС	Описание
Доступ к локальным задачам	`Windows` `Linux`	Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь, при отсутствии дополнительных ограничений политики, может настраивать и запускать задачи. При этом параметры расписания запуска задачи остаются недоступными для пользователя. Пользователь может запускать задачи только вручную. Если флажок снят, то использование локальных задач прекращается. В этом режиме локальные задачи не запускаются по расписанию. Задачи недоступны для запуска и настройки в локальном интерфейсе Kaspersky Endpoint Security, а также при работе с командной строкой. Пользователь по-прежнему может запустить проверку файла или папки, выбрав пункт **Проверить на вирусы** в контекстном меню файла или папки. При этом задача проверки запустится со значениями параметров, установленными по умолчанию для задачи выборочной проверки.
Просмотр групповых задач	`Windows`	Если флажок установлен, то групповые задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь может просмотреть полный список задач в интерфейсе приложения. Если флажок снят, Kaspersky Endpoint Security показывает пустой список задач.
Управление групповыми задачами	`Windows` `Linux`	Если флажок установлен, пользователь может запускать и останавливать заданные в консоли Kaspersky Endpoint Security групповые задачи. Пользователь может запускать и останавливать задачи в интерфейсе приложения или в упрощенном интерфейсе приложения. Если флажок снят, Kaspersky Endpoint Security запускает задачи автоматически по расписанию, или администратор запускает задачи вручную в консоли Kaspersky Endpoint Security.
Статус компьютера	`Windows`	Параметры отображения статусов клиентских компьютеров с установленным приложением Kaspersky Endpoint Security в Web Console при появлении ошибок применения политики или выполнения задачи. Доступны статусы *OK*, *Предупреждение* и *Критический*.
Уведомления о статусе приложения	`Windows`	Параметры отображения уведомлений о событиях, возникающих в работе программы, в области уведомлений. Установите флажки напротив тех категорий событий, уведомления о которых вы хотите видеть в области уведомлений. • **Наличие активных угроз**. • **Необходимость перезагрузки компьютера**. • **Проблемы с базами вредоносного ПО**. • **Проблемы с уровнем защиты**. • **Проблемы с лицензией**. • **Наличие обновлений**. При возникновении событий, относящихся к выбранным категориям, значок приложения в области уведомлений будет меняться на или в зависимости от важности предупреждения.
Уведомления о состоянии локальных баз вредоносного ПО	`Windows`	Параметры уведомлений о неактуальности антивирусных баз, которые использует приложение. Вы можете указать количество дней, через которое Kaspersky Endpoint Security отправит пользователю уведомления "Базы устарели" и "Базы сильно устарели".
Настройки запуска приложения	`Linux`	Параметры запуска приложения: • **Максимальное количество неудачных последовательных попыток запуска приложения**. • **Максимальное время ожидания запуска приложения (мин.)**. По истечению указанного периода ожидания запуска приложения процесс kesl будет перезапущен.

Настройка	ОС	Описание
Устанавливать обновления приложения без перезагрузки	`Windows`	Обновление приложения без перезагрузки позволяет обеспечить бесперебойную работу серверов при обновлении версии приложения. Обновление приложения без перезагрузки имеет следующие ограничения: • Вы можете обновлять версию приложения без перезагрузки начиная с версии 11.10.0. Для обновление более ранних версий приложения необходимо выполнять перезагрузку компьютера. • Вы можете устанавливать патчи без перезагрузки начиная с версии 11.11.0. Для установки патчей для более ранних версий приложения может потребоваться перезагрузка компьютера. • Обновление версии приложения без перезагрузки невозможно выполнить на компьютерах с включенным шифрованием данных (Шифрование Kaspersky (FDE), BitLocker, Шифрование файлов (FLE)). Для обновления версии приложения на компьютерах с включенным шифрованием данных необходимо выполнять перезагрузку компьютера. • Обновление версии приложения без перезагрузки невозможно выполнить на виртуальных машинах. Для обновления версии приложения на виртуальных машинах необходимо выполнять перезагрузку виртуальной машины. После обновления Kaspersky Endpoint Security до версии 11.10.0 и выше без перезагрузки на компьютере будет установлено два приложения Kaspersky Endpoint Security. Не удаляйте предыдущую версию приложения вручную. Предыдущая версия приложения будет удалена автоматически после перезагрузки компьютера. Значение параметра по умолчанию отличается в зависимости от типа операционной системы. Если приложение установлено на рабочую станцию, функция обновления без перезагрузки выключена. Если приложение установлено на сервер, функция обновления без перезагрузки включена.
Совместимость с приложениями для удаленного администрирования	`Windows`	При появлении сбоев в работе Kaspersky Endpoint Security с инструментами для удаленного администрирования (англ. Remote Administration Tool, RAT) вы можете включить режим совместимости. Сбои могут быть связаны с проблемами совместимости RAT и функции безопасного рабочего стола (англ. Secure Desktop) приложения. Эта функция предназначена для подтверждения действий, которые могут снизить безопасность компьютера. Функция позволяет приложению показывать диалоговое окно подтверждения, изолированное от других процессов. Функция обеспечивает безопасность запроса за счет повышенных прав. Таким образом, подтвердить действие может только пользователь, а не вредоносное ПО. Режим совместимости с RAT может снизить уровень безопасности компьютера. Рекомендуется не включать режим совместимости, если Kaspersky Endpoint Security с RAT работает корректно. По умолчанию функция выключена. Пример. При работе с браузером в режиме RemoteApp Kaspersky Endpoint Security может не показывать диалоговое окно подтверждения при переходе на сайт с недоверенным сертификатом, так как RemoteApp не поддерживает функцию безопасного рабочего стола приложения. Это может привести к тому, что браузер перестает отвечать. Для корректной работы браузера в режиме RemoteApp нужно включить режим совместимости. Вы также можете попробовать включить режим совместимости при появлении сбоев в работе функции безопасного рабочего стола с другим сторонним ПО.

Производительность

для Windows, macOS и Linux

Под производительностью Kaspersky Endpoint Security подразумевается потребление энергии и ресурсов компьютера.

Настройка	ОС	Описание
Уступать ресурсы другим приложениям	`Windows`	Потребление ресурсов компьютера Kaspersky Endpoint Security при проверке компьютера может увеличить нагрузку на центральный процессор и дисковые подсистемы. Это может замедлить работу других приложений. Для оптимизации производительности в Kaspersky Endpoint Security предусмотрен *режим передачи ресурсов другим приложениям*. В этом режиме операционная система может понизить приоритет потоков задач проверки Kaspersky Endpoint Security при высокой нагрузке на центральный процессор. Это позволит перераспределить ресурсы операционной системы для других приложений. То есть задачи проверки получат меньше процессорного времени. В результате Kaspersky Endpoint Security будет проверять компьютер дольше. По умолчанию режим передачи ресурсов другим приложениям включен.
Откладывать или пропускать задачи по расписанию при работе от аккумулятора	`Windows` `macOS` `Linux`	Если функция включена, то Kaspersky Endpoint Security переходит в режим энергосбережения. `Windows` Приложение Kaspersky Endpoint Security *откладывает* выполнение задач, для которых задан запуск по расписанию. По мере необходимости вы можете самостоятельно запускать задачи проверки и обновления. `macOS` `Linux` Приложение Kaspersky Endpoint Security *отменяет* выполнение задач, для которых задан запуск по расписанию. По мере необходимости вы можете самостоятельно запускать задачи проверки и обновления. Если включен режим энергосбережения, при работе от аккумулятора не запускаются следующие задачи, даже если для них задан запуск по расписанию: • *Поиск вредоносного ПО*; • *Обновление баз вредоносного ПО*; • *Проверка целостности приложения*; • *Поиск IOC*.
Ограничить потребление ресурсов процессора для задач проверки	`Windows` `macOS` `Linux`	Для оптимизации производительности Kaspersky Endpoint Security вы можете ограничить использование ресурсов процессора для задач проверки. В зависимости от операционной системы отличается список задач, для которых ограничивается использование ресурсов процессора: • `Windows` `Linux` Поиск вредоносного ПО • `macOS` `Linux` Проверка важных областей • `Linux` Инвентаризация • `Linux` Проверка контейнеров Если функция включена, средняя нагрузка на все ядра процессора при выполнении задач проверки стремится к указанному значению.
Ограничение на использование памяти для задач проверки (МБ)	`Linux`	Вы можете настраивать ограничение на использование памяти для задач проверки (*Поиск вредоносного ПО*, *Проверка важных областей*, *Инвентаризация* и *Проверка контейнеров*).
Настроить исключение памяти процессов из проверки	`Linux`	Вы можете настраивать исключения из проверки памяти процессов. Приложение не будет проверять память указанных процессов. Укажите путь к процессам, которые приложение исключит из проверки памяти процессов. Для указания пути вы можете использовать маски. По умолчанию список пуст.
Ограничить использование памяти приложением	`Linux`	Вы можете настраивать ограничение на использование резидентной памяти приложением. По умолчанию установлено автоматическое ограничение. **Метод расчета ограничения**: • **Без ограничений**. При выборе этого элемента списка использование резидентной памяти не ограничивается. • **Задать точное значение (%)**. • **Задать точное значение (МБ)**. • **Использовать меньшее из двух значений (% или МБ)**. • **Использовать большее из двух значений (% или МБ)**. • **Ограничивать автоматически (рекомендуется)**. При выборе этого элемента списка использование резидентной памяти ограничивается автоматически.
Включить мониторинг стабильности работы приложения	`Linux`	Вы можете включать и выключать мониторинг стабильности работы приложения Kaspersky Endpoint Security, который позволяет отслеживать количество нештатных остановок приложения и уведомлять администратора о нестабильной работе приложения. Если флажок установлен, приложение отслеживает состояние работы Kaspersky Endpoint Security. Для применения параметра требуется перезапустить приложение. Если приложение работает нестабильно, в свойствах устройства с установленным приложением отображается сообщение: *<Количество> нештатных остановок приложения начиная с <дата и время>*.

Настройки сети

для Windows, macOS и Linux

Вы можете настроить параметры прокси-сервера для подключения к интернету, выбрать режим контроля сетевых портов и настроить проверку защищенных соединений.

Настройки сети

Настройка	ОС	Описание
Доверенные корневые сертификаты	`Windows` `macOS` `Linux`	Список доверенных корневых сертификатов. Kaspersky Endpoint Security позволяет устанавливать доверенные корневые сертификаты на компьютеры пользователей, если, например, вам нужно развернуть новый центр сертификации. Приложение позволяет добавить сертификат в специальное хранилище сертификатов Kaspersky Endpoint Security. При этом сертификат будет доверенным только для приложения Kaspersky Endpoint Security. То есть пользователь будет иметь доступ к веб-сайту с новым сертификатом в браузере. Если другое приложение попытается получить доступ к веб-сайту, вы можете получить ошибку соединения из-за проблем с сертификатом. Для добавления сертификата в системное хранилище сертификатов, вы можете использовать групповые политики Active Directory.
Прокси-сервер	`Windows` `macOS` `Linux`	Параметры прокси-сервера для доступа пользователей клиентских компьютеров в интернет. Приложение Kaspersky Endpoint Security использует эти параметры в работе некоторых компонентов защиты, в том числе для обновления баз и модулей приложения.
Использовать аутентификацию на прокси-сервере	`Windows` `macOS` `Linux`	Если флажок установлен, приложение использует аутентификацию с помощью имени пользователя и пароля при соединении с прокси-сервером. `Windows` Для Windows-устройств требуется выбрать тип аутентификации: • **NTLM-аутентификация**. NTLM-аутентификация с помощью учетной записи текущего пользователя (значение по умолчанию). • **NTLM-аутентификация с именем пользователя и паролем**. NTLM-аутентификация с помощью учетных данных, заданных вручную. • **Имя пользователя и пароль**. Аутентификация с использованием учетных данных, заданных вручную. • **Автоматическая аутентификация**. • **Kerberos-аутентификация.** Kerberos-аутентификация с помощью учетной записи текущего пользователя. • **Kerberos-аутентификация с именем пользователя и паролем**. Kerberos-аутентификация с использованием учетных данных, заданных вручную.
Не использовать прокси-сервер для локальных адресов	`Windows` `macOS`	Если флажок установлен, то при обновлении Kaspersky Endpoint Security из папки общего доступа прокси-сервер не используется.
Не использовать прокси-сервер для компонентов	`Linux`	Установите флажки рядом с теми компонентами приложения, в работе которых не нужно использовать прокси-сервер: • **Endpoint Detection and Response Expert (on-premise)** – не использовать прокси-сервер при подключении к серверам KATA. • **KATA Sandbox** – не использовать прокси-сервер при подключении к серверам Central Node, обеспечивающим взаимодействие с KATA Sandbox. • **Network Detection and Response (KATA)** – не использовать прокси-сервер при подключении к серверам Network Detection and Response.
Не использовать прокси-сервер для указанных IP-адресов и DNS-имен	`Linux`	Таблица содержит список IP-адресов и DNS-имен, для подключения к которым не будет использоваться прокси-сервер. Для указания адреса вы можете использовать маски (символы `*` и `?`). Вы можете добавлять, изменять, удалять адреса в таблице.
Проверка защищенных соединений	`Windows` `macOS` `Linux`	Функция позволяет компонентам Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Cloud Discovery контролировать и обрабатывать зашифрованные соединения (соединения по протоколу HTTPS). `Linux` Для Linux-устройств доступна **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.

Настройка	ОС	Описание
Доверенные домены	`Windows` `Linux`	Список веб-адресов, для которых Kaspersky Endpoint Security не проверяет сетевые соединения. В этом случае Kaspersky Endpoint Security не будет проверять HTTPS-трафик доверенных веб-адресов при работе компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль. Вы можете ввести имя домена или IP-адрес. Kaspersky Endpoint Security поддерживает символ `*` для ввода маски в имени домена.
Ограничивать трафик при лимитном подключении	`Windows`	Если флажок установлен, приложение ограничивает собственный сетевой трафик в том случае, если подключение к интернету является лимитным. Приложение Kaspersky Endpoint Security определяет высокоскоростное мобильное подключение к интернету как лимитное, а подключение по Wi-Fi – как безлимитное. Учет стоимости подключения работает на компьютерах под управлением Windows 8 и выше.
Внедрять в трафик скрипт взаимодействия с веб-страницами	`Windows`	Если флажок установлен, Kaspersky Endpoint Security внедряет в трафик скрипт взаимодействия с веб-страницами. Этот скрипт обеспечивает работу компонента Веб-Контроль. Скрипт позволяет регистрировать события работы Веб-Контроля. Специалисты "Лаборатории Касперского" рекомендуют внедрить в трафик скрипт взаимодействия с веб-страницами для корректной работы Веб-Контроля.
Расшифровать защищенное соединение с сайтом, использующим EV-сертификат	`Windows`	EV-сертификаты (англ. Extended Validation Certificate) подтверждают подлинность веб-сайтов и повышают безопасность соединения. Браузеры сообщают о наличии на веб-сайте EV-сертификата с помощью значка замка в адресной строке браузера. Также браузеры могут полностью или частично окрашивать адресную строку в зеленый цвет. Если переключатель включен, приложение расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если переключатель выключен, приложение не имеет доступа к содержанию HTTPS-трафика. Поэтому приложение контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://bing.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.
Блокировать соединения по протоколу SSL 2.0	`Windows`	Если флажок установлен, то приложение контролирует и блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. При этом приложение не контролирует сетевой трафик по этому протоколу.
Блокировать соединения по протоколу TLS 1.0	`Windows`	Если флажок установлен, то приложение блокирует сетевые соединения, устанавливаемые по протоколу TLS 1.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу TLS 1.0. Приложение контролирует сетевой трафик по этому протоколу. Все компоненты приложения работают без ограничений.
Блокировать соединения по протоколу SSL 3.0	`Windows`	Если флажок установлен, то приложение блокирует сетевые соединения, устанавливаемые по протоколу SSL 3.0. Если флажок снят, то приложение не блокирует сетевые соединения, устанавливаемые по протоколу SSL 3.0. Приложение контролирует сетевой трафик по этому протоколу. Все компоненты приложения работают без ограничений.
Контролируемые порты	`Windows` `macOS` `Linux`	**Контролировать все сетевые порты**. Режим контроля сетевых портов, при котором компоненты защиты (Защита от файловых угроз, Защита от веб-угроз, Защита от почтовых угроз) контролируют потоки данных, передаваемые через любые открытые сетевые порты компьютера. **Контролировать только выбранные сетевые порты**. Режим контроля сетевых портов, при котором компоненты защиты контролируют выбранные сетевые порты компьютера и сетевую активность выбранных приложений. Список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика, настроен в соответствии с рекомендациями специалистов "Лаборатории Касперского". Для Mac-устройств возможно контролировать только выбранные порты.
Контролируемые приложения	`Windows`	Список приложений, для которых весь трафик на всех портах будет контролироваться вне зависимости от настроек проверки портов.

Настройка	ОС	Описание
Выберите, какое хранилище сертификатов будет использовать браузер Firefox	macOS	**Связка ключей для корневых системных сертификатов (рекомендовано)**. Если выбран этот вариант, Kaspersky Endpoint Security использует корневой сертификат из связки ключей System Roots для проверки зашифрованного HTTPS-трафика в браузере Mozilla Firefox. Этот вариант выбран по умолчанию. **Хранилище сертификатов в настройках браузера Mozilla Firefox**. Если выбран этот вариант, Kaspersky Endpoint Security использует сертификат из хранилища сертификатов браузера. В этом случае вам нужно вручную добавить сертификат Kaspersky Endpoint Security в хранилище сертификатов браузера Mozilla Firefox. Дополнительные сведения см. в статье Как добавить сертификат Kaspersky в хранилище сертификатов Mozilla Firefox.
Режим перехвата трафика	Linux	**iptables**. Kaspersky Endpoint Security использует для перехвата трафика утилиту iptables. **eBPF**. Приложение использует для перехвата трафика технологию eBPF.

Проверка контейнеров

для Linux

Приложение проверяет в реальном времени запущенные контейнеры и пространства имен. Приложение поддерживает интеграцию с системой управления контейнерами Docker, средой CRI-O, утилитами Podman и runc.

Для работы компонента Проверка контейнеров должен быть включен компонент Защита от файловых угроз. Во время проверки контейнеров и пространств имен используются параметры защиты от файловых угроз.

Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с контейнерами и пространствами имен.

Настройки Проверки контейнеров

Настройка	ОС	Описание
Действие при обнаружении угрозы	Linux	**Пропустить контейнер**. При обнаружении зараженного объекта приложение не выполняет никаких действий над контейнером. **Остановить контейнер**. При обнаружении зараженного объекта приложение останавливает контейнер. **Остановить контейнер, если не удалось вылечить**. Если не удалось вылечить зараженный объект, приложение останавливает контейнер.
Использовать Docker	Linux	Использование среды Docker. Для использования среды нужно ввести путь или URI (универсальный идентификатор ресурса) Docker-сокета.
Использовать CRI-O	Linux	Использование среды CRI-O. Для использования среды нужно ввести путь к конфигурационному файлу CRI-O.
Использовать Podman	Linux	Использование утилиты Podman. Для использования утилиты нужно ввести путь к исполняемому файлу утилиты и путь к корневой директории хранилища контейнеров.
Использовать runc	Linux	Использование утилиты runc. Для использования утилиты нужно ввести путь к исполняемому файлу утилиты и путь к корневой директории хранилища состояний контейнеров.

Служба технической поддержки

для Windows и Linux

Для исследования возможных сбоев Kaspersky Endpoint Security на компьютерах специалистам Службы технической поддержки может понадобиться информация о системе и о событиях, произошедших в ходе работы приложения. Эта информация хранится в файлах дампов и файлах трассировки.

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Security на момент создания этого файла дампа.

Файл трассировки позволяет отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка.

Файлы дампов и файлы трассировки могут содержать конфиденциальные данные. Для контроля доступа к данным вам нужно самостоятельно обеспечить защиту этих файлов.

Файлы дампов и файлы трассировки хранятся на вашем компьютере в течение всего времени использования приложения и безвозвратно удаляются при удалении приложения.

После применения профиля безопасности на компьютерах приложение начинает записывать файлы дампов. После сбоя при следующем запуске приложение открывает окно загрузки информации для Службы технической поддержки. В этом окне вы сможете просмотреть информацию о созданных файлах дампов и подтвердить отправку файлов в "Лабораторию Касперского".

Настройки технической поддержки

Настройка	ОС	Описание
Запись дампов	`Windows` `Linux`	Если запись дампов включена, Kaspersky Endpoint Security создает файлы дампов при сбое в работе приложения. `Linux` Файлы дампов требуют значительного места на диске. Если на жестком диске менее 4 ГБ свободного места, включение записи дампов может привести к заполнению всего свободного пространства на диске.
Защита файлов дампов и файлов трассировки	`Windows`	Если защита файлов дампов и файлов трассировки включена, доступ к файлам имеют следующие пользователи: • К файлам дампов имеют доступ системный и локальный администраторы, а также пользователь, включивший запись файлов дампов и файлов трассировки. • К файлам трассировки имеют доступ только системный и локальный администраторы.
Путь к файлу дампа	`Windows` `Linux`	Файлы дампов хранятся в следующих папках: • `Windows`: `%ProgramData%\Kaspersky Lab\KES.[AppVersion]\Traces`. Изменить папку, в которой хранятся файлы дампов, нельзя. • `Linux`: `var/opt/kaspersky/kesl/common/dumps` и `var/opt/kaspersky/kesl/common/dumps-user`. 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, где хранятся файлы дампов по умолчанию, требуются root-права.
Путь к папке трассировки	`Windows` `Linux`	Файлы трассировки хранятся в следующих папках: • `Windows`: `%ProgramData%\Kaspersky Lab\KES.[AppVersion]\Traces`. Изменить папку, в которой хранятся файлы трассировки, нельзя. • `Linux`: `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, где хранятся файлы трассировки по умолчанию, требуются root-права.
Максимальный размер файла трассировки (МБ)	`Linux`	Поле ввода максимального размера файла трассировки приложения (в мегабайтах).
Максимальное количество файлов трассировки	`Linux`	Поле ввода максимального количества файлов трассировки приложения.
Веб-ресурсы Службы технической поддержки	`Windows`	Таблица с контактами технической поддержки, к которой пользователи могут обратиться в случае сбоев в приложении Kaspersky Endpoint Security. Также вы можете настроить шаблоны сообщений для пользователей с инструкцией как получить помощь. По умолчанию в приложении размещены ссылки на сайт Kaspersky.

Отчеты и хранилище

для Windows, macOS и Linux

Этот раздел позволяет вам настроить параметры создания и хранения отчетов о событиях, которые происходят во время работы Kaspersky Endpoint Security, а также настроить хранение объектов в резервном хранилище и карантине.

Отчеты

Информация о работе каждого компонента Kaspersky Endpoint Security, о событиях шифрования данных, о выполнении каждой задачи проверки, задачи обновления и задачи проверки целостности, а также о работе приложения в целом сохраняется в *отчетах*.

`Windows` Отчеты хранятся в папке `C:\ProgramData\Kaspersky Lab\KES.12.4.0\Report`.

Резервное хранилище

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке:

- `Windows`: `C:\ProgramData\Kaspersky Lab\KES.12.4.0\QB`.
- `Linux`: `/var/opt/kaspersky/kesl/common/objects-backup/`.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security.

Карантин

Карантин – это специальное локальное хранилище на компьютере. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства.

Настройки Отчетов и хранилища

Настройка	ОС	Описание
Удалять отчеты через (дни)	`Windows` `macOS`	Если флажок установлен, то максимальный срок хранения отчетов ограничен заданным интервалом времени. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчета.
Ограничить размер файла отчетов до (МБ)	`Windows`	Если флажок установлен, то максимальный размер файла отчетов ограничен заданным значением. После достижения максимального размера файла отчета Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчетов таким образом, чтобы размер файла отчетов не превышал максимального значения.

Настройка	ОС	Описание
Сохранять только недавние события	macOS	Если флажок установлен, во время каждого запуска задачи Kaspersky Endpoint Security удаляет информацию о некритических событиях, которые произошли с момента предыдущего запуска задачи, но сохраняет в отчете важную информацию (например, об обнаруженных вредоносных объектах).
Записывать некритические события	macOS	Если флажок установлен, то Kaspersky Endpoint Security записывает события некритического характера (например, информационные события) в отчет. События некритического характера не влияют на обеспечение защиты.
Удалять объекты через (дни)	Windows macOS Linux	Если флажок установлен, то максимальный срок хранения файлов ограничен заданным интервалом времени. По истечении максимального срока хранения Kaspersky Endpoint Security удаляет наиболее старые файлы из резервного хранилища.
Ограничить размер резервного хранилища до (МБ)	Windows Linux	Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. После достижения максимального размера резервного хранилища приложение Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения.
Ограничить размер карантина	Windows Linux	**Максимальный размер карантина (МБ)**. Если флажок установлен, то максимальный размер карантина ограничен заданным значением. При достижении максимального размера карантина Kaspersky Endpoint Security отправляет событие в Kaspersky Security Center *Недостаточно места в хранилище карантина* и создает событие в журнале событий операционной системы. При этом приложение прекращает помещать новые объекты на карантин. Вам нужно вручную очистить карантин. **Уведомлять при заполнении карантина на (%)**. Пороговое значение карантина. Например, вы можете задать пороговое значение карантина 50 %. При достижении порогового значения карантина, приложение отправляет соответствующее событие в Kaspersky Security Center и публикует событие в системном журнале событий. При этом приложение продолжает помещать новые объекты на карантин.

Интеграция с KSC

Этот раздел позволяет вам настроить интеграцию Kaspersky Endpoint Security с Kaspersky Security Center.

Настройки Интеграции с Kaspersky Security Center

Настройка	ОС	Описание
Использовать Kaspersky Security Center в качестве прокси-сервера для активации	Windows macOS Linux	Если флажок установлен, то для подключения к серверам активации приложение использует Сервер администрирования Kaspersky Security Center в качестве прокси-сервера. Это нужно при активации приложения в изолированном сегменте сети без доступа в интернет с помощью кода активации. При активации приложения с помощью файла ключа доступ в интернет не нужен. Неприменимо, если приложение используется в режиме Легкого агента.
Передача данных на Сервер администрирования	Windows macOS Linux	Категории событий на клиентских компьютерах, информация о которых должна передаваться на Сервер администрирования. Вы можете выключить передачу некоторых данных для оптимизации дискового пространства на Сервере администрирования. Приложение передает следующие категории событий: • Windows **О цепочке развития угрозы**. • Windows macOS Linux **О файлах карантина**. • Windows Linux **О файлах в резервном хранилище**. • Windows Linux **О необработанных файлах**. • Windows macOS Linux **Об установленных устройствах**. • Windows Linux **О запускаемых приложениях**. • Windows **Об ошибках шифрования файлов**. • Windows **Отчет о состоянии правил Адаптивного контроля аномалий**. • Windows **Отчет о срабатываниях правил Адаптивного контроля аномалий**.

Настройки взаимодействия с ОС

для Linux

Для полноценной работы приложение должно использовать перехват системных событий – файловых операций и запуска процессов. Если приложение не использует перехват системных событий, проверка файлов в режиме реального времени не выполняется, уровень защиты устройства снижается.

Настройки взаимодействия с ОС

Настройка	ОС	Описание
Механизм перехвата	`Linux`	Механизм перехвата системных событий, который приложение использует в своей работе: • **Технология fanotify**. 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.
Если обновляемый модуль ядра не запускается	`Linux`	Действие, которое приложение выполняет в случае ошибки запуска обновляемого модуля ядра: • **Использовать технологию fanotify**. Если выбран этот вариант, приложение переходит к использованию технологии fanotify для перехвата системных событий. • **Выключить перехват системных событий (снижение уровня защиты)**. Если приложение не использует перехват системных событий, проверка файлов в режиме реального времени не выполняется, уровень защиты устройства снижается. Настройка доступна, если выбран механизм перехвата **Обновляемый модуль ядра**.
Источник телеметрии	`Linux`	Источник, который приложение Kaspersky Endpoint Security использует для сбора телеметрии: • **Использовать только eBPF**. Приложение использует для сбора телеметрии только технологию eBPF. • **По умолчанию**. Приложение использует для сбора телеметрии технологию eBPF и службу auditd.
Режим работы auditd	`Linux`	Режим, в котором служба auditd записывает события аудита для дальнейшей передачи в решения Detection and Response: • **Монопольный**. Если выбран этот вариант, приложение Kaspersky Endpoint Security использует службу auditd в монопольном режиме. Сторонние приложения не могут подключаться в поток аудита. • **Режим многоадресной рассылки**. Если выбран этот вариант, служба auditd может принимать несколько подключений от разных процессов, использующих аудит системы.

Настройки уведомлений

для Windows, macOS и Linux

Этот раздел позволяет вам настроить отправку уведомлений о событиях на управляемых устройствах и общих событиях на адреса электронной почты пользователей этой рабочей области.

В процессе работы приложения возникают различного рода *события*. Они могут иметь информационный характер или нести важную информацию. Например, с помощью события приложение может уведомлять об успешно выполненном обновлении баз приложения или может фиксировать ошибку в работе компонента, которую требуется устранить.

События, возникающие в работе Kaspersky Endpoint Security, по уровню важности делятся на следующие типы:

- *Критические события* – события, представляющие серьезную угрозу безопасности компьютера (обнаружение вредоносных объектов, уязвимостей, проблем в работе Kaspersky Endpoint Security). Критические события требуют вашего немедленного внимания. Рекомендуется не выключать уведомления о возникновении критических событий.

- *Отказы функционирования* – события, возникающие при сбое в работе Kaspersky Endpoint Security (ошибка обработки, ошибка в настройках задачи). Такие события не представляют прямую угрозу безопасности компьютера, однако требуют ваших действий для корректной работы Kaspersky Endpoint Security по защите устройств.

- *Предупреждения* – события, которые не требуют ваших немедленных действий, но в дальнейшем могут представлять угрозу для безопасности компьютера.

- *Информационные сообщения* – события, носящие информационный характер.

Вне зависимости от того, включена или выключена доставка уведомлений, Kaspersky Endpoint Security записывает в отчеты приложения информацию о всех событиях, возникающих в работе приложения.

Для каждого события Kaspersky Endpoint Security вы можете настроить способ получения уведомлений:

- `Windows` **Уведомлять по почте**.

- `Windows` **Сохранять в локальном отчете**.

- `Windows` `macOS` **Уведомлять на экране**.

- `Windows` `Linux` **Сохранять в журнале событий операционной системы**.

Настройки телеметрии

для Windows, macOS и Linux

Этот раздел позволяет вам настроить отправку телеметрии с управляемых устройств на серверы сбора телеметрии. *Телеметрия* – список событий, которые произошли на защищаемом компьютере. Kaspersky Endpoint Security анализирует телеметрию и отправляет ее на серверы Kaspersky Anti Targeted Attack Platform или 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.

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.

Вы можете настроить параметры синхронизации для каждого встроенного агента в разделе "Встроенные агенты" и выбрать оптимальные значения исходя из нагрузки на сеть.

В этом разделе вы можете настроить:

- Правила включения и исключения из телеметрии.
- Сбор телеметрии, отправляемой на серверы KATA, серверы сбора телеметрии или серверы реагирования.

Телеметрия EDR Expert (on-premise)

для Windows, macOS и Linux

Настройки телеметрии EDR Expert (on-premise)

Настройка	ОС	Описание
Телеметрия EDR Expert (on-premise)	`Windows` `macOS` `Linux`	**Импорт** и **Экспорт**. Вы можете экспортировать настройки телеметрии EDR Expert (on-premise) 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 настроек отправляемых событий или для миграции списка в другую политику.
Общие исключения	`Windows` `macOS` `Linux`	Для оптимизации передаваемых данных вы можете настроить правила исключения для определенных типов событий. В этом случае Kaspersky Endpoint Security не собирает телеметрию, подходящую под условия правила. Это позволит уменьшить расход трафика и сократить количество событий от доверенных объектов и процессов. **Имя правила**. **Действие**: • **Не собирать**. Если выбран этот вариант, Kaspersky Endpoint Security не будет собирать телеметрию, удовлетворяющую условиям правила. • **Исключить IOA**. Если выбран этот вариант, Kaspersky Endpoint Security не будет собирать телеметрию на основании срабатывания IOA-правила. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. **Условие**. Условие срабатывания правила. Укажите параметр телеметрии, условный оператор и значение параметра. По умолчанию Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. Вы можете добавить несколько условий или группы условий, используя логические операторы И или ИЛИ.
Все типы событий	`Windows` `macOS` `Linux`	Список типов событий, для которых сбор телеметрии определяется по умолчанию "Лабораторией Касперского". Вы можете вручную настроить отправку на сервер каждого типа событии, а также правила исключения и включения телеметрии.

Телеметрия EDR (KATA) / NDR (KATA)

для Windows и Linux

Для повышения производительности и оптимизации отправки данных на сервер сбора телеметрии вы можете настроить исключения из телеметрии. Например, вы можете отменить обработку данных о сетевых коммуникациях для отдельных приложений.

Настройка	ОС	Описание
Исключенные процессы	`Windows` `Linux`	Kaspersky Endpoint Security не обрабатывает данные, связанные с процессами из списка. **Оптимизировать объем отправляемой телеметрии**. Kaspersky Endpoint Security позволяет оптимизировать объем отправляемых данных и исключить из телеметрии события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB, службы WinRM и процесса Агента администрирования klnagent.exe, а также расширенную информацию о типе сетевых пакетов для всех типов сетевых протоколов. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **Использовать для следующих типов событий**: • **Изменение файла**. • **Сетевые события**. • **Интерактивный ввод команд в консоли**. • **Модуль загружен**. • **Изменение в реестре**. • **Логи DNS**. • **Доступ к процессу**. • **Внедрение кода**. • `Windows` **Запрос WMI**. • **Канал**. • **LDAP**. • `Windows` **AMSI**.
Исключенные сетевые коммуникации	`Windows` `Linux`	Kaspersky Endpoint Security не обрабатывает данные, связанные с сетевыми коммуникациями из списка. В правиле исключения вы можете указать: **Название правила**. **Направление**. **Протокол**. **Необработанный сокет**. **Номер протокола**. **Локальный адрес**. Сетевой адрес компьютера, для которого Kaspersky Endpoint Security исключает телеметрию из сетевого трафика. **Локальный порт или диапазон**. **Удаленный адрес**. Сетевой адрес компьютера, для которого Kaspersky Endpoint Security исключает телеметрию из сетевого трафика. **Удаленный порт или диапазон**. Для IP-адресов поддерживается только формат IPv4. **Использовать правило для выбранных приложений**. Если флажок установлен, Kaspersky Endpoint Security исключает EDR-телеметрию из сетевого трафика для исполняемых файлов приложений из списка.

Настройка	ОС	Описание
Исключенные операции с файлами	`Windows` `Linux`	Kaspersky Endpoint Security не обрабатывает файловые операции из списка. В правиле исключения вы можете указать: **Название правила**. **Имя или маска файла**. Имя или маска имени файла, при доступе к которым Kaspersky Endpoint Security применяет правило исключения. Kaspersky Endpoint Security поддерживает символы `*` и `?` для ввода маски. **Выберите файловую операцию**. Тип файловой операции, к которой будет применяться правило. **Предыдущий путь**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные операции с DNS	`Windows` `Linux`	Kaspersky Endpoint Security не обрабатывает операции с DNS из списка. В правиле исключения вы можете указать: **Название правила**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **Операции с DNS**: • **IP-адрес DNS-сервера**. • **Параметры запроса**. • **Статус.** • **Имя домена.** • **ID типа настроек.** • **Ответная информация**. Содержание ответа DNS-сервера на запрос.

Настройка	ОС	Описание
Исключенные операции с LDAP	`Windows`	Kaspersky Endpoint Security не обрабатывает операции с LDAP из списка. В правиле исключения вы можете указать: **Название правила**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **Операции с LDAP**: • **Область поиска LDAP**. область поиска LDAP. Может иметь одно из следующих значений: ADS_SCOPE_BASE, ADS_SCOPE_ONELEVEL, ADS_SCOPE_SUBTREE. • **Фильтр**. • **Отличительное имя для поиска объектов в LDAP**. Имя записи в каталоге LDAP. • **Атрибуты объекта, используемые для поиска операций с LDAP**. Атрибуты, заданные в поисковом запросе в качестве возвращаемых.
Исключенные запросы доступа к процессу	`Windows`	Kaspersky Endpoint Security не обрабатывает запросы доступа к процессам из списка. В правиле исключения вы можете указать: **Название правила**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс**, **Родительский процесс**, **Файл целевого процесса**, **Дескриптор исходного процесса** и **Дескриптор целевого процесса**. • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **Запросы доступа к процессу**: • **Тип операции**. • **Запрошенный доступ к процессу**. • **Трассировка стека вызовов**.

Настройка	ОС	Описание
Исключенные внедрения в код	`Windows`	Kaspersky Endpoint Security не обрабатывает внедрения кода из списка. В правиле исключения вы можете указать: **Название правила**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **Внедрения в код**: • **Метод доступа**. • **Стек вызовов**. Стек вызовов API на момент перехвата функции, связанной с внедрением кода • **Измененная командная строка**. • **Адрес внедрения**. Адрес в адресном пространстве целевого процесса, куда был размещен удаленно запускаемый код. Поле не заполняется, если внедрение кода произошло с помощью методов SET_WINDOWS_HOOK и ARG_SPOOFING. • **Измененная командная строка**. • **Имя внедряемой библиотеки DLL**. Имя DLL, содержащей процедуру перехватчика и имя функции, которой передается управление после внедрения. Поле заполняется, если внедрение кода произошло с помощью метода SET_WINDOWS_HOOK. • **Путь внедряемой библиотеки DLL**. Путь к DLL, содержащей процедуру перехватчика. Поле заполняется, если внедрение кода произошло с помощью метода SET_WINDOWS_HOOK.

Настройка	ОС	Описание
Исключенные запросы WMI	`Windows`	Kaspersky Endpoint Security не обрабатывает запросы WMI из списка. В правиле исключения вы можете указать: **Название правила**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **Запросы WMI**: • **Тип операции WMI**. • **Удаленный запрос**. • **Имя компьютера, с которого выполнена команда WMI**. • **Учетная запись пользователя WMI**. • **Выполненная команда WMI**. • **Пространство имен WMI**. • **Фильтр потребителя событий WMI**. • **Имя созданного потребителя событий WMI**. • **Исходный код потребителя событий WMI**.

Настройка	ОС	Описание
Исключенные операции с каналами	`Windows`	Kaspersky Endpoint Security не обрабатывает операции с каналами из списка. В правиле исключения вы можете указать: **Название правила**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **Операции с каналами**: • **Имя канала**. • **Тип операции**.
Исключенные изменения реестра	`Windows`	Kaspersky Endpoint Security не обрабатывает изменения реестра из списка. В правиле исключения вы можете указать: **Название правила**. Kaspersky Endpoint Security применяет критерии срабатывания по правилу логического И. **Процесс** и **Родительский процесс**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **Изменения реестра**: • **Тип операции**. • **Путь**. Путь к разделу реестра, в котором произошло изменение. • **Имя значения**. Имя измененного параметра, например, RegistrySizeLimit. • **Значение**. • **Полное имя файла реестра**.

Настройка	ОС	Описание
Исключенные операции с устройствами	`Windows`	Kaspersky Endpoint Security не обрабатывает операции, связанные с USB-устройствами из списка. В правиле исключения вы можете указать: **Название правила**. **Тип устройства**. **Идентификатор устройства**. **Имя устройства**.

Телеметрия KUMA

для Windows

По умолчанию отправка событий на Сервер KUMA выключена. Для работы KUMA вам нужно включить отправку телеметрии. Для выбора источника событий доступны стандартные журналы: *Application*, *Security* или *System*. Также вы можете указать журнал стороннего приложения. Для повышения производительности и оптимизации отправки данных на Сервер KUMA вы можете вручную добавить отдельные журналы событий.

Настройки телеметрии KUMA

Настройка	ОС	Описание
Журналы событий Windows	`Windows`	Список журналов событий Windows, которые приложение отправляет в KUMA. Вы можете вручную добавить журналы по одному или импортировать JSON-файл с настройками. Для каждого журнала событий можете выбрать режим отправки: • **Отправлять все события**. В этом режиме приложение отправляет все события журнала Windows кроме событий, добавленных в правила исключения. • **Отправлять только выбранные события**. В этом режиме приложение отправляет только события, добавленные в правила включения. Также вы можете настроить правила исключения или включения для соответствующего режима отправки событий. Для добавления правил необходимо указать идентификатор события в журнале событий Windows. Вы можете перечислить несколько идентификаторов событий в одном правиле. Для указания нескольких идентификаторов событий используйте запятую в качестве разделителя.

Встроенные агенты

Managed Detection and Response

для Windows, macOS и Linux

Kaspersky Endpoint Security поддерживает работу с решением Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* – решение, которое автоматически обнаруживает и анализирует инциденты безопасности в вашей инфраструктуре. Для этого MDR использует данные телеметрии, полученные от конечных точек, и машинное обучение. Данные об инцидентах MDR передает экспертам "Лаборатории Касперского". Далее эксперты могут самостоятельно обработать инцидент и, например, добавить новую запись в антивирусные базы. Или эксперты могут дать рекомендации по обработке инцидента и, например, предложить изолировать компьютер от сети. Подробную информацию о работе решения см. в справке Kaspersky Managed Detection and Response.

Для работы Managed Detection and Response должны быть включены следующие компоненты:

- Kaspersky Security Network (расширенный режим)
- Анализ поведения

Эти компоненты должны быть включены обязательно. В противном случае Kaspersky Managed Detection and Response не работает, так как не получает необходимые данные телеметрии.

Настройки компонента Managed Detection and Response

Настройка	ОС	Описание
Конфигурационный файл MDR	`Windows` `macOS` `Linux`	BLOB-файл содержит идентификатор клиента и информацию о лицензии Kaspersky Managed Detection and Response. BLOB-файл находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробную информацию о BLOB-файле см. в справке Kaspersky Managed Detection and Response.

Endpoint Detection and Response Optimum

для Windows, macOS и Linux

В Kaspersky Endpoint Security включен встроенный агент для работы решения Kaspersky Endpoint Detection and Response Optimum (далее также "EDR Optimum"). *Kaspersky Endpoint Detection and Response* – решения, предназначенные для защиты IT-инфраструктуры организации от сложных кибернетических угроз. Функционал решений сочетает автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для противодействия сложным атакам, в том числе новым эксплойтам (exploits), программам-вымогателям (ransomware), бесфайловым атакам (fileless attacks), а также методам, использующим легитимные системные инструменты.

Kaspersky Endpoint Detection and Response анализирует потенциально опасные действия на устройствах пользователей и предоставляет *Специалистам по безопасности* или *Администратору* информацию о возможной атаке для принятия своевременных действий по реагированию или автоматически применяет заданные вами действия по реагированию.

Для работы Endpoint Detection and Response должны быть включены следующие компоненты:

- Защита от файловых угроз
- Защита от веб-угроз
- Защита от почтовых угроз
- Защита от эксплойтов
- Анализ поведения
- Предотвращение вторжений
- Откат вредоносных действий
- Адаптивный контроль аномалий

Список компонентов может отличаться для разных платформ.

Настройки компонента Endpoint Detection and Response

Настройка	ОС	Описание
Включить расширенное логирование активности в системе	`Windows` `macOS` `Linux`	Настройка обеспечивает корректность задачи **Ретроспективный поиск IOC**. Использует значительные ресурсы компьютера.

Настройка	ОС	Описание
Сетевая изоляция	`Windows` `macOS` `Linux`	Автоматическая изоляция компьютера от сети в результате реагирования на обнаруженные угрозы. После включения Сетевой изоляции приложение разрывает все активные соединения и блокирует все новые соединения TCP/IP на компьютере. Приложение оставляет активными только следующие соединения: • соединения, указанные в исключениях из Сетевой изоляции; • соединения, инициированные службами Kaspersky Endpoint Security; • соединения, инициированные Агентом администрирования Kaspersky Security Center.
Разблокировать автоматически изолированное устройство через (часы)	`Windows` `macOS` `Linux`	Сетевая изоляция может быть выключена автоматически по истечении заданного периода времени или вручную.
Исключения из сетевой изоляции	`Windows` `macOS` `Linux`	Список правил исключений из Сетевой изоляции. Сетевые соединения, подпадающие под заданные правила, не будут заблокированы на компьютерах после включения Сетевой изоляции. Для настройки исключений из Сетевой изоляции в приложении доступен список *стандартных сетевых профилей*. По умолчанию в исключения входят сетевые профили, состоящие из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент. Также вы можете изменить параметры стандартных сетевых профилей или задать исключения вручную. Исключения, заданные в свойствах политики, применяются, только если Сетевая изоляция включена приложением автоматически, в результате реагирования на обнаружение угрозы. Исключения, заданные в свойствах компьютера, применяются, только если Сетевая изоляция включена вручную в свойствах компьютера в консоли Kaspersky Security Center или в деталях алерта.
Запрет запуска объектов	`Windows` `macOS` `Linux`	Контроль запуска исполняемых файлов и скриптов, а также открытия файлов офисного формата. Например, вы можете запретить запуск приложений, использование которых считается небезопасным, на выбранном компьютере. Запрет запуска объектов поддерживает определенный набор расширений файлов офисного формата и определенный набор интерпретаторов скриптов. Для работы Запрета запуска объектов вам нужно добавить правила запрета запуска объектов.
Действие при запуске или открытии объекта	`Windows` `macOS` `Linux`	**Заблокировать и записать в журнал событий**. В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета. Также приложение публикует в журнал событий и Kaspersky Security Center событие о попытках запуска объектов или открытия документов. **Записать в журнал событий**. В этом режиме Kaspersky Endpoint Security публикует в журнал событий и Kaspersky Security Center событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.
Правила запрета запуска	`Windows` `macOS` `Linux`	*Правило запрета запуска* – это набор критериев, которые приложение учитывает при реагировании на запуск объекта, например, при блокировании запуска объекта. Приложение идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.
Учитывать регистр при вводе пути	`Linux`	Если флажок установлен, приложение будет учитывать регистр при создании правил запрета запуска.
Cloud Sandbox	`Windows` `macOS` `Linux`	*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 получения информации об анализируемых объектах требуется подключение к KSN.

Endpoint Detection and Response Expert (on-premise)

для Windows, macOS и Linux

Endpoint Detection and Response Expert (версия 7.1 и ниже)

Kaspersky Endpoint Security поддерживает работу с компонентом Kaspersky Endpoint Detection and Response Expert (версия 7.1 и ниже, далее также – "EDR (KATA)") в составе решения Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* – решение, предназначенное для своевременного обнаружения сложных угроз, таких как целевые атаки, сложные постоянные угрозы (англ. Advanced Persistent Threat, APT), атаки "нулевого дня" и другие. Kaspersky Anti Targeted Attack Platform включает в себя три функциональных блока:

- Kaspersky Anti Targeted Attack (далее также "*KATA*");
- Kaspersky Endpoint Detection and Response (далее также "*EDR (KATA)*");
- Network Detection and Response (далее также "*NDR (KATA)*").

Вы можете приобрести все функциональные блоки или приобрести функциональные блоки по отдельности. Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform.

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

Настройка интеграции с EDR (KATA) и NDR (KATA) выполняется в консоли Kaspersky Security Center. Дальнейшее управление встроенным агентом осуществляется в консоли Kaspersky Anti Targeted Attack Platform, включая запуск задач, управление объектами на карантине, просмотр отчетов и другие действия.

Endpoint Detection and Response Expert (версия 8.0 и выше)

Kaspersky Endpoint Security поддерживает работу с решениями класса Endpoint Detection and Response Expert (версия 8.0 и выше, далее также "EDR Expert (on-premise)") от "Лаборатории Касперского". К таким решениям относится, например, Kaspersky Symphony XDR. *Endpoint Detection and Response Expert (on-premise)* – решения для обеспечения кибербезопасности, с помощью которых организация получает возможность защититься от большинства киберрисков и покрыть основные сценарии распространения угроз.

На основании журналов и телеметрии, полученных от инфраструктуры организации, EDR Expert (on-premise) автоматически выявляет атаки и позволяет проводить расследование инцидентов с помощью единого графа расследования, который комбинирует все собираемые в EDR Expert (on-premise) события – как от приложений "Лаборатории Касперского", так и от сторонних ИБ-продуктов.

Компоненты, необходимые для работы Endpoint Detection and Response Expert

Для работы Endpoint Detection and Response Expert должны быть включены следующие компоненты:

- Защита от файловых угроз
- Защита от веб-угроз
- Защита от почтовых угроз
- Защита от эксплойтов
- Анализ поведения
- Предотвращение вторжений
- AMSI-защита
- Фоновая проверка
- Kaspersky Security Network

Список компонентов может отличаться для разных платформ.

Настройки компонента Endpoint Detection and Response Expert (on-premise)

Настройка	ОС	Описание
Решение Endpoint Detection and Response Expert	`Windows` `macOS` `Linux`	Решения Endpoint Detection and Response Expert, с которым интегрируется Kaspersky Endpoint Security. • **Endpoint Detection and Response Expert (версия 7.1 и ниже)**. • **Endpoint Detection and Response Expert (версия 8.0 и выше)**.
Настройки подключения	`Windows` `macOS` `Linux`	Настройте следующие параметры для подключения к серверу KATA или к серверу сбора телеметрии: • **Время ожидания соединения с сервером**. 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.

Настройка	ОС	Описание
Отправлять запрос на синхронизацию на сервер каждые (мин.) *(доступен только для Endpoint Detection and Response Expert (версия 7.1 и ниже))*	`Windows` `macOS` `Linux`	Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Endpoint Security передает данные об изменениях в параметрах приложения и задачах.
Подключение к серверам KATA / **Подключение к серверам сбора телеметрии**	`Windows` `macOS` `Linux`	Введите IP-адрес и порт подключения к серверу Kaspersky Anti Targeted Attack Platform или серверу сбора телеметрии. Вы можете добавить несколько адресов сервера Central Node (для KATA) или сервера сбора телеметрии. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку. Архитектура решений EDR (KATA) и EDR Expert (on-premise) отличается. Для обработки телеметрии EDR Expert (on-premise) использует сервер сбора телеметрии, EDR (KATA) использует сервер Central Node. Поэтому при интеграции приложения с EDR Expert (on-premise) вам нужно добавить сервер сбора телеметрии.
Отправлять телеметрию в KATA / **Отправлять телеметрию на серверы сбора телеметрии**	`Windows` `macOS` `Linux`	Функция позволяет полностью выключить отправку телеметрии на сервер KATA или сервер сбора телеметрии в зависимости от выбранного решения. Например, если вы используете Kaspersky Anti Targeted Attack Platform совместно с другим решением, которое также использует телеметрию, вы можете выключить отправку телеметрии для KATA (EDR). Это позволит оптимизировать нагрузку на серверы для этих решений. Если у вас развернуто решение Managed Detection and Response и KATA (EDR), вы можете использовать телеметрию MDR, а создавать задачи реагирования на угрозы в KATA (EDR).
Отправлять телеметрию только с IOA *(доступен только для Endpoint Detection and Response Expert (версия 8.0 и выше))*	`Windows` `Linux`	Функция позволяет оптимизировать отправку телеметрии на сервер и отправлять только телеметрию с IOA. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию *потоковой проверки*, которая позволяет отслеживать такие события в режиме реального времени.
Максимальная задержка отправки событий (сек.)	`Windows` `macOS` `Linux`	Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации.
Максимальное количество пакетов событий	`Windows`	Приложение выполняет синхронизацию с сервером при заполнении буфера событиями.
Включить регулирование количества запросов	`Windows` `macOS` `Linux`	Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события. **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. 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.
Подключение к серверам реагирования *(доступен только для Endpoint Detection and Response Expert (версия 8.0 и выше))*	`Windows` `macOS` `Linux`	Настройки подключения к серверам реагирования. Введите IP-адрес сервера реагирования (IPv4 или IPv6) и порт подключения к серверу. Вы можете добавить несколько адресов сервера реагирования. 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.

Настройка	ОС	Описание

Настройки подключения
(доступен только для Endpoint Detection and Response Expert (версия 8.0 и выше))
	`Windows`
	`macOS`
	`Linux`
		Настройте следующие параметры для подключения к серверу реагирования:
		• **Время ожидания соединения с сервером**. Максимальное время ожидания ответа от сервера реагирования. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу реагирования.
		• **Сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером реагирования.
		• **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером реагирования. Для использования двусторонней аутентификации вам нужно в параметрах сервера реагирования включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров сервера реагирования 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.

Network Detection and Response (KATA)

для Windows и Linux

Kaspersky Endpoint Security поддерживает работу с компонентом Kaspersky Network Detection and Response в составе решения Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* – решение, предназначенное для своевременного обнаружения сложных угроз, таких как целевые атаки, сложные постоянные угрозы (англ. Advanced Persistent Threat, APT), атаки "нулевого дня" и другие. Kaspersky Anti Targeted Attack Platform включает в себя три функциональных блока:

- Kaspersky Anti Targeted Attack (далее также "*KATA*");
- Kaspersky Endpoint Detection and Response (далее также "*EDR (KATA)*");
- Network Detection and Response (далее также "*NDR (KATA)*").

Вы можете приобрести все функциональные блоки или приобрести функциональные блоки по отдельности. Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform.

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Anti Targeted Attack Platform. Приложение Kaspersky Endpoint Security также передает на сервер Kaspersky Anti Targeted Attack Platform данные об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз.

Настройка интеграции с EDR (KATA) и NDR (KATA) выполняется в консоли Kaspersky Security Center. Дальнейшее управление встроенным агентом осуществляется в консоли Kaspersky Anti Targeted Attack Platform, включая запуск задач, управление объектами на карантине, просмотр отчетов и другие действия.

Для работы Network Detection and Response (KATA) должны быть включены следующие компоненты:

- Защита от файловых угроз
- Защита от веб-угроз

- Защита от почтовых угроз
- Защита от эксплойтов
- Анализ поведения
- Предотвращение вторжений
- AMSI-защита
- Фоновая проверка
- Kaspersky Security Network

Список компонентов может отличаться для разных платформ.

Настройки компонента Network Detection and Response (KATA)

Настройка	ОС	Описание
Настройки подключения к серверам KATA	`Windows` `Linux`	**Время ожидания соединения с сервером**. 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.
Подключение к серверам KATA	`Windows` `Linux`	Параметры подключения к серверам Kaspersky Anti Targeted Attack Platform. Введите IP-адрес сервера Central Node (IPv4 или IPv6) и порт подключения к серверу. Вы можете добавить несколько адресов сервера Central Node. Kaspersky Endpoint Security пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Endpoint Security пытается установить соединение через второй IP-адрес и так далее по списку.
Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)	`Windows` `Linux`	Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Endpoint Security передает данные об изменениях в параметрах приложения и задачах.
Максимальная задержка отправки событий (сек.)	`Windows` `Linux`	Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации.

Настройка	ОС	Описание
Включить регулирование количества запросов	`Windows` `Linux`	Функция позволяет оптимизировать нагрузку на сервер. Если функция включена, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Endpoint Security прекращает отправлять события. **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Endpoint Security восстанавливает передачу событий по истечению часа. 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.

Sandbox

для Windows и Linux

Kaspersky Endpoint Security поддерживает интеграцию с решением Kaspersky Sandbox и с компонентом Sandbox, который входит в состав решения Kaspersky Anti Targeted Attack Platform. *Sandbox* обнаруживает и автоматически блокирует сложные угрозы на компьютерах. Sandbox анализирует поведение объектов для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации. Sandbox выполняет анализ и проверку объектов на специальных серверах с развернутыми виртуальными образами операционных систем Microsoft Windows (серверы Sandbox). Подробнее о решении см. в справке Kaspersky Sandbox и справке Kaspersky Anti Targeted Attack Platform.

Компонент KATA Sandbox позволяет проверять файлы не только в автоматическом режиме, но и вручную из контекстного меню файла.

Для работы KATA Sandbox должно быть развернуто решение Kaspersky Anti Targeted Attack Platform версии 7.0 или выше.

Настройки компонента Sandbox

Настройка	ОС	Описание
Режим интеграции	`Windows` `Linux`	**Kaspersky Sandbox**. Интеграция с решением Kaspersky Sandbox. Приложение отправляет файлы на проверку в Kaspersky Sandbox только в автоматическом режиме. **KATA Sandbox**. Интеграция с компонентом Sandbox, который входит в состав решения Kaspersky Anti Targeted Attack Platform. Вы можете выбрать режим отправки файлов на проверку: • **Вручную**. Пользователь вручную отправляет файл на проверку из контекстного меню (**Отправить в Sandbox**). • **Автоматически**. Приложение автоматически обнаруживает объекты и отправляет их на проверку в Sandbox. • **Комбинированный**. Приложение автоматически отправляет объекты на проверку в Sandbox. При необходимости, пользователь также может отправить отдельные файлы на проверку из контекстного меню.
Подключение к серверам Sandbox	`Windows` `Linux`	**Kaspersky Sandbox**. Параметры подключения к серверам Sandbox. На серверах развернуты виртуальные образы операционных систем Microsoft Windows, в которых запускаются проверяемые объекты. Введите IP-адрес сервера Sandbox (IPv4, IPv6, DNS) и порт подключения к серверу. **KATA Sandbox**. Параметры подключения к серверу Central Node. Central Node выбирает оптимальные параметры для проверки и обеспечивает распределение нагрузки между серверами Sandbox. Введите IP-адрес сервера Central Node (IPv4, IPv6, DNS) и порт подключения к серверу.

Настройка	ОС	Описание
Настройки подключения к серверам	`Windows` `Linux`	**Время ожидания соединения с сервером**. Время ожидания соединения с сервером Sandbox (для Kaspersky Sandbox) или Central Node (для KATA). По истечению заданного времени ожидания Kaspersky Endpoint Security отправит запрос на следующий сервер. Вы можете увеличить время ожидания соединения с сервером, если у вас низкая скорость соединения или соединение нестабильно. Рекомендованное значение времени ожидания запроса не более 0,5 сек. **Очередь запросов**. Размер папки хранения очереди запросов. При отправке нескольких объектов на проверку в Sandbox приложение Kaspersky Endpoint Security создает очередь запросов. По умолчанию размер папки хранения очереди запросов ограничен 100 МБ. После достижения максимального размера Sandbox перестает добавлять новые запросы в очередь и отправляет соответствующее событие в Kaspersky Security Center. Вы можете настроить размер папки хранения очереди запросов в зависимости от конфигурации сервера. **TLS-сертификат сервера**. Для настройки доверенного соединения с сервером Sandbox (для Kaspersky Sandbox) или Central Node (для KATA) вам нужно подготовить TLS-сертификат. Далее вам нужно добавить сертификат на компьютер с помощью политики. Также вам нужно добавить сертификат на сервер Sandbox (для Kaspersky Sandbox) или Central Node (для KATA). **Использовать двустороннюю аутентификацию** (только для KATA Sandbox). Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и сервером Central Node. Для использования двусторонней аутентификации вам нужно в параметрах сервера Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.
Действие при обнаружении угрозы	`Windows` `Linux`	**Копию поместить на карантин, объект удалить**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удаляет вредоносный объект, обнаруженный на компьютере. Перед удалением объекта Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин. **Запустить проверку важных областей**. Если выбран этот вариант действия, то Kaspersky Endpoint Security запускает задачу *Проверка важных областей*. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы. **Создать задачу поиска IOC**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически создает задачу *Поиск IOC (автономная задача поиска IOC)*. Вы можете настроить режим запуска задачи, область поиска и действие при обнаружении IOC (*Копию поместить на карантин, объект удалить* или *Запустить проверку важных областей*). Для настройки других параметров задачи *Поиск IOC* перейдите в свойства задачи.
Область поиска IOC	`Windows` `Linux`	**Важные файловые области**. Если выбран этот вариант, Kaspersky Endpoint Security выполняет поиск IOC только в важных файловых областях компьютера: например, выборочных каталогах профиля пользователей и критических объектах системы. **Файловые области на системном диске компьютера**. Если выбран этот вариант, Kaspersky Endpoint Security выполняет поиск IOC на системном диске компьютера. Также приложение выполняет поиск IOC по файловому пути, в котором была обнаружена угроза, вне зависимости от выбранной области поиска.
Запуск задачи поиска IOC	`Windows` `Linux`	**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 в случае обнаружения угрозы. `Windows` **Выполнять только во время простоя компьютера**. Режим запуска, при котором Kaspersky Endpoint Security запускает задачу *Поиск IOC*, если включена экранная заставка или компьютер заблокирован. Если пользователь разблокировал компьютер, Kaspersky Endpoint Security приостанавливает выполнение задачи. Таким образом, приложение может выполнять задачу несколько дней.

Интеграция с KUMA

для Windows и Linux

Kaspersky Endpoint Security поддерживает работу с решением Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* – решение класса SIEM для управления информацией о безопасности и событиями безопасности в ИТ-инфраструктуре организации. KUMA позволяет обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб организации.

Приложение Kaspersky Endpoint Security устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере (телеметрия) отправляются на сервер Kaspersky Unified Monitoring and Analysis Platform (KUMA).

По умолчанию отправка событий на Сервер KUMA выключена. Для работы KUMA сначала включите отправку телеметрии в разделе "Общие настройки → Настройки телеметрии".

Kaspersky Endpoint Security не выполняет все функции агента для KUMA. Приложение только отправляет в KUMA события без разметки. Для доступа ко всем функциям KUMA вам нужно приобрести лицензию на решение и развернуть решение в соответствии с Руководством администратора KUMA.

Настройки компонента KUMA

Настройка	ОС	Описание
Настройки подключения к серверам	`Windows` `Linux`	**Время ожидания соединения с сервером**. Максимальное время ожидания ответа от сервера KUMA. По истечению времени ожидания Kaspersky Endpoint Security пытается подключиться к другому серверу KUMA. **Сертификат сервера**. TLS-сертификат предназначен для установки доверенного соединения с сервером KUMA. Вы можете получить TLS-сертификат в консоли Kaspersky Unified Monitoring and Analysis Platform (см. инструкцию в справке Kaspersky Unified Monitoring and Analysis Platform). **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Endpoint Security и KUMA. Для использования двусторонней аутентификации вам нужно в консоли KUMA в параметрах коннектора типа tcp выбрать режим TLS **Нестандартный PFX** (см. параметры коннектора типа tcp в справке Kaspersky Unified Monitoring and Analysis Platform). Далее вам нужно получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. После настройки параметров KUMA 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.
Максимальная задержка отправки событий (сек.)	`Windows` `Linux`	Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации.
Использовать шифрование TLS	`Windows` `Linux`	Если функция включена, Kaspersky Endpoint Security использует TLS-сертификат для установки доверенного соединения с сервером KUMA.
Подключение к серверам KUMA	`Windows` `Linux`	Параметры подключения к серверам KUMA. Укажите IP-адрес (IPv4 или IPv6), протокол подключения к серверам и порт подключения к серверу. Вы можете добавить несколько адресов сервера KUMA. 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.

Режим Легкого агента

Настройки обнаружения SVM

для Windows и Linux

При запуске Легкий агент устанавливает и поддерживает соединение с виртуальной машиной защиты 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 фрагменты файлов, которые необходимо проверять. Результаты проверки доступны для всех виртуальных машин с установленным Легким агентом (технология SharedCache). Таким образом, технология SharedCache 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. Для взаимодействия компонентов решения и виртуальной инфраструктуры предназначен компонент Сервер 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.

Настройки обнаружения SVM

Настройка	ОС	Описание
Использовать Сервер интеграции	`Windows` `Linux`	Сервер интеграции удобно использовать в больших виртуальных инфраструктурах, так как Сервер интеграции автоматически распределяет нагрузку между SVM. Введите параметры подключения к Серверу интеграции: • IP-адрес в формате IPv4 или полное доменное имя (FQDN) устройства, на котором установлен Сервер интеграции. • Номер порта для подключения к Серверу интеграции. По умолчанию указан порт 7271. • Пароль администратора Сервера интеграции (пароль учетной записи admin).
Использовать список адресов SVM, заданный вручную	`Windows` `Linux`	Сформируйте список SVM для подключения Легкого агента. Введите 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. 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.

Настройки подключения к Серверу интеграции

для Windows и Linux

Сервер интеграции – компонент решения, который обеспечивает взаимодействие между Kaspersky Security для виртуальных сред Легкий агент и виртуальной инфраструктурой. Сервер интеграции 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 Сервер интеграции автоматически распределяет нагрузку между SVM. Сервер интеграции получает информацию о доступных SVM, анализирует эту информацию и предоставляет Легким агентам список Серверов защиты (SVM), оптимальных для подключения.

Настройки подключения к серверу интеграции

Настройка	ОС	Описание
Адрес	`Windows` `Linux`	IP-адрес в формате IPv4 или полное доменное имя (FQDN) Сервера интеграции. Если в качестве адреса указано NetBIOS-имя, localhost или 127.0.0.1, подключение к Серверу интеграции завершается с ошибкой.
Порт	`Windows` `Linux`	Номер порта для подключения к Серверу интеграции. По умолчанию указан порт 7271.
Аутентификация на Сервере интеграции	`Windows` `Linux`	Пароль администратора Сервера интеграции (пароль учетной записи `admin`). 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.

Тег для подключения к SVM

для Windows и Linux

К SVM могут подключаться несколько Легких агентов. Для распределения подключения Легких агентов вы можете указать отдельный список SVM в разделе "Настройки обнаружения 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 Kaspersky Security для защиты 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.

Установите флажок **Использовать тег для подключения**, чтобы подключать Легкие агенты к SVM с помощью тегов. 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 `;`.

Алгоритм выбора SVM

для Windows и Linux

В инфраструктуре организации может быть развернуто несколько SVM, к которым могут подключаться Легкие агенты. Для оптимизации нагрузки на сеть и ресурсы виртуальной инфраструктуры вам нужно распределить Легкие агенты между SVM.

Настройки Алгоритма выбора SVM

Настройка	ОС	Описание
Использовать стандартный алгоритм выбора SVM	`Windows` `Linux`	Если применяется этот алгоритм, после установки и запуска на виртуальной машине Легкий агент выбирает для подключения SVM, которая является *локальной* для Легкого агента. В основном Легкий агент определяет локальные SVM по расположению SVM в виртуальной инфраструктуре. Если SVM расположены в том же гипервизоре, что и Легкий агент, Легкий агент считает SVM локальными. Для некоторых виртуальных инфраструктур вам нужно определять локальные SVM вручную с помощью файла конфигурации. 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.
Использовать расширенный алгоритм выбора SVM	`Windows` `Linux`	Расширенный алгоритм позволяет вам вручную задать критерии выбора локальных SVM или выключить поиск локальных SVM. Для этого вам нужно выбрать расположение SVM в виртуальной инфраструктуре: Гипервизор, Кластер или Дата-центр. То есть, вам нужно выбрать область обнаружения локальных SVM. Если подключиться к локальным SVM в заданной области обнаружения не удалось, Легкий агент прекращает попытки подключения. Также расширенный алгоритм позволяет выключить поиск локальных SVM для Легкого агента. В этом случае Легкий агент выбирает SVM с наименьшим количеством подключенных Легких агентов во всей виртуальной инфраструктуре.

Защита соединения

для Windows и Linux

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 Kaspersky Security для виртуальных сред Легкий агент.

Защита соединения с помощью шифрования может снижать производительность работы решения Kaspersky Security для защиты виртуальных сред Легкий агент.

Приложение 6. 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.

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.

Компонент приложения	Рекомендуемое состояние компонента	Рекомендации
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	–
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	–

Компонент приложения	Рекомендуемое состояние компонента	Рекомендации
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.

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.

Рекомендуемые настройки

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	–

Компонент приложения	Рекомендуемое состояние компонента	Рекомендации
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	–

Источники информации о Kaspersky Endpoint Security

Страница Kaspersky Endpoint Security в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Endpoint Security в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Endpoint Security, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение приложений "Лаборатории Касперского" на Форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме.

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Глоссарий

SIEM-система

Система Security Information and Event Management. Решение для управления информацией и событиями в системе безопасности организации.

SVM

Secure virtual machine – специальная виртуальная машина, на которой установлена служба scanserver (Сервер защиты, компонент Kaspersky Endpoint Security для виртуальных сред Легкий агент).

Активация приложения

Перевод приложения в полнофункциональный режим. Активация выполняется пользователем во время или после установки приложения. Для активации приложения пользователю необходим код активации или файл ключа.

Активная политика

Политика, которую приложение использует в данный момент для контроля утечек данных. Приложение может использовать несколько политик одновременно.

Активный ключ

Ключ, используемый в текущий момент для работы приложения.

База вредоносных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как опасное. Список сформирован специалистами "Лаборатории Касперского", регулярно обновляется и входит в поставку приложения "Лаборатории Касперского".

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами "Лаборатории Касперского" как фишинговые. База регулярно обновляется и входит в поставку приложения "Лаборатории Касперского".

Базы приложения

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска баз. Базы приложения формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

Группа администрирования

Набор устройств, объединенных в Kaspersky Security Center в соответствии с выполняемыми функциями и устанавливаемым на них набором приложений "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы администрирования могут входить другие группы. Для каждого из установленных в группе администрирования приложений могут быть созданы групповые политики и сформированы групповые задачи.

Групповая задача

Задача, назначенная для группы администрирования и выполняемая на всех управляемых устройствах, входящих в состав группы.

Групповая политика

см. Политика.

Доверенное устройство

Устройство, полный доступ к которому разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Зараженный объект

Объект, участок кода которого полностью совпадает с участком кода известной программы, представляющей угрозу. Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими объектами.

Защита от шифрования

Вредоносная активность программ-шифровальщиков, направленная на шифрование файлов с данными пользователя. Зашифрованные файлы недоступны для чтения и использования.

Исключение

Исключение – объект, исключаемый из проверки приложением "Лаборатории Касперского". Исключать из проверки можно файлы определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по названию согласно классификации Вирусной энциклопедии. Для каждой задачи могут быть заданы свои исключения.

Легкий агент

Компонент Kaspersky Endpoint Security для виртуальных сред Легкий агент. Устанавливается на каждую виртуальную машину, которую требуется защищать.

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации "Лаборатория Касперского". Документ содержит информацию о предоставляемой лицензии.

Лицензия

Ограниченное по времени право на использование приложения, предоставляемое вам на основании Лицензионного соглашения.

Ложное срабатывание

Ситуация, когда незараженный объект определяется приложением "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

Маска файла

Представление имени файла общими символами. Основными символами, используемыми в масках файлов, являются * и ? (где * – любое число любых символов, а ? – любой один символ).

Объекты автозапуска

Набор приложений, необходимых для запуска и корректной работы установленных на вашем компьютере операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

Параметры приложения

Параметры работы приложения, общие для всех типов его задач и отвечающие за работу приложения в целом, например: параметры производительности приложения, параметры ведения отчетов, параметры резервного хранилища.

Подписка

Использование приложения с выбранными настройками (дата окончания, количество устройств). Вы можете приостанавливать или возобновлять подписку, продлевать ее в автоматическом режиме, а также отказываться от нее.

Политика

Политика определяет параметры работы приложения и доступ к настройке приложения, установленного на устройствах группы администрирования. Для каждого приложения требуется создать свою политику. Вы можете создать неограниченное количество различных политик для приложений, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждому приложению.

Прокси-сервер

Служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-сервером в определенных целях.

Резервный ключ

Ключ, подтверждающий право на использование приложения, но не используемый в текущий момент.

Сервер администрирования

Компонент приложения Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

Сервер интеграции

Компонент Kaspersky Endpoint Security для виртуальных сред Легкий агент. Осуществляет взаимодействие между компонентами Kaspersky Endpoint Security и виртуальной инфраструктурой.

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы и FTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.

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.

AMD64 – товарный знак или зарегистрированный товарный знак Advanced Micro Devices, Inc.

Amazon является товарным знаком Amazon.com, Inc. или аффилированных лиц компании.

Mac, FireWire – товарные знаки Apple Inc.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

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, Google Public DNS – товарные знаки Google LLC.

HUAWEI, EulerOS, FusionSphere являются товарными знаками Huawei Technologies Co., Ltd.

Intel, Core являются товарными знаками Intel Corporation или ее дочерних компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Hyper-V, Outlook, Visual C++ и Windows являются товарными знаками группы компаний Microsoft.

OpenStack – зарегистрированный товарный знак OpenStack Foundation в США и других странах.

Oracle, JavaScript – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Red Hat, 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.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

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.