kaspersky

Kaspersky Embedded Systems Security для Linux

© 2026 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Embedded Systems Security 4.0 для Linux

О Kaspersky Embedded Systems Security 4.0 для Linux

- Комплект поставки
- Аппаратные и программные требования
  - Аппаратные требования
  - Программные требования
  - Особенности работы приложения на разных ОС
  - Поддерживаемые версии Kaspersky Security Center

Что нового

Подготовка к установке приложения Kaspersky Embedded Systems Security

Установка и первоначальная настройка приложения Kaspersky Embedded Systems Security

- Установка и первоначальная настройка Агента администрирования Kaspersky Security Center
- Установка плагинов управления Kaspersky Embedded Systems Security
  - Установка веб-плагина Kaspersky Embedded Systems Security
  - Установка MMC-плагина Kaspersky Embedded Systems 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 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
    - Определение типа перехватчика файловых операций
    - 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
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 Embedded Systems 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 Embedded Systems Security
Лицензирование приложения
О Лицензионном соглашении
О лицензии
О Лицензионном сертификате
О лицензионном ключе
О коде активации
О файле ключа
О подписке
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 приложению Kaspersky Security Center
Данные, предоставляемые при переходе по ссылкам из интерфейса приложения
Данные, предоставляемые при использовании Kaspersky Security Network
Концепция управления приложением
Управление приложением через Kaspersky Security Center
О плагинах управления Kaspersky Embedded Systems Security
О политиках Kaspersky Security Center

- О задачах для Kaspersky Embedded Systems 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 kess-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
Управление сетевым экраном
О динамических правилах
О сетевых пакетных 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 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
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
Окно Доверенные сертификаты Контроля приложений
Настройка контроля приложений в командной строке
Параметры задачи Контроль приложений
Создание и изменение списка категорий
Просмотр списка категорий
Настройка списка правил контроля приложений
Управление списком доверенных сертификатов 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
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
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

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
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
Обнаружение 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
Включение и выключение проверки пространств имен
Отмена запуска задач при работе от аккумулятора
Настройка дополнительных параметров телеметрии
Доверенная зона
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 Kaspersky Managed Detection and Response
О действиях по реагированию
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 устройства

- Работа с карантином
  - 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
- 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 пользовательский интерфейс
  - Включение и выключение компонентов приложения
  - Запуск и остановка задач проверки
  - Запуск выборочной проверки
  - 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 приложением
    - Команды управления параметрами и задачами приложения
      - Команды управления общими параметрами приложения
      - Команды управления параметрами задач
      - Команды управления задачами
      - 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 резервным хранилищем
Команды управления карантином
Команды управления сетевой изоляцией устройства
Команды управления пользователями и ролями
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 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 Защита от атак BadUSB (ID: 37)
Общие параметры приложения
Параметры проверки сетевого трафика
Параметры расписания задач
Приложение 3. Коды возврата командной строки
Приложение 4. Параметры для взаимодействия с внешними службами
Источники информации о Kaspersky Embedded Systems Security
Глоссарий
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
- Исключение
- Лечение объектов
- Лицензионный сертификат
- Лицензия
- Ложное срабатывание
- Маска файла
- Объекты автозапуска
- Параметры приложения
- Подписка
- Политика
- Прокси-сервер
- Резервный ключ
- Сервер администрирования
- Серверы обновлений "Лаборатории Касперского"

Информация о стороннем коде

Уведомления о товарных знаках

Справка Kaspersky Embedded Systems Security 4.0 для Linux

	**Что нового** Узнайте, что нового в этой версии приложения.		**Обновление баз и модулей приложений** Проверьте надежность системы защиты.
	**Аппаратные и программные требования** Проверьте аппаратные требования и поддерживаемые операционные системы.		**Оптимизация потребления ресурсов** Узнайте, как оптимизировать потребление ресурсов операционной системы.
	**Установка и первоначальная настройка** Узнайте, как подготовить устройство к установке приложения, как установить приложение и выполнить первоначальную настройку приложения.		**Мониторинг и отчеты** Проверьте состояние защиты устройства и узнайте о том, как просмотреть события и отчеты о работе приложения.
	**Обновление предыдущей версии приложения** Узнайте, как обновить приложение до версии Kaspersky Embedded Systems Security 4.0 для Linux.		**Предоставление данных** Узнайте о предоставлении данных и защите персональных данных и конфиденциальной информации.
	**Лицензирование и активация** Ознакомьтесь с терминологией лицензирования и узнайте об активации приложения.		**Обращение в Службу технической поддержки** Узнайте о способах получения данных при обращении в Службу технической поддержки.

О Kaspersky Embedded Systems Security 4.0 для Linux

Приложение Kaspersky Embedded Systems Security 4.0 для Linux (далее также Kaspersky Embedded Systems 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.

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 Embedded Systems 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 Embedded Systems Security может проверять следующие съемные диски: CD/DVD-приводы, Blu-ray диски, флеш-накопители (включая USB-модемы), внешние жесткие диски и дискеты.

- **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 Embedded Systems 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 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.

- **Анализ поведения**. Компонент *Анализ поведения* позволяет контролировать вредоносную активность приложений в операционной системе. При обнаружении вредоносной активности Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security на различные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Перед лечением или удалением Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security поддерживает возможность интеграции с решением Kaspersky Managed Detection and Response для расширения возможностей использования приложения. Интеграция с Kaspersky Managed Detection and Response обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.

Для поддержки приложения в актуальном состоянии предусмотрены дополнительные функции приложения:

- Активация приложения с помощью файла ключа или кода активации.
- Обновление баз и модулей приложения с серверов обновлений "Лаборатории Касперского", через Сервер администрирования или из указанного пользователем источника по расписанию и по требованию.
- 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 Embedded Systems 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.

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

Комплект поставки

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

В комплект поставки приложения Kaspersky Embedded Systems Security входят следующие файлы:

- kess-4.0.0-<номер сборки>.i386.rpm, kess_4.0.0-<номер сборки>_i386.deb

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

- kess-4.0.0-<номер сборки>.x86_64.rpm, kess_4.0.0-<номер сборки>_amd64.deb

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

- kess-4.0.0-<номер сборки>.aarch64.rpm, kess_4.0.0-<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.

- kess-gui-4.0.0-<номер сборки>.i386.rpm, kess-gui_4.0.0-<номер сборки>_i386.deb

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

- kess-gui-4.0.0-<номер сборки>.x86_64.rpm, kess-gui_4.0.0-<номер сборки>_amd64.deb

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

- kess-gui-4.0.0-<номер сборки>.aarch64.rpm, kess-gui_4.0.0-<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.

- kess-4.0.0.<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 Embedded Systems Security.

Аппаратные требования

Приложение Kaspersky Embedded Systems Security имеет следующие минимальные 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).

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).

Программные требования

Для установки Kaspersky Embedded Systems 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 9.4, 9.5, 9.6.
  - 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.10015-17 (очередное обновление 1.7.3).
  - Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7).

    Работа приложения на операционных системах Astra Linux в режиме мандатного разграничения доступа поддерживается, если включено использование системного механизма пространств имен.
  - 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.
  - EulerOS 2.0 SP10.
  - Oracle® Linux 9.4, 9.5, 9.6.
  - Red Hat® Enterprise Linux® 9.4, 9.5, 9.6.
  - Red Hat Enterprise Linux 10.0, 10.1.
  - Rocky Linux™ 9.4, 9.5, 9.6.
  - SUSE® Linux Enterprise Server 15.4, 15.5, 15.6, 15.7.
  - Ubuntu® 22.04 LTS.
  - Ubuntu 24.04 LTS.

- Альт Рабочая станция 11.
- Альт Сервер 11
- Альт СП Рабочая Станция релиз 10.
- Альт СП Сервер релиз 10.
- 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.

- 64-битные операционные системы для архитектуры Arm:
  - Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
  - CentOS Stream 9.
  - Debian GNU/Linux 12.13.
  - 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.

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.

Особенности работы приложения на разных ОС

Работа приложения на операционных системах Astra Linux в режиме мандатного разграничения доступа поддерживается, если включено использование системного механизма пространств имен.

Для работы приложения Kaspersky Embedded Systems Security требуется дополнительная настройка операционной системы в следующих случаях:

- Astra Linux Special Edition в режиме замкнутой программной среды.
- Альт СП в режиме замкнутой программной среды.
- При использовании системы контроля доступа SELinux на операционных системах, построенных на основе Red Hat Enterprise Linux.

Не поддерживается работа приложения Kaspersky Embedded Systems Security в следующих случаях:

- На операционных системах, построенных на основе Red Hat Enterprise Linux, в подсистеме IMA.
- На операционных системах, построенных на основе Red Hat Enterprise Linux, в режиме FIPS.
- На операционных системах Ubuntu и операционных системах, основанных на кодовой базе SUSE Linux Enterprise Server, в системе мандатного управления доступом AppArmor.
- В системе безопасности Grsecurity (на всех операционных системах).
- При использовании механизма seccomp (на всех операционных системах).
- При использовании технологий WSL1 и WSL2 (на всех операционных системах).
- При использовании параметров монтирования файловых систем (например, noexec, nosuid и других).
- При установке приложения Kaspersky Embedded Systems Security внутри контейнера.

На операционных системах с auditd версии 3.0.7 и ядром Linux версии 4.18 при использовании Анализа поведения возможны зависания приложения и ssh-соединений.

Поддерживаемые версии Kaspersky Security Center

Вы можете управлять приложением Kaspersky Embedded Systems Security с помощью Kaspersky Security Center следующих версий:

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

Для управления приложением Kaspersky Embedded Systems Security через Kaspersky Security Center требуется Агент администрирования Kaspersky Security Center.

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

Что нового

В приложении Kaspersky Embedded Systems Security 4.0 для Linux появились следующие возможности и доработки:

- Добавлена поддержка работы приложения на устройствах с архитектурой Arm.
- Добавлен новый функциональный компонент Защита от атак BadUSB. Компонент позволяет предотвратить подключение к клиентскому устройству зараженных USB-устройств, имитирующих клавиатуру.
- Скоро станет доступна интеграция Kaspersky Embedded Systems Security с решением Kaspersky Managed Detection and Response. Kaspersky Managed Detection and Response – решение, которое автоматически обнаруживает и анализирует инциденты безопасности в вашей инфраструктуре. Для этого решение Kaspersky Managed Detection and Response использует данные телеметрии, полученные от банкоматов и POS-терминалов, и машинное обучение.
- Доработан компонент Контроль устройств:
  - Добавлена возможность настроить список пользователей или групп пользователей, для которых добавленные устройства будут доверенными.
  - Добавлена возможность разрешать доступ к устройствам хранения данных только на чтение.
  - Добавлена возможность предоставить по запросу пользователя временный доступ к заблокированным устройствам.
  - В плагинах управления приложением реализована возможность добавления доверенных устройств на основании событий, передаваемых в Kaspersky Security Center, и расширены режимы импорта списка доверенных устройств из файла.
  - Улучшено информирование пользователя с помощью событий за счет добавления новых событий, уточнения и унификации текстов событий в плагинах и в командной строке.
- Доработан компонент Контроль приложений.
  - Добавлена возможность в режиме "список разрешенных" разрешать запуск скриптов, подписанных доверенными сертификатами.
  - Добавлен счетчик доверенных сертификатов.
- Добавлена возможность выбрать режим перехвата трафика, который приложение использует в своей работе: использование технологии eBPF или использование утилиты iptables и механизмов ядра, связанных с ней.
- Добавлена возможность настраивать исключения из перехвата трафика. Теперь вы можете указывать соединения, которые приложение будет исключать из перехвата трафика, с помощью плагинов управления приложением и с помощью командной строки.
- Добавлена возможность выбрать источник телеметрии (только eBPF или eBPF и auditd). Для auditd вы также можете выбрать режим работы (монопольный режим или режим многоадресной рассылки).
- Обновлен интерфейс политики в Web Console. Изменилась структура разделов в политике, чтобы быстрее находить нужные функции.

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

- Реализована возможность включать и выключать использование прокси-сервера KSN при взаимодействии приложения Kaspersky Embedded Systems Security с серверами KSN. Если использование прокси-сервера KSN включено, Kaspersky Embedded Systems Security взаимодействует с серверами KSN с помощью службы прокси-сервера KSN на Сервере администрирования. Если использование прокси-сервера KSN выключено, Kaspersky Embedded Systems Security взаимодействует с серверами KSN напрямую.

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

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

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

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

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

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

- 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.

- Добавлена возможность настраивать параметры резервного хранилища в свойствах управляемого устройства.

Версия 3.4

В приложении Kaspersky Embedded Systems Security 3.4 для Linux появились следующие возможности и доработки:

- Доработан компонент Контроль приложений. Добавлена возможность запретить запуск приложений, за исключением приложений, подписанных доверенными подписями.

- Добавлены параметры для задачи Инвентаризация. Теперь вы можете выбрать действие с категорией "Золотой образ" при завершении задачи.

- Реализован облачный режим работы приложения, в котором приложение использует облегченную версию баз вредоносного ПО. Это позволяет снизить нагрузку на оперативную память устройства.

- Реализован автоматический перезапуск приложения при обновлении. Теперь при обновлении приложение перезапускается автоматически, чтобы избавить администратора от дополнительного шага перезапуска приложения.

- В общие параметры приложения добавлены параметры, позволяющие задать ограничение на использование ресурсов процессора. При этом параметр `ScanPriority` был удален для задач проверки с типом *ODS* и *InventoryScan*.

- Реализована возможность выключения 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.

- В конфигурационный файл параметров приложения добавлены параметры, позволяющие указать директорию хранения файлов дампов и минимальное свободное место на диске после создания файлов дампов.

- Добавлена возможность просмотра журнала удаленной установки приложения и управления процессом трассировки в Web Console в свойствах управляемого устройства или в Консоли администрирования с помощью утилиты удаленной диагностики.

- Добавлена возможность экспорта и импорта списка доверенных устройств в плагинах управления приложением для компонента Контроль устройств.

- Добавлена возможность экспорта и импорта исключений по процессам в плагинах управления приложением для компонента Анализ поведения.

- Добавлена возможность настраивать взаимодействие приложения напрямую с серверами KSN при недоступности службы прокси-сервера KSN.

- В плагинах управления приложением в разделе **Хранилища** → **Резервное хранилище** реализована возможность отправить файл в "Лабораторию Касперского" на проверку.

- В графическом пользовательском интерфейсе реализовано уведомление пользователя о работе компонентов и задач приложения в информирующем режиме, при котором в случае обнаружения угрозы компоненты и задачи приложения не пытаются лечить или удалять вредоносные объекты, запрещать доступ или блокировать активность программ, а только информируют пользователя об обнаружении угрозы. Также в плагинах управления добавлено уведомление о включении информирующего режима для компонентов Защита от файловых угроз и Контроль устройств.

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

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

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

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

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

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

- В процедуру первоначальной настройки приложения в интерактивном режиме добавлена проверка наличия пользователей в привилегированных группах, а также улучшена проверка на наличие SELinux в системе.

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

- Защита и проверка контейнеров как отдельная функциональность не предоставляется. Если в предыдущей версии приложения были настроены задачи проверки контейнеров, то после обновления приложения эти задачи становятся недоступны и не отображаются. Проверка файлов в запускаемых контейнерах возможна в рамках Защиты от файловых угроз при включенной проверке пространств имен.

- Обновлен список поддерживаемых операционных систем.

Подготовка к установке приложения Kaspersky Embedded Systems Security

Перед началом установки приложения Kaspersky Embedded Systems 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 Embedded Systems 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 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 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 Embedded Systems Security. Для корректной работы Kaspersky Embedded Systems 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 kess 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 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.

- 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 Embedded Systems 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.

Установка и первоначальная настройка приложения Kaspersky Embedded Systems Security

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

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

Процедура установки приложения состоит из следующих этапов:

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

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

2. **Установка плагина управления Kaspersky Embedded Systems Security**

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

   - Веб-плагин управления Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security распространяется в пакетах форматов DEB и RPM. Предусмотрены отдельные пакеты для приложения и графического пользовательского интерфейса. Установите Kaspersky Embedded Systems Security и, если требуется, графический пользовательский 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 Embedded Systems Security**

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

Если вы установили приложение Kaspersky Embedded Systems 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 Embedded Systems Security с помощью командной строки, после завершения установки запустите скрипт первоначальной настройки или выполните первоначальную настройку в автоматическом режиме.

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 Embedded Systems Security

Для управления приложением Kaspersky Embedded Systems Security через Kaspersky Security Center используются следующие плагины управления Kaspersky Embedded Systems Security:

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

Вы можете одновременно установить плагины управления для разных версий приложения Kaspersky Embedded Systems 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 Embedded Systems Security

Веб-плагин управления Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security, то Лицензионное соглашение и весь интерфейс в Kaspersky Security Center Web Console будут отображаться на английском языке.

Установка MMC-плагина Kaspersky Embedded Systems Security

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

Перед установкой MMC-плагина управления Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security: **Kaspersky Embedded Systems Security <номер версии> для Linux**.

Установка и первоначальная настройка приложения с помощью Kaspersky Security Center

Вы можете установить приложение Kaspersky Embedded Systems 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 Embedded Systems Security. Инсталляционный пакет Kaspersky Embedded Systems 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 конфигурационном файле autoinstall.ini, который включен в инсталляционный пакет, или в свойствах инсталляционного пакета.

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 во время подготовки приложения к работе.

2. Развертывание приложения Kaspersky Embedded Systems 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 Embedded Systems Security, установленного на клиентских устройствах, вам нужно поместить эти устройства в группы администрирования. Перед началом установки приложения Kaspersky Embedded Systems 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".

Чтобы подготовить архивный файл для создания инсталляционного пакета:

1. Скачайте архив kess.zip на странице загрузки приложений в разделе **Kaspersky Embedded Systems Security для Linux** (**Дополнительный дистрибутив → Files for Product remote installation**).
2. Распакуйте архив kess.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 Embedded Systems Security:
     - kess-4.0.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
     - kess_4.0.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
     - kess-4.0.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
     - kess_4.0.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)
     - kess-4.0.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
     - kess_4.0.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)
   - для установки графического интерфейса приложения:
     - kess-gui-4.0.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
     - kess-gui_4.0.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
     - kess-gui-4.0.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
     - kess-gui_4.0.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)
     - kess-gui-4.0.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
     - kess-gui_4.0.0-<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 вы не планируете использовать 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 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 kess.zip.

4. Если вы хотите настроить параметры первоначальной настройки приложения с помощью конфигурационного файла, откройте конфигурационный файл autoinstall.ini и внесите необходимые изменения.

   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 Embedded Systems 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.
   - **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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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.
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.
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.
Запустить задачу обновления баз после установки	Если флажок установлен, после установки приложения запускается задача обновления баз и модулей приложения. По умолчанию флажок установлен.
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.
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.
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 Embedded Systems Security. По умолчанию флажок установлен.
Удалить пользователей из привилегированных групп	Установите флажок, чтобы перед установкой приложения автоматически удалить пользователей из привилегированных групп kessadmin и kessaudit. 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.

Параметр	Описание
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 kess_startup.log в директории /var/log/kaspersky/kess/. 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.

Создание инсталляционного пакета в Консоли администрирования

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

Чтобы подготовить файлы для создания инсталляционного пакета:

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

2. Распакуйте архив kess.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 Embedded Systems Security:
     - kess-4.0.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
     - kess_4.0.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
     - kess-4.0.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
     - kess_4.0.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)
     - kess-4.0.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
     - kess_4.0.0-<номер сборки>_arm64.deb (для 64-битных операционных систем для архитектуры Arm с dpkg)
   - для установки графического интерфейса приложения:
     - kess-gui-4.0.0-<номер сборки>.i386.rpm (для 32-битных операционных систем с rpm)
     - kess-gui_4.0.0-<номер сборки>_i386.deb (для 32-битных операционных систем с dpkg)
     - kess-gui-4.0.0-<номер сборки>.x86_64.rpm (для 64-битных операционных систем с rpm)
     - kess-gui_4.0.0-<номер сборки>_amd64.deb (для 64-битных операционных систем с dpkg)

- kess-gui-4.0.0-<номер сборки>.aarch64.rpm (для 64-битных операционных систем для архитектуры Arm с rpm)
- kess-gui_4.0.0-<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 вы не планируете устанавливать графический интерфейс, вам нужно отказаться от его использования, настроив параметр `USE_GUI=No` в конфигурационном файле autoinstall.ini. 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 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. Для этого откройте конфигурационный файл autoinstall.ini и установите значение параметра `UPDATE_EXECUTE=no`. Файл autoinstall.ini находится в папке, в которую вы распаковали архив kess.zip.

   Если вы хотите настроить параметры первоначальной настройки приложения, откройте конфигурационный файл autoinstall.ini и внесите необходимые изменения.

Чтобы создать инсталляционный пакет Kaspersky Embedded Systems 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 Embedded Systems Security. Для этого откройте стандартное окно Windows с помощью кнопки **Обзор** и укажите путь к файлу kess.kud. Файл находится в папке, в которую вы распаковали архив kess.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 Embedded Systems 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	Описание
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**.
Запустить задачу обновления баз после установки	Если флажок установлен, после установки приложения запускается задача обновления баз и модулей приложения. По умолчанию флажок установлен.
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.
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.
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 Embedded Systems Security. По умолчанию флажок установлен.
Удалить пользователей из привилегированных групп	Установите флажок, чтобы перед установкой приложения автоматически удалить пользователей из привилегированных групп kessadmin и kessaudit. 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 kess_startup.log в директории /var/log/kaspersky/kess/. 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.

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 сразу 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 Embedded Systems 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/kess/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 kess-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.

5. 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.

Параметры конфигурационного файла autoinstall.ini

Параметр	Описание	Значения
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.	`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. Если вы включили использование KSN, автоматически включается облачный режим работы приложения, при котором Kaspersky Embedded Systems Security использует облегченную версию баз вредоносного ПО.

Параметр	Описание	Значения
GROUP_CLEAN	Обязательный параметр. Автоматическое удаление пользователей из привилегированных групп kessadmin и kessaudit 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.
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 RFC 3066. Если параметр `LOCALE` не указан, используется язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация операционной системы не поддерживается, устанавливается значение по умолчанию `en_US.utf8`.
INSTALL_LICENSE	Код активации для добавления лицензионного ключа в приложение.	`<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.	`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.	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.	`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 задачи защиты от файловых угроз (для операционных систем, не поддерживающих технологию fanotify).	`yes` (значение по умолчанию) – компилировать модуль ядра при запуске задачи Защита от файловых угроз. `no` – не компилировать модуль ядра.
USE_GUI	Установка и использование графического интерфейса приложения.	`yes` – установить и использовать графический интерфейс приложения (файлы для установки графического интерфейса помещены 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 Embedded Systems Security.	`yes` (значение по умолчанию) – выполнить автоматическую настройку SELinux для работы с Kaspersky Embedded Systems Security. `no` – не выполнять автоматическую настройку SELinux для работы с Kaspersky Embedded Systems Security.
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.
ENABLE_TRACES_ON_FIRST_STARTUP	Создание файла трассировки приложения при первом запуске после установки. Для записи трассировки автоматически создается файл kess_startup.log в директории /var/log/kaspersky/kess/. 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> (приложение не обрабатывает пробелы между именем параметра и его значением).

Подготовка приложения к работе с помощью Kaspersky Security Center

После развертывания приложения Kaspersky Embedded Systems Security через Kaspersky Security Center требуется подготовить приложение к работе. Для этого 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 Embedded Systems Security.

   > Kaspersky Embedded Systems 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 Embedded Systems Security.

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

Установка и первоначальная настройка приложения с помощью командной строки

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

Установка с помощью командной строки состоит из следующих этапов:

1. Установка приложения и графического интерфейса приложения. Вы можете использовать следующие варианты установки приложения:

   - 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 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 путем запуска специального скрипта первоначальной настройки, который входит в комплект поставки приложения Kaspersky Embedded Systems 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 Embedded Systems Security из пакета формата RPM на 32-битную операционную систему, выполните следующую команду:

```
# rpm -i kess-4.0.0-<номер сборки>.i386.rpm
```

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

```
# rpm -i kess-4.0.0-<номер сборки>.x86_64.rpm
```

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

```
# rpm -i kess-4.0.0-<номер сборки>.aarch64.rpm
```

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

```
# apt-get install ./kess_4.0.0-<номер сборки>_i386.deb
```

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

```
# apt-get install ./kess_4.0.0-<номер сборки>_amd64.deb
```

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

```
# apt-get install ./kess_4.0.0-<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 kess-gui-4.0.0-<номер сборки>.i386.rpm
```

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

```
# rpm -i kess-gui-4.0.0-<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 kess-gui-4.0.0-<номер сборки>.aarch64.rpm
```

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

```
# apt-get install ./kess-gui_4.0.0-<номер сборки>_i386.deb
```

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

```
# apt-get install ./kess-gui_4.0.0-<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 ./kess-gui_4.0.0-<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 Embedded Systems Security.

Мастер первоначальной настройки требуется запускать с root-правами.

Чтобы запустить мастер первоначальной настройки, выполните следующую команду:

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

Мастер пошагово запрашивает значения параметров приложения Kaspersky Embedded Systems 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 Embedded Systems Security обеспечивает защиту устройства только после обновления баз приложения.

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 Embedded Systems 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 Embedded Systems 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/kess/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 Embedded Systems Security. Вы можете включить, выключить или изменить режим Kaspersky Security Network в любой момент.

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

Удаление пользователей из привилегированных групп

Этот шаг отображается, только если обнаружены пользователи в группе kessadmin и/или в группе kessaudit.

На этом шаге укажите, следует ли удалить пользователей из привилегированных групп kessadmin и kessaudit. Пользователи, включенные в группы kessadmin и kessaudit, получают привилегированный доступ к функциям приложения.

Введите `yes`, чтобы удалить всех обнаруженных пользователей из группы kessadmin и/или kessaudit. Пользователи, для которых группа kessadmin или kessaudit 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.

Определение типа перехватчика файловых операций

На этом шаге определяется тип перехватчика файловых операций для используемой операционной системы. Для операционных систем, не поддерживающих технологию fanotify, будет запущена компиляция модуля ядра.

При наличии всех необходимых пакетов модуль ядра будет автоматически скомпилирован при запуске задачи Защита от файловых угроз.

Если в процессе компиляции модуля ядра необходимые пакеты на устройстве не обнаружены, приложение Kaspersky Embedded Systems 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 Embedded Systems 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

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

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

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 Embedded Systems 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

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

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 Embedded Systems 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/kess/bin/kess-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 Embedded Systems 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 `kess-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.

Параметры конфигурационного файла первоначальной настройки

Параметр	Описание	Значения
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.	`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. Если вы включили использование KSN, автоматически включается облачный режим работы приложения, при котором Kaspersky Embedded Systems Security использует облегченную версию баз вредоносного ПО.

Параметр	Описание	Значения
GROUP_CLEAN	Обязательный параметр. Удаление пользователей из привилегированных групп kessadmin и kessaudit.	`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.
LOCALE	Дополнительный параметр. Языковой стандарт, используемый для локализации текстов Лицензионного соглашения, Политики конфиденциальности и Положения о Kaspersky Security Network, а также событий приложения, отправляемых в Kaspersky Security Center.	Языковой стандарт в формате, определенном в RFC 3066. Если параметр `LOCALE` не указан, устанавливается язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация операционной системы не поддерживается, устанавливается значение по умолчанию `en_US.utf8`. Локализация графического интерфейса и командной строки приложения зависит от локализации, указанной в переменной окружения `LANG`. Если в переменной окружения `LANG` указана локализация, которую приложение Kaspersky Embedded Systems Security не поддерживает, то графический интерфейс и командная строка отображаются в английской локализации.
INSTALL_LICENSE	Код активации или полный путь к файлу ключа для добавления лицензионного ключа в приложение.	`<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.	`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.	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.	`yes` – запускать задачу обновления. `no` – не запускать задачу обновления.

Параметр	Описание	Значения
KERNEL_SRCS_INSTALL	Автоматический запуск компиляции модуля ядра при запуске задачи Защита от файловых угроз для операционных систем, не поддерживающих технологию fanotify.	`yes` – компилировать модуль ядра при запуске задачи Защита 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 Embedded Systems Security.	`yes` – выполнить автоматическую настройку SELinux для работы с Kaspersky Embedded Systems Security. `no` – не выполнять автоматическую настройку SELinux для работы с Kaspersky Embedded Systems Security.
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.
ENABLE_TRACES_ON_FIRST_STARTUP	Создание файла трассировки приложения при первом запуске после установки. Для записи трассировки автоматически создается файл kess_startup.log в директории /var/log/kaspersky/kess/. 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.

Если вы хотите изменить параметры в конфигурационном файле первоначальной настройки, укажите значения параметров в формате <имя параметра>=<значение параметра> (приложение не обрабатывает пробелы между именем параметра и его значением).

Настройка разрешающих правил в системе SELinux

Если во время первоначальной настройки приложению Kaspersky Embedded Systems Security не удалось настроить систему SELinux автоматически или вы отказались от автоматической настройки, вы можете вручную настроить систему SELinux для работы с приложением Kaspersky Embedded Systems 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 Embedded Systems 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/kess/4.0.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kess/libexec/kess
   - /var/opt/kaspersky/kess/4.0.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kess/bin/kess-control
   - /var/opt/kaspersky/kess/4.0.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kess/libexec/kess-gui
   - /var/opt/kaspersky/kess/4.0.0.<номер сборки>_<метка времени установки>/opt/kaspersky/kess/shared/kess

4. Запустите следующие задачи:

   - задачу Защита от файловых угроз:

     ```
     kess-control --start-task 1
     ```

   - задачу Проверка важных областей:

     ```
     kess-control --start-task 4 -W
     ```

   Рекомендуется запустить все задачи, которые вы планируете запускать при использовании приложения Kaspersky Embedded Systems Security.

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

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

   ```
   # grep kess /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 Embedded Systems Security, выполнив следующие команды:

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

   В случае появления новых audit-сообщений, связанных с Kaspersky Embedded Systems 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 Embedded Systems Security (выполните шаги 1, 3–8).

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

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 (очередное обновление 1.7) и Astra Linux Special Edition (очередное обновление 1.8)

Чтобы запустить приложение в операционной системе Astra Linux Special Edition (очередное обновление 1.7 или очередное обновление 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/kess/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.

Запуск приложения в ОС Альт СП в режиме замкнутой программной среды

В этом разделе описаны действия, которые требуется выполнить, 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 kess для дальнейшего внесения изменений в политику IMA, выполнив команду:

   ```
   groupadd kess
   ```

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

   ```
   cat /etc/group | grep kess
   ```

4. Внесите изменения в политику IMA, чтобы исключить группу kess. 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 Embedded Systems 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 Embedded Systems Security /var/opt и /opt.

c. Сохраните изменения.

6. Установите приложение Kaspersky Embedded Systems 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 kess и права на директории для обновляемых компонентов приложения Kaspersky Embedded Systems Security, выполнив следующие команды:

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

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

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

```
kess-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 kess
```

Оптимизация потребления ресурсов приложением

Этот раздел содержит рекомендации специалистов "Лаборатории Касперского" по настройке приложения Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security использует ресурсы процессора, ввод-вывод дисковой подсистемы и оперативную память.

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

```
top -bn1|grep kess
```

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 kess
```

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 Embedded Systems 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:

   ```
   kess-control --get-task-list
   ```

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

   ```
   kess-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:

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

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

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

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

   ```
   kess-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/kess.

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:

```
kess-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/kess/kess.* | 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/kess/kess.* | 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/kess/kess.* | 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/kess/kess.* | 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:

    ```
    kess-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:

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

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

```
kess-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:

```
kess-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:

```
kess-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:

```
kess-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:

```
kess-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/kess/kess.* | 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/kess/kess.* | 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 Embedded Systems 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:

   ```
   kess-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 Embedded Systems Security использует во время выполнения задач проверки с типами OAS и ODS.

Ограничение на использование памяти может быть полезным для систем с большим объемом оперативной памяти (более 5 ГБ).

Вы можете регулировать размер оперативной памяти, используемой приложением при проверке файлов, с помощью параметра `ScanMemoryLimit` в конфигурационном файле kess.ini. Значение параметра по умолчанию: 8192 МБ. Минимальное значение параметра: 2 МБ. 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.

Чтобы указать ограничение на использование памяти при проверке файлов:

1. Остановите Kaspersky Embedded Systems Security.
2. Откройте файл /var/opt/kaspersky/kess/common/kess.ini на редактирование.
3. В секции `[General]` укажите нужное количество оперативной памяти в мегабайтах в значении параметра `ScanMemoryLimit`:

   ```
   ScanMemoryLimit=< количество памяти в мегабайтах >
   ```

4. Запустите Kaspersky Embedded Systems Security.

Ограничение на использование памяти при проверке файлов изменится при перезапуске приложения.

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:

    ```
    kess-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/kess/common/kess.ini, создать секцию `[Environment]` и добавить в нее параметр `TcpSynInterceptDisabled=1`.

2. Перезапустить приложение:

   ```
   systemctl restart kess
   ```

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 версию приложения Kaspersky Embedded Systems Security 3.4 для Linux до версии Kaspersky Embedded Systems Security 4.0 для Linux.

Перед началом обновления приложения Kaspersky Embedded Systems 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 Embedded Systems Security с помощью Kaspersky Security Center, вам нужно обновить Агент администрирования на защищаемых устройствах. Обновление выполняется путем установки новой версии Агента администрирования.

   Если Агент администрирования не обновлен, управлять приложением через Kaspersky Security Center будет невозможно.

   > 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 Embedded Systems Security**

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

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

   Вам нужно обновить приложение, установленное на защищаемых устройствах. Если вы используете графический пользовательский интерфейс приложения, вам также нужно обновить графический пользовательский интерфейс.

   Вы можете обновлять приложение и графический пользовательский 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 Embedded Systems Security запущено до начала процесса обновления, если обновление завершено успешно, то запустится новая версия приложения.

При обновлении версии приложения файлы дампов предыдущей версии удаляются.

После обновления приложения рекомендуется запустить задачу обновления баз.

Об обновлении плагинов управления Kaspersky Embedded Systems Security

Обновление плагина управления Kaspersky Embedded Systems 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 Embedded Systems Security;
- MMC-плагин управления Kaspersky Embedded Systems Security.

Политики и задачи, настроенные для предыдущих версий приложения Kaspersky Embedded Systems 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.

Экспорт и импорт параметров политики из предыдущих версий в Web Console не поддерживается. Некоторые значения параметров задач вы можете переносить из предыдущей версии задачи в новую путем экспорта и импорта параметров.

Плагины управления предыдущей версии продолжают работать после установки новой версии плагинов управления Kaspersky Embedded Systems Security. С их помощью вы можете управлять приложением Kaspersky Embedded Systems Security предыдущей версии.

Если вы обновили приложение на всех клиентских устройствах, вы можете удалить плагины управления Kaspersky Embedded Systems 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 пользовательского интерфейса выполняется путем удаленной установки новой версии пакетов приложения и графического пользовательского интерфейса на защищаемом устройстве.

Обновление с помощью Kaspersky Security Center состоит из следующих этапов:

1. Создание инсталляционного пакета.

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

2. Развертывание приложения Kaspersky Embedded Systems 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.

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 (~/.kess/<версия приложения>/license.<идентификатор языка>);
- новая версия Политики конфиденциальности расположена в директории (~/.kess/<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 (~/.kess/<версия приложения>/ksn_license.<ID языка>). Отказ от использования Kaspersky Security Network не прерывает процесс обновления приложения Kaspersky Embedded Systems 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 `KESS_EULA_AGREED=yes`, `KESS_PRIVACY_POLICY_AGREED=yes` и `KESS_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:

     ```
     # [KESS_EULA_AGREED=yes] [KESS_PRIVACY_POLICY_AGREED=yes] [KESS_USE_KSN=yes/no] rpm -U --replacefiles --replacepkgs kess-4.0.0-<номер сборки>.<arch>.rpm [kess-gui-4.0.0-<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:

     ```
     # [KESS_EULA_AGREED=yes] [KESS_PRIVACY_POLICY_AGREED=yes] [KESS_USE_KSN=yes/no] apt-get install ./kess_4.0.0-<номер сборки>_<arch>.deb [./kess-gui_4.0.0-<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 Embedded Systems Security будет автоматически перезапущено.

Пример:
Установить пакет приложения в формате RPM с пакетом графического пользовательского интерфейса для 64-битных операционных систем:

```
# KESS_EULA_AGREED=yes KESS_PRIVACY_POLICY_AGREED=yes KESS_USE_KSN=yes rpm -U --replacefiles --replacepkgs kess-4.0.0-< номер сборки >.x86_64.rpm kess-gui-4.0.0-< 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.

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`.

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`.

Удаление приложения

Процедура удаления приложения Kaspersky Embedded Systems 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 Embedded Systems Security.

2. **Удаление Агента администрирования**

   Если вы использовали Kaspersky Security Center для управления приложением Kaspersky Embedded Systems 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 Embedded Systems Security**

   Если вы использовали Kaspersky Security Center для управления приложением Kaspersky Embedded Systems Security, вам нужно удалить веб-плагин или MMC-плагин управления Kaspersky Embedded Systems 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.

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 Embedded Systems 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 kess kess-gui
```

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

```
# apt-get purge kess kess-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 kess
```

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

```
# apt-get purge kess
```

Удаление пакета графического интерфейса

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

```
# rpm -e kess-gui
```

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

```
# apt-get purge kess-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 Embedded Systems Security

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

Чтобы удалить MMC-плагин управления Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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/kess/doc/license.<идентификатор языка>.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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.

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. Для приложения Kaspersky Embedded Systems Security предусмотрен отдельный лицензионный ключ для активации интеграции с Kaspersky Managed Detection and Response – ключ MDR.

Вы можете добавить лицензионный ключ в приложение 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 или ключ для коммерческой лицензии (коммерческий ключ). Вы можете добавить в качестве активного ключа только один основной лицензионный ключ и один лицензионный ключ MDR.

- *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.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Embedded Systems Security. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Embedded Systems Security или после заказа пробной версии Kaspersky Embedded Systems 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 Embedded Systems Security или после заказа пробной версии Kaspersky Embedded Systems 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 Embedded Systems Security – это заказ на использование приложения с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на приложение Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security.

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 Embedded Systems Security на защищенном устройстве требуется добавить лицензионный ключ в приложение. Также для приложения Kaspersky Embedded Systems Security предусмотрен отдельный лицензионный ключ для активации интеграции с Kaspersky Managed Detection and Response – ключ MDR.

Если вы не активировали приложение Kaspersky Embedded Systems 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.

Вы также 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.

> 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 Embedded Systems Security.
   b. В раскрывающемся списке **Тип задачи** выберите **Добавление ключа**.

c. В поле **Название задачи** введите короткое описание, например, `Активация Kaspersky Embedded Systems 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 Embedded Systems Security, активируются по пробной лицензии Kaspersky Security Center Cloud Console автоматически. При этом активировать приложение Kaspersky Embedded Systems 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.

Чтобы добавить в приложение активный лицензионный ключ, выполните команду:

```
kess-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:

```
kess-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.

Чтобы удалить активный ключ, выполните команду:

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

Чтобы удалить резервный ключ, выполните команду:

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

Просмотр информации об используемых лицензионных ключах

Вы можете просматривать информацию о лицензионных ключах, которые использует приложение Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security. Вы можете посмотреть информацию о лицензии, которую использует приложение Kaspersky Embedded Systems 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 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 Embedded Systems 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 Embedded Systems 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.

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

```
kess-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 активный 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, если резервный ключ добавлен.
  - 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 MDR, если активный ключ MDR добавлен:
    - 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 MDR, если резервный ключ MDR добавлен:
    - 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 `kess-control --app-info`.

Предоставление данных

Этот раздел содержит информацию о данных, которые приложение Kaspersky Embedded Systems 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 Embedded Systems Security 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 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 приложению Kaspersky Security Center

Во время работы приложение Kaspersky Embedded Systems 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 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);
- 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;
- 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).

Данные, предоставляемые при переходе по ссылкам из интерфейса приложения

При переходе по ссылкам из интерфейса приложения Kaspersky Embedded Systems 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:

- идентификатор регионального центра активации;
- дату и время активации ПО;
- дату окончания срока действия лицензии;
- идентификатор лицензии;
- статус лицензии, по которой используется ПО;
- идентификатор конфигурации;
- контрольную сумму кода активации ПО;
- полную версию ПО;
- уникальный идентификатор устройства;
- идентификатор ПО;
- контрольную сумму файла ключа, с помощью которого активировано ПО;
- идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО;
- идентификатор сертификата, которым подписан заголовок подтверждения статуса лицензионного ключа ПО;
- дату и время создания подтверждения статуса лицензионного ключа ПО;
- контрольную сумму подтверждения статуса лицензионного ключа ПО;
- версию подтверждения статуса лицензионного ключа ПО;

- версию кода активации ПО;
- идентификатор подтверждения статуса активного лицензионного ключа;
- идентификатор конфигурации;
- результат действий, выполненных ПО;
- код ошибки;
- тип контрольной суммы обрабатываемого объекта;
- контрольную сумму обрабатываемого объекта;
- идентификатор компонента ПО;
- версию списка отозванных заключений службы ПО;
- идентификатор сработавшей записи в антивирусных базах ПО;
- временную метку сработавшей записи в антивирусных базах ПО;
- тип сработавшей записи в антивирусных базах ПО;
- название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя;
- формат данных в запросе к инфраструктуре Правообладателя;
- адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP-адрес);
- номер порта;
- веб-адрес источника запроса к веб-службе (referer);
- тип установленного ПО.

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:

- идентификаторы выполненных команд;
- дату и время получения данных;
- идентификатор операции, выполняемой со сторонним ПО;
- идентификатор обновления стороннего ПО;
- эвристически определенное имя отправителя сообщения электронной почты;

- идентификатор сообщения электронной почты;
- счетчик событий;
- время события;
- содержимое фрагмента в обрабатываемом объекте;
- уникальный идентификатор журнала активности обрабатываемого объекта;
- дату и время истечения сертификата;
- дату и время выдачи сертификата;
- архитектуру центрального процессора;
- уникальный идентификатор события;
- дату и время события;
- объем полного и используемого дискового пространства;
- текст сообщения об ошибке;
- название и версию ОС;
- количество циклов обновления и применения антивирусных баз;
- дату и время последнего обновления и применения антивирусных баз;
- идентификатор базы категоризации ПО;
- идентификатор записи в базах ПО;
- версию записи в базе данных ПО;
- дату и время выпуска баз ПО;
- временную метку баз ПО;
- битовую маску параметров DNS-запроса;
- тип запроса к DNS-серверу;
- модель центрального процессора;
- марку центрального процессора;
- контрольную сумму названия устройства пользователя (MD5, SHA2-256, SHA1);
- локальный порт, на который была проведена атака;
- дату и время на устройстве пользователя;
- идентификатор устройства;

- сообщения из системного журнала, содержащие информацию об ошибке;
- номер сборки ОС;
- номер обновления ОС;
- редакцию ОС;
- расширенную информацию о редакции ОС;
- идентификатор ОС;
- версию пакета обновления ОС;
- дату и время запуска ОС;
- идентификатор учетной записи, от имени которой был запущен контролируемый процесс;
- IP-адрес;
- сетевые интерфейсы компьютера;
- метод осуществления HTTP-запроса;
- место внедрения кода в обрабатываемом процессе;
- область действия, к которой принадлежит IP-адрес;
- уникальный идентификатор пользователя в системах Правообладателя;
- тип лицензии;
- идентификатор ключа из хранилища ключей, используемого для шифрования;
- имя компьютера в сети (доменное имя);
- протокол, используемый для передачи данных в KSN;
- идентификатор службы KSN, к которой обращается ПО;
- характеристики шифрования пакета данных, отправляемых в KSN;
- идентификатор пакета данных, отправляемых в KSN;
- внешний IP-адрес;
- локальный IP-адрес;
- MAC-адрес источника сетевой атаки;
- направление сетевого подключения;
- источник обрабатываемого сетевого трафика (локальный или удаленный хост);
- название сетевого протокола, используемого в обнаруженной сетевой атаке;

- тип учетной записи, с правами которой был запущен возможно зараженный объект;
- атрибуты обрабатываемого объекта;
- порядковый номер фрагмента в обрабатываемом объекте;
- загрузочные секторы ОС;
- данные внутреннего журнала, сформированного антивирусным компонентом ПО для обрабатываемого объекта;
- результат проверки сертификата;
- наименование эмитента сертификата;
- публичный ключ сертификата;
- алгоритм вычисления публичного ключа сертификата;
- серийный номер сертификата;
- дату и время подписи объекта;
- имя и параметры владельца сертификата;
- отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования;
- дату и время последней модификации обрабатываемого объекта;
- дату и время создания обрабатываемого объекта;
- характеристики обнаружения;
- уникальное имя объекта;
- файл обрабатываемого сообщения электронной почты;
- обрабатываемые объекты или их части;
- атрибуты обрабатываемого исполняемого файла;
- дату и время создания обрабатываемого исполняемого файла;
- описание обрабатываемого объекта, указанное в его свойствах;
- энтропию обрабатываемого объекта;
- формат обрабатываемого объекта;
- размер образа приложения;
- признак доверенности проверяемого объекта по KSN;
- результат проверки объекта в KSN;

- количество запусков ПО с момента последней отправки контрольной суммы файла;
- дату и время компоновки исполняемого файла;
- контрольную сумму (MD5) обрабатываемого объекта;
- имя обрабатываемого объекта;
- названия упаковщиков, которыми был упакован обрабатываемый объект;
- название ПО;
- контрольную сумму (MD5) маски, по которой была заблокирована веб-служба;
- контрольную сумму (SHA256) обрабатываемого объекта;
- информацию о том, кем был подписан обрабатываемый объект;
- размер обрабатываемого объекта;
- признак того, что объект находится в автозапуске;
- код типа объекта;
- название продавца ПО;
- заключение ПО по обрабатываемому объекту;
- версию обрабатываемого объекта;
- дату и время первого запуска обрабатываемого объекта;
- источник заключения по обрабатываемому объекту;
- источник получения обрабатываемого объекта;
- имя приложения, частью которого является обрабатываемый объект;
- уровень целостности обрабатываемого объекта;
- IP-адрес, с которого был загружен файл, соответствующий процессу;
- участки оперативной памяти защищаемого компьютера;
- идентификатор модуля ПО;
- результат проверки подписи модуля, целостность которого проверяется ПО;
- адрес загрузки модуля ПО;
- обнаруженные файловые операции, выполненные над обрабатываемым объектом;
- результат операции с обрабатываемым объектом;
- код файловой операции;

- путь к обрабатываемому объекту;
- код каталога файлов;
- идентификатор процесса в системе (PID);
- командную строку запуска;
- полные имена файлов, к которым обращался обрабатываемый процесс;
- IP-адрес, к которому обращался обрабатываемый процесс;
- права доступа, которыми обладает обрабатываемый объект;
- информацию о результатах проверки подписи файла;
- путь к исходному объекту;
- идентификатор уязвимости;
- класс опасности уязвимости;
- место срабатывания в обрабатываемом веб-трафике;
- файл обрабатываемой веб-страницы;
- пакеты данных обрабатываемого веб-трафика;
- идентификатор открытого окна обрабатываемой программы;
- разрядность ОС;
- путь к исполняемому файлу родительского процесса;
- идентификатор родительского процесса в системе (PID);
- аргументы командной строки, переданные процессу при запуске;
- дату и время запуска компонента мониторинг активности;
- версию компонента ПО;
- данные о лицензии для идентификации группы пользователей в компании, которая приобрела лицензию, по комментарию в свойствах лицензии;
- идентификатор обновления ПО;
- дату и время установки ПО;
- тип установки ПО;
- количество устройств/учетных записей, на которое рассчитана лицензия ПО;
- вложенную ошибку, возникшую при работе приложения;

- тип события, по которому собран пакет статистики;
- версию ПО;
- информацию об обновлениях ПО;
- идентификатор установки ПО (PCID);
- название компонента ПО;
- номер строки в тексте скрипта, где возникла ошибка;
- статус работоспособности ПО после обновления;
- название созданной/измененной службы ОС;
- ключ сеанса входа;
- алгоритм шифрования ключа сеанса входа;
- стек памяти в процессе ПО в момент сбоя;
- тип пользовательского сценария;
- данные атрибута;
- веб-адрес, с которого был загружен файл, соответствующий процессу;
- ответ DNS-сервера;
- IP-адрес DNS-сервера;
- имя модуля, в котором предположительно произошел сбой;
- дату и время окончания получения статистик;
- тип ошибки;
- действия пользователя с элементом интерфейса в окне программы;
- время пребывания объекта в буфере;
- IP-адрес атакующего компьютера;
- признак того, что обнаружение является отладочным;
- признак обрабатываемого объекта, по которому было отозвано решение по этому объекту;
- идентификатор задачи, в рамках которой произошло обнаружение;
- количество подключений к KSN, взятых из кеша;
- количество запросов, для которых был найден ответ в локальной базе запросов;
- количество неуспешных подключений к KSN;

- количество неуспешных KSN-транзакций;
- распределение по времени выполнения отмененных запросов к KSN;
- распределение по времени выполнения неуспешных подключений к KSN;
- распределение по времени выполнения неуспешных KSN-транзакций;
- распределение по времени выполнения успешных подключений к KSN;
- распределение по времени выполнения успешных KSN-транзакций;
- распределение по времени выполнения успешных запросов к KSN;
- распределение по времени выполнения запросов к KSN, превысивших ограничение на время ожидания;
- количество новых подключений к KSN;
- количество неуспешных запросов к KSN из-за ошибок маршрутизации;
- количество неуспешных запросов из-за выключенного KSN в параметрах ПО;
- количество неуспешных запросов к KSN из-за сетевых проблем;
- количество успешных подключений к KSN;
- количество успешных KSN-транзакций;
- количество выполненных запросов к KSN;
- тип сообщения статистики;
- степень уверенности в определении обращения к фишинговой веб-службе;
- цель фишинговой атаки;
- весовую характеристику обнаруженного обращения к фишинговой веб-службе;
- идентификатор протокола;
- идентификатор операции, выполняемой ПО;
- дату и время начала получения статистики;
- вероятность отправки статистики компонентом мониторинг активности;
- код события, обрабатываемого компонентом мониторинг активности дольше стандартного времени обработки;
- время обработки события в базах, обработка которого компонентом мониторинг активности длилась дольше стандартного времени;
- время задержки обработки события о совершении действия в ОС в подсистеме поведенческого анализа;
- количество задержанных событий текущего типа, совершенных в ОС;

- максимально допустимое время обработки события компонентом мониторинг активности;
- время задержки обработки события о совершении действия в ОС в подсистеме проактивной защиты;
- количество обработанных событий, совершенных в ОС;
- количество обработанных синхронных событий, совершенных в ОС;
- суммарную задержку всех событий текущего типа, совершенных в ОС;
- время задержки обработки события о совершении действия в ОС в подсистеме постоянного хранения событий;
- время обработки события, обработка которого компонентом мониторинг активности длилась дольше стандартного времени;
- общее количество событий, обработка которых компонентом мониторинг активности длилась дольше стандартного времени;
- суммарную задержку всех событий, совершенных в ОС;
- количество ожидающих синхронных событий, совершенных в ОС;
- дату и время обнаружения стороннего ПО компонентом мониторинг активности;
- номер обнаруженного ПО в контексте компонента мониторинг активности;
- причину обнаружения стороннего ПО компонентом мониторинг активности;
- дату и время получения события о совершении действия в ОС;
- версию отправляемой статистики;
- технические характеристики применяемых технологий обнаружения;
- версию определенного компилятора;
- свойства и контрольные суммы частей исполняемого файла;
- версию эмулятора;
- глубину эмуляции;
- тип задачи проверки исполняемого файла, в результате которой отправляется статистика;
- время хранения обрабатываемого объекта;
- алгоритм расчета отпечатка цифрового сертификата;
- название компонента;
- временную метку компонента обновления (обновленную версию);
- временную метку компонента (локальную версию);

- число неуспешных завершений установки обновления для компонента обновления;
- код категории ошибки;
- число ошибок установки обновления для компонента обновления;
- временную метку корневого индекса загружаемых обновлений;
- временную метку корневого индекса имеющихся обновлений;
- код ошибки задачи обновления;
- значение фильтра TARGET для задачи обновления;
- тип задачи обновления;
- версию компонента обновления;
- битовую маску параметров обрабатываемого объекта;
- контрольную сумму от имени пользователя;
- идентификатор безопасности учетной записи (SID);
- DNS-адрес веб-службы, к которой осуществляется обращение;
- источник хоста;
- заголовок обрабатываемого HTTP-запроса;
- IP-адрес (IPv4) веб-службы, на который осуществлялось обращение;
- IP-адрес (IPv6) веб-службы, на который осуществлялось обращение;
- признак того, что сообщение является одним из набора сообщений, относящихся к одному обращению к веб-службе;
- обрабатываемый веб-адрес;
- информация о клиенте, использующем сетевой протокол (user agent);
- идентификатор зоны безопасности из потока NTFS;
- идентификатор ПО, полученный из лицензии;
- идентификатор лицензии ПО;
- серийный номер лицензионного ключа ПО;
- локализацию ПО;
- идентификатор компании-партнера, у которого был размещен заказ на покупку лицензии на использование ПО;
- идентификатор ребрендинга ПО;

- статус работы компонента ПО;
- идентификатор ПО, для которого предназначена лицензия;
- признак участия в KSN;
- время задержки отправки статистики.

Концепция управления приложением

Для управления приложением Kaspersky Embedded Systems Security вы можете использовать:

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

Набор действий, которые вы можете выполнять с помощью графического пользовательского интерфейса приложения Kaspersky Embedded Systems 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 Embedded Systems Security на клиентских устройствах. Вы можете удаленно устанавливать и удалять, запускать и останавливать приложение Kaspersky Embedded Systems Security; настраивать параметры работы приложения, отдельных компонентов и задач приложения; запускать и останавливать задачи на управляемых устройствах.

Для управления приложением Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security через Kaspersky Security Center Cloud Console также обеспечивает веб-плагин.

MMC-плагин и веб-плагин позволяют создавать в Kaspersky Security Center политики и задачи для управления работой приложения Kaspersky Embedded Systems 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 Embedded Systems Security определяет общие параметры работы приложения Kaspersky Embedded Systems Security и параметры работы отдельных функциональных компонентов приложения на устройствах, где применяется политика.

- *Задачи* для Kaspersky Embedded Systems Security, созданные в Kaspersky Security Center, выполняются на защищаемых устройствах и реализуют такие функции Kaspersky Embedded Systems 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).

Независимо от консоли управления Kaspersky Security Center, которую вы используете, чтобы управлять через Kaspersky Security Center работой приложения Kaspersky Embedded Systems 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 Embedded Systems Security и настроить правила автоматического перемещения устройств в группы администрирования. Или вы можете вручную переместить устройства в группы администрирования после установки приложения Kaspersky Embedded Systems Security (см. подробнее в документации Kaspersky Security Center).

О плагинах управления Kaspersky Embedded Systems Security

Для управления приложением Kaspersky Embedded Systems Security через Kaspersky Security Center требуются следующие плагины управления:

- Веб-плагин управления Kaspersky Embedded Systems Security (далее также *веб-плагин*) обеспечивает взаимодействие приложения Kaspersky Embedded Systems 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 Embedded Systems Security с помощью веб-плагина доступно всем администраторам, у которых есть доступ к Kaspersky Security Center Web Console в браузере.

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

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

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

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

О политиках Kaspersky Security Center

Политика – это набор параметров приложения Kaspersky Embedded Systems 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;
- исключения памяти процессов из проверки в параметры приложения;
- доверенные домены в параметрах сети;
- доверенные корневые сертификаты в параметрах сети;
- контролируемые порты в параметрах сети.

Параметры работы приложения изменяются в соответствии с параметрами политики после первого применения политики.

Если во время удаления политики приложение не запущено, то после запуска приложения эта политика продолжает применяться на устройстве и приложение продолжает работать с параметрами, заданными этой политикой.

Подробнее о политиках и профилях политик, а также о механизме наследования параметров см. в справке Kaspersky Security Center.

О задачах для Kaspersky Embedded Systems Security, созданных в Kaspersky Security Center

Вы можете создавать в Kaspersky Security Center задачи следующих типов для приложения Kaspersky Embedded Systems 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 Embedded Systems Security.

Общая информация о задачах, созданных в Kaspersky Security Center, приведена в документации Kaspersky Security Center.

Для управления приложением Kaspersky Embedded Systems 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.
- *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.

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.

Чтобы войти в Web Console:

1. В браузере перейдите по адресу <веб-адрес Сервера администрирования>:<номер порта>.

   Откроется страница входа.

2. 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.

3. Нажмите на кнопку **Войти**.

   Если Сервер администрирования не отвечает или вы указали неверные учетные данные, отобразится сообщение об ошибке.

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.

  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 Embedded Systems Security 3.4 для Linux в версию Kaspersky Embedded Systems Security 4.0 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.

   Перейдите к следующему шагу мастера.

5. 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.

6. 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**. Политика, которая в настоящее время не применяется к устройству. Если выбран этот вариант, политика становится неактивной, 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.

7. Если вы хотите настроить другие параметры политики, перейдите на закладку **Параметры приложения** и внесите необходимые изменения.

   Вы также можете изменить параметры политики позже.

8. 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

Вы можете настраивать параметры политики на закладке **Параметры приложения** окна свойств политики.

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 сетевых соединений и средств коммуникации	**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.
Контроль безопасности	**Контроль устройств**. В этом подразделе вы можете настраивать параметры контроля устройств. **Контроль приложений**. В этом подразделе вы можете настраивать параметры контроля приложений. **Контроль целостности системы**. В этом подразделе вы можете настраивать параметры контроля целостности системы.

Раздел	Подразделы
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 Embedded Systems 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 использование механизма пространств имен. **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: • Использование Kaspersky Security Center в качестве прокси-сервера. • Параметры отправки информации в хранилище Kaspersky Security Center. **Настройки взаимодействия с ОС**. В этом подразделе вы можете настраивать дополнительные параметры сбора телеметрии. **Настройки уведомлений**. В этом подразделе вы можете настраивать параметры уведомлений о событиях.
Встроенные агенты	**Managed Detection and Response**. В этом подразделе вы можете включать и выключать интеграцию с Kaspersky Managed Detection and Response.
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.

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 **Kaspersky Embedded Systems Security 4.0 для Linux**.

   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 Embedded Systems 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. Если требуется, настройте основные параметры Защиты от файловых угроз.

   Перейдите к следующему шагу мастера.

9. Если требуется, измените настроенные по умолчанию параметры защиты от файловых угроз.

   Перейдите к следующему шагу мастера.

10. Если требуется, настройте исключения из защиты от файловых угроз.

    Перейдите к следующему шагу мастера.

11. Если требуется, измените настроенные по умолчанию действия при обнаружении угрозы.

    Перейдите к следующему шагу мастера.

12. 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**.

13. 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

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 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 Embedded Systems 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.
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.
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 настраивать использование механизма пространств имен. **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.

Управление задачами в Web Console

Вы можете выполнять следующие действия над задачами для Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 **OK** 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 Embedded Systems Security на устройстве, а также локально управлять работой приложения.

Работу функциональных компонентов приложения обеспечивают *локальные задачи Kaspersky Embedded Systems Security*, которые выполняются в операционной системе. Вы можете включать и выключать функциональные компоненты приложения на устройстве путем запуска и остановки задач Kaspersky Embedded Systems Security в командной строке. Однократные проверки устройства также выполняются путем запуска задач Kaspersky Embedded Systems Security. Вы можете задавать параметры работы функциональных компонентов на устройстве и параметры проверки устройства, настраивая *параметры задач* Kaspersky Embedded Systems Security.

Помимо параметров задач для настройки работы приложения предусмотрены следующие параметры:

- Параметры проверки защищенных соединений.
- Общие параметры приложения, которые определяют работу приложения в целом и работу отдельных функций.

Управление приложением Kaspersky Embedded Systems Security в командной строке выполняется с помощью *команд управления Kaspersky Embedded Systems Security*.

Включение автоматического дополнения команды kess-control (bash completion)

Для оболочки bash есть возможность включить автоматическое дополнение команды kess-control.

Чтобы включить автоматическое дополнение команды kess-control в текущей сессии оболочки bash, выполните следующую команду:

```
source /opt/kaspersky/kess/shared/bash_completion.sh
```

Чтобы включить автоматическое дополнение для всех новых сессий оболочки bash, выполните следующую команду:

```
echo "source /opt/kaspersky/kess/shared/bash_completion.sh" >> ~/.bashrc
```

Управление задачами в командной строке

Для управления приложением Kaspersky Embedded Systems 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 `kess-control --scan-file`. В результате выполнения команды приложение создает и запускает временную задачу проверки файлов.

- *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 Embedded Systems Security.

- *Анализ поведения*. Эта задача позволяет контролировать вредоносную активность приложений в операционной системе. Задача запускается автоматически при запуске приложения Kaspersky Embedded Systems 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.

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

Задача	Имя задачи в командной строке	ID задачи	Тип задачи
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
Анализ поведения	Behavior_Detection	20	BehaviorDetection
Контроль приложений	Application_Control	21	AppControl
Инвентаризация	Inventory_Scan	22	InventoryScan
Инвентаризация (пользовательская)	задается пользователем	от 100	InventoryScan
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. Вы можете создавать задачи следующих типов: *ODS*, *Update*, *Rollback*, *ODFIM* и *InventoryScan*;
- Изменять параметры всех пользовательских задач и всех предустановленных задач, кроме задач типов *Rollback* и *License*.
- Настраивать расписание запуска задач.

Просмотр списка задач в командной строке

Чтобы просмотреть список задач приложения, выполните следующую команду:

```
kess-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 Embedded Systems 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, Inventory_Scan, Update и Rollback недоступна.

Просмотр состояния задачи в командной строке

Чтобы посмотреть состояние задачи, выполните следующую команду:

```
kess-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

Вы можете создавать задачи следующих типов: *ODS*, *Update*, *Rollback*, *ODFIM* 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:

```
kess-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:

```
kess-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*.

Чтобы запустить задачу, выполните следующую команду:

```
kess-control --start-task <идентификатор/имя задачи> [-W] [--progress]
```

где:

- `<идентификатор/имя задачи>` – 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:
Запустить задачу с идентификатором 1 и включить вывод текущих событий, связанных с задачей:

```
kess-control --start-task 1 -W
```

Если при запуске задачи произошла ошибка и задача не запустилась, то после перезапуска приложения выполняется повторная попытка запуска задачи.

Чтобы остановить задачу, выполните следующую команду:

```
kess-control --stop-task <идентификатор/имя задачи> [-W]
```

где:

- `<идентификатор/имя задачи>` – идентификатор, присвоенный задаче в момент создания, или имя задачи в командной строке.
- `[-W]` – включение вывода текущих событий, связанных с этой задачей.

Чтобы приостановить задачу, выполните следующую команду:

```
kess-control --suspend-task <идентификатор/имя задачи>
```

Чтобы возобновить задачу, выполните следующую команду:

```
kess-control --resume-task <идентификатор/имя задачи>
```

Удаление задачи в командной строке

Вы можете удалять только пользовательские задачи. Предустановленные задачи недоступны для удаления.

Чтобы удалить задачу, выполните следующую команду:

```
kess-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:

```
kess-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:

```
kess-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*.

В командной строке вы можете изменять параметры задач с помощью команды `kess-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 `kess-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:

   `kess-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 Embedded Systems Security, требуется запускать команду `--set-settings` с ключом `--accept`.

Изменение параметров задачи с помощью ключей командной строки

С помощью ключей команды `kess-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:

```
kess-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 Embedded Systems 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:

```
kess-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:

```
kess-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:

```
kess-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:

```
kess-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:

```
kess-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:

```
kess-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

Вы можете настраивать расписание запуска для задач следующих типов: *ODS*, *Update*, *Rollback*, *ODFIM* 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:

```
kess-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:

```
kess-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:

```
kess-control --get-schedule 6 --file update_schedule.ini
```

Вывести в консоль расписание задачи обновления:

```
kess-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 `kess-control --get-schedule`.
2. Измените в файле значения нужных параметров и сохраните изменения.
3. Выполните команду:

   `kess-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:

```
kess-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:

```
kess-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=2025/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 или не блокировать файлы во время проверки).
- Настраивать исключения из проверки точек монтирования (глобальные исключения).
- Настраивать исключения из проверки памяти процессов.
- Включать и выключать обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным.
- 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:

```
kess-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:

```
kess-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 kess_config.ini. Сохранить созданный файл в текущей директории:

```
kess-control --get-app-settings --file kess_config.ini
```

Изменение общих параметров приложения

В командной строке вы можете изменять общие параметры приложения с помощью команды `kess-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:

   `kess-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:

```
kess-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/kess_config.ini:

```
kess-control --set-app-settings --file /home/test/kess_config.ini
```

Установить низкий уровень детализации файла трассировки:

```
kess-control --set-app-settings TraceLevel=NotDetailed
```

Добавить точку монтирования, которую требуется исключить из перехвата файловых операций:

```
kess-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):

  ```
  kess-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:

  ```
  kess-control -E --query "< условия фильтра >"
  ```

- Вывод информации об определенных объектах в резервном хранилище:

  ```
  kess-control -B --query "< условия фильтра >"
  ```

- Удаление определенных объектов из резервного хранилища:

  ```
  kess-control -B --mass-remove --query "< условия фильтра >"
  ```

  Примеры:

  Вывести информацию о событиях, которые содержат текст "etc" в поле FileName:

  ```
  kess-control -E --query "FileName like '%etc%'"
  ```

  Вывести информацию о событиях с типом ThreatDetected (обнаружена угроза):

  ```
  kess-control -E --query "EventType == 'ThreatDetected'"
  ```

  Вывести информацию о событиях с типом ThreatDetected, сформированных задачами типа ODS:

  ```
  kess-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):

  ```
  kess-control -E --query "Date > '1583425000'"
  ```

  Вывести информацию о событиях, сформированных после даты, указанной в формате YYYY-MM-DD hh:mm:ss:

  ```
  kess-control -E --query "Date > '2022-12-22 18:52:45'"
  ```

  Вывести информацию о файлах в резервном хранилище, имеющих высокий (High) уровень важности:

  ```
  kess-control -B --query "DangerLevel == 'High'"
  ```

Экспорт и импорт параметров приложения

Если вы управляете приложением Kaspersky Embedded Systems Security через Kaspersky Security Center, импорт параметров недоступен.

Kaspersky Embedded Systems 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 параметры проверки защищенных соединений, 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:

```
kess-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:

```
kess-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`. 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.

После импорта параметров приложения внутренние идентификаторы задач могут измениться. Для управления задачами рекомендуется использовать имена задач.

Управление ролями пользователей с помощью командной строки

Доступ к функциям приложения Kaspersky Embedded Systems 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: *kessadmin*, *kessuser*, *kessaudit* и *nokess*. 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:

- kessadmin соответствует роли Администратор;
- kessuser соответствует роли Пользователь;
- kessaudit соответствует роли Аудитор;
- nokess назначается пользователю, если не назначена ни одна из ролей. В этом случае пользователь относится к отдельной группе *пользователи без прав*.

Роли пользователей

Название роли	Роль в приложении	Группа пользователей ОС	Права
Администратор	admin	kessadmin	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	kessuser	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	kessaudit	Просмотр параметров приложения. Просмотр статуса приложения. Просмотр всех задач, их параметров и расписания запуска. Просмотр всех событий. Просмотр всех объектов в резервном хранилище.
—	—	nokess	Роль в приложении не назначена, права отсутствуют.

Просмотр списка пользователей и ролей

Чтобы просмотреть список пользователей и их ролей, выполните следующую команду:

```
kess-control [-U] --get-user-list
```

Назначение роли пользователю

Чтобы назначить роль определенному пользователю, выполните следующую команду:

```
kess-control [-U] --grant-role <роль> <пользователь>
```

Пример:
Назначить роль audit пользователю test15:

```
kess-control --grant-role audit test15
```

Отзыв роли у пользователя

Чтобы отозвать роль у определенного пользователя, выполните следующую команду:

```
kess-control [-U] --revoke-role <роль> <пользователь>
```

Пример:
Отозвать роль audit у пользователя test15:

```
kess-control --revoke-role audit test15
```

Запуск и остановка приложения

После установки приложения Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security

Чтобы запустить приложение, выполните следующую команду:

```
systemctl start kess
```

Чтобы остановить приложение, выполните следующую команду:

```
systemctl stop kess
```

Чтобы перезапустить приложение, выполните следующую команду:

```
systemctl restart kess
```

Мониторинг статуса приложения Kaspersky Embedded Systems Security

Мониторинг статуса приложения Kaspersky Embedded Systems 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 kess
```

Просмотр состояния защиты устройства и информации о работе приложения

Вы можете просматривать информацию о состоянии защиты устройства и о статусе работы приложения Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security на устройстве. В свойствах приложения Kaspersky Embedded Systems 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 `kess-control --app-info`, которая выводит информацию о работе приложения и состоянии функциональных компонентов и задач приложения;

  - команды `kess-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 `kess-control --get-statistic`, которая выводит статистику о работе приложения и список точек монтирования;

  - команды `kess-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 Embedded Systems Security.
- **Объекты, которые не удалось вылечить** – количество зараженных объектов, которые приложению Kaspersky Embedded Systems 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 Embedded Systems Security.

   Откроется окно свойств приложения.

В окне **Kaspersky Embedded Systems Security 4.0 для Linux** отображается следующая информация о приложении Kaspersky Embedded Systems 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 Embedded Systems 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.
- 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 **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 Embedded Systems Security и откройте окно свойств приложения двойным щелчком мыши или с помощью кнопки **Свойства** в нижней части окна.

   Откроется окно **Параметры Kaspersky Embedded Systems Security 4.0 для Linux**.

В окне **Параметры Kaspersky Embedded Systems Security 4.0 для Linux** отображается следующая информация о Kaspersky Embedded Systems 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 Embedded Systems 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 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:

```
kess-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 Embedded Systems 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 Embedded Systems Security**. Дата и время (UTC) окончания срока действия лицензии приложения.
- Информация о лицензии для активации дополнительной функциональности приложения. Поля отображаются, если на защищенное устройство добавлен ключ для дополнительной функциональности MDR:
  - **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.
- **Статус подписки**. Статус подписки. Это поле отображается, если приложение используется по подписке.
- **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.
- **Использование Kaspersky Security Network**. Информация об использовании Kaspersky Security Network: `Расширенный режим KSN`, `Стандартный режим KSN` или `Выключен`.
- **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`.
- **Защита от файловых угроз**. Статус защиты от файловых угроз в реальном времени.
- **Контроль целостности системы**. Статус компонента Контроль целостности системы.
- **Управление сетевым экраном**. Статус компонента Управление сетевым экраном.
- **Защита от шифрования**. Статус компонента Защита от шифрования.
- **Защита от веб-угроз**. Статус компонента Защита от веб-угроз.
- **Контроль устройств**. Статус компонента Контроль устройств.
- **Проверка съемных дисков**. Статус компонента Проверка съемных дисков.
- **Защита от атак BadUSB**. Статус компонента Защита от атак BadUSB.

- **Защита от сетевых угроз**. Статус компонента Защита от сетевых угроз.
- **Анализ поведения**. Статус компонента Анализ поведения.
- **Контроль приложений**. Статус компонента Контроль приложений.
- **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 kess.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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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.

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 Embedded Systems 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.

   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:

```
kess-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 Embedded Systems 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 Embedded Systems 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.

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 Embedded Systems Security во время своей работы оказывает влияние на операционную систему. Для анализа происходящего предусмотрена возможность сбора метрик, связанных с производительностью приложения.

Чтобы настроить сбор метрик о ресурсах операционной системы, используемых приложением, выполните следующую команду:

```
kess-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 kess. 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 kess. 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 kess. 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 kess. 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 kess в пользовательском пространстве, от начала запуска процесса kess 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 kess в пространстве ядра, от начала запуска процесса kess и до настоящего момента. Рекомендуется выставить пороговое значение самостоятельно на основе данных системы. Получить данные можно самостоятельно или с помощью скрипта для сбора информации. За примером скрипта вы можете обратиться в Службу технической поддержки.
lfs_system_cpu_usage_milliseconds метка type=total Counter	Количество миллисекунд процессорного времени, потребленное процессом kess в пользовательском пространстве и в пространстве ядра, от начала работы процесса kess и до настоящего момента. Если процессорное время процесса kess превышает всю остальную нагрузку, рекомендуется обратиться в Службу технической поддержки.

Внутреннее название метрики, метка и тип метрики	Описание и рекомендуемое пороговое значение
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 kess 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 kess 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 kess до настоящего момента.
lfs_tcpSynInterceptor_verdict_count метка verdict=unknown Counter	Общее количество сетевых соединений от начала работы процесса kess 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 и Защита от сетевых угроз), перехваченных приложением Kaspersky Embedded Systems 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 и Защита от сетевых угроз. Если разница между общим количеством задач и количеством выполненных задач неснижаемо растет, требуется добавить ресурсов, настроить исключения или обратиться в Службу технической поддержки.
lfs_tproxy_threadPool_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.

Внутреннее название метрики, метка и тип метрики	Описание и рекомендуемое пороговое значение
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.
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.

Внутреннее название метрики, метка и тип метрики	Описание и рекомендуемое пороговое значение
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.

Рекомендуется анализировать метрики в системах визуализации данных, например Grafana.

Для получения информации о характеристиках операционной системы и вашего устройства можно использовать скрипт. За примером скрипта и интеграции с системой Grafana вы можете обратиться в Службу технической поддержки.

Экспортированные метрики можно публиковать в основные системы мониторинга, например Prometheus и Zabbix. Для интеграции с системами мониторинга можно использовать скрипт, который будет получать информацию от приложения и публиковать ее в систему мониторинга. Для получения скрипта вы можете 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 Embedded Systems 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.

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.

Вы можете использовать групповую задачу *Обновление*, которую мастер первоначальной настройки создает после установки MMC-плагина управления или веб-плагина управления Kaspersky Embedded Systems 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.

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 Embedded Systems 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 Embedded Systems Security. Источником обновлений могут быть FTP-, HTTP- или HTTPS-серверы (например, серверы обновлений "Лаборатории Касперского") и локальные или сетевые директории, смонтированные пользователем.

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 Embedded Systems Security переключается к следующему источнику.

Приложение Kaspersky Embedded Systems 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 Embedded Systems 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*. При выборе собственного HTTPS-сервера в качестве источника обновления вам нужно убедиться, что он имеет корректную цепочку сертификатов. Использование самоподписанного сертификата возможно только в качестве корневого в цепочке сертификатов. В этом случае его требуется добавить в список доверенных сертификатов на устройстве.

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 Embedded Systems 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. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы 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 Embedded Systems 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. При нажатии на кнопку **Удалить** выбранный элемент будет удален из таблицы. Кнопка доступна, если в таблице выбран хотя бы 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.

Параметр	Описание	Значения
`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 `[CustomSources.item_#]`.

   Адрес источника обновлений должен совпадать с адресом, указанным в параметрах Kaspersky Update Utility.

Откат обновления баз и модулей приложения

После первого обновления баз приложения становится доступна функция отката баз приложения к их предыдущей версии.

Каждый раз, когда пользователь запускает процесс обновления, приложение Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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.

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**).

Параметры компонента Защита от файловых угроз

Параметр	Описание
Исключения из проверки	*Исключение из проверки* – это совокупность условий, при выполнении которых Kaspersky Embedded Systems 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 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 компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского". Kaspersky Embedded Systems Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
Действие при обнаружении угрозы	**Лечить. Удалять, если лечение невозможно**. Если выбрано это действие, приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, приложение удаляет файл. **Лечить. Блокировать, если лечение невозможно**. Если выбрано это действие, приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, приложение блокирует эти файлы (чтение/запись). **Блокировать**. Если выбрано это действие, приложение автоматически блокирует зараженные файлы без попытки их вылечить. 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	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. Для Linux-устройств вы можете изменять или удалять области проверки компонентом Защита от файловых угроз. Для работы компонента укажите хотя бы одну область защиты.
Проверка составных файлов	Распространенной практикой сокрытия вирусов и других приложений, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие приложения, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить типы проверяемых составных файлов, таким образом увеличив скорость проверки. • **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**. • **Файлы почтовых форматов**. Проверка файлов сообщений электронной почты в текстовом формате.
Не проверять архивы размером более (МБ)	Если флажок установлен, то приложение не проверяет составные файлы, размеры которых больше заданного значения. Если флажок снят, приложение проверяет составные файлы любого размера. Приложение проверяет файлы больших размеров, извлеченные из архивов, независимо от состояния флажка.

Параметр	Описание
Ограничить время проверки объектов до (сек)	Если флажок установлен, то приложение прекращает проверку составных файлов по истечению указанного времени. Если указано значение `0`, время проверки не ограничено.
Блокировать доступ к файлам во время проверки	Если флажок установлен, приложение блокирует доступ к файлам на устройстве на время проверки компонентами Защита от файловых угроз и Контроль устройств.

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 Embedded Systems Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS. Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – ресурсы файловой системы устройства, указанные в поле ниже. Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать **маски**. 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**.

Параметр	Описание
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.

Параметры Защиты от файловых угроз

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security проверяет самораспаковывающиеся архивы. Если флажок снят, Kaspersky Embedded Systems 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 Embedded Systems Security проверяет файлы почтовых баз. Если флажок снят, Kaspersky Embedded Systems 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 Embedded Systems Security проверяет сообщения в текстовом формате. Если флажок снят, Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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.

Параметр	Описание
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 Embedded Systems 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 Embedded Systems Security проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, Kaspersky Embedded Systems Security записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, Kaspersky Embedded Systems 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 Embedded Systems Security записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, Kaspersky Embedded Systems 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 Embedded Systems Security записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, Kaspersky Embedded Systems 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 Embedded Systems Security проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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.
	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**. 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 Embedded Systems Security исключает из проверки.

Примеры:
Маска `*.txt` – все текстовые файлы.
Маска `*_my_file_??.html` – html-файлы, начинающиеся с любых символов и заканчивающиеся сочетанием `_my_file_`, за которым следуют любые два символа (например, 2020_my_file_09.html).

Вы можете включить объединение списка исключений при наследовании в дочерних политиках. Для объединения элементов списка требуется установить флажок **Объединять значения при наследовании**. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.

Окно Исключения по названию угрозы

Вы можете настроить исключение объектов из проверки по названию угрозы. Приложение не будет блокировать указанные угрозы. По умолчанию список названий угроз пуст.

Вы можете добавлять, изменять и удалять названия угроз.

Вы можете включить объединение списка исключений при наследовании в дочерних политиках. Для объединения элементов списка требуется установить флажок **Объединять значения при наследовании**. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.

Окно Исключения по процессам

Окно содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса и файлов, изменяемых указанным процессом, из проверки. По умолчанию список содержит две области исключения, содержащие пути к Агентам администрирования. Вы можете удалить эти исключения, если требуется.

Параметры области исключения по процессам

Параметр	Описание
Объединять значения при наследовании	Флажок включает или выключает объединение списка при наследовании в дочерних политиках. Если флажок установлен, элементы списка родительской политики отображаются в дочерних политиках и в список дочерней политики можно добавить элементы. Если флажок снят, то элементы списка не объединяются при наследовании параметров политик. По умолчанию флажок снят.
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно → Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно → Экспортировать выбранное** или **Дополнительно → Экспортировать все**.

Окно Доверенный процесс

В этом окне вы можете добавить или настроить область исключения по процессам.

Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Это название будет отображаться в таблице окна **Исключения по процессам**. Поле ввода не должно быть пустым.
Путь к исключаемому процессу	Полный путь к процессу, который вы хотите исключить из проверки.
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.
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. 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.
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.

Параметр	Описание	Значения
SkipPlainTextFiles	Временное исключение из проверки файлов в текстовом формате. Если значение этого параметра SkipPlainTextFiles=Yes, приложение 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.	Yes – не проверять файлы в текстовом формате, если эти файлы повторно используются тем же процессом в течение 10 минут после последней проверки. No (значение по умолчанию) – проверять файлы в текстовом формате.
SkipDatabaseJournals	Временное исключение из проверки файлы журналов баз данных. Если значение этого параметра SkipDatabaseJournals=yes, 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.	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`
`Path`	Путь к директории с проверяемыми объектами.	`< путь к локальной директории >` – проверять 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. `Shared:NFS` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу NFS. `Shared:SMB` – проверять ресурсы файловой системы устройства, доступ к которым предоставляется по протоколу Samba. `Mounted:NFS` – проверять удаленные директории, смонтированные на устройстве по протоколу NFS. `Mounted:SMB` – проверять удаленные директории, смонтированные на устройстве по протоколу Samba. `AllRemoteMounted` – проверять все удаленные директории, смонтированные на устройстве с помощью протоколов Samba и NFS. `AllShared` – проверять все ресурсы файловой системы устройства, доступ к которым предоставляется по протоколам Samba и NFS. `<file system type>` – проверять все ресурсы указанной файловой системы устройства.
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры:		
`AreaDesc`	Описание области исключения из проверки, содержит дополнительную информацию об области исключения.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из проверки.	`Yes` (значение по умолчанию) – исключать указанную область. `No` – не исключать указанную область.

Параметр	Описание	Значения
`AreaMask.item_#`	Ограничение области исключения из проверки. В области исключения приложение не проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение исключает из проверки все объекты в области исключения. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать из проверки все объекты).
`Path`	Путь к директории с исключаемыми объектами.	`<путь к локальной директории>` – 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. `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. `<тип файловой системы>` – исключать из проверки все ресурсы указанной файловой системы устройства.
Секция **[ExcludedForProgram.item_#]** содержит следующие параметры:		
`ProgramPath`	Путь к исключаемому процессу.	`<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. `<тип файловой системы>` – 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:

   ```
   kess-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:

   `kess-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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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**.
Путь	Поле ввода пути к 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. 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**.
Путь	Поле ввода пути к 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. 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 Embedded Systems 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 Embedded Systems Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать **маски**. 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.

Параметр	Описание
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, приложение проверяет загрузочные секторы. Если флажок снят, приложение не проверяет загрузочные секторы. По умолчанию флажок снят.
Проверять память ядра и запущенные процессы	Флажок включает или выключает проверку памяти устройства. Если флажок установлен, приложение проверяет память ядра и запущенные процессы. Если флажок снят, приложение не проверяет память ядра и запущенные процессы. По умолчанию флажок снят.
Проверять объекты автозапуска	Флажок включает или выключает проверку объектов автозапуска. Если флажок установлен, приложение проверяет объекты автозапуска. Если флажок снят, приложение не проверяет объекты автозапуска. По умолчанию флажок снят.
Устройства для проверки	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях, во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области проверки

Таблица содержит маски имен устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять и удалять.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.

Параметр	Описание
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.

Параметр	Описание
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Окно Действия при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Embedded Systems 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 Embedded Systems 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.
	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**. 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 Embedded Systems 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 `kess-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.

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.
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 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`
`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.

Выборочная проверка файлов и директорий в командной строке

Вы можете выполнять выборочную проверку указанных файлов и директорий с помощью команды `kess-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:

```
kess-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.

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.
`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.*`

Параметр	Описание	Значения
`UseExcludeThreats`	Включение исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats.item_#`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (значение по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.
`UseOASExclusions`	Включение использования исключений Защиты от файловых угроз при проверке.	`Yes` (значение по умолчанию) – использовать исключения Защиты от файловых угроз. `No` – не использовать исключения Защиты от файловых угроз.
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию о незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию о проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию о необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (значение по умолчанию) – включить эвристический анализатор. `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка, минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) – рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.

Параметр	Описание	Значения
`DeviceNameMasks.item_#`	Список имен устройств, загрузочные секторы которых будет проверять приложение. Значение этого параметра не должно быть пустым. Для выполнения задачи требуется указать хотя бы одну маску имени устройства.	`AllObjects` – проверять загрузочные секторы всех устройств. `< 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.
`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 Embedded Systems 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**.
Путь	Поле ввода пути к 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. 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.

Параметр	Описание
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.
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.
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**. 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 Embedded Systems 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 Embedded Systems Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне вы можете добавить или настроить область проверки.

Параметры области проверки

Параметр	Описание
Название области проверки	Поле ввода названия области проверки. Это название будет отображаться в таблице окна **Области проверки**. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область проверки во время работы. Если флажок снят, приложение не обрабатывает эту область проверки во время работы. В дальнейшем вы можете включить эту область в параметры работы приложения, установив флажок. По умолчанию флажок установлен.

Параметр	Описание
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** (значение по умолчанию) – локальные директории. Если выбран этот элемент, вам нужно указать путь к локальной директории. • **Смонтированная** – смонтированные удаленные или локальные директории. Если выбран этот элемент, вам нужно указать протокол или название файловой системы. • **Общая** – ресурсы файловой системы защищаемого сервера, доступные по протоколу Samba или NFS. • **Все удаленные смонтированные** – все удаленные директории, смонтированные на устройстве по протоколам Samba и NFS. • **Все общие** – все ресурсы файловой системы защищаемого сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая** или **Смонтированная**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba. • **Пользовательская** – ресурсы файловой системы устройства, указанные в поле ниже.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область проверки. Для указания пути вы можете использовать **маски**. 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 Embedded Systems Security проверяет файлы. Если флажок снят, Kaspersky Embedded Systems Security не проверяет файлы. По умолчанию флажок снят.

Параметр	Описание
Проверять загрузочные секторы	Флажок включает или выключает проверку загрузочных секторов. Если флажок установлен, Kaspersky Embedded Systems Security проверяет загрузочные секторы. Если флажок снят, Kaspersky Embedded Systems 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 Embedded Systems Security проверяет память ядра и запущенные процессы. Если флажок снят, Kaspersky Embedded Systems 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 Embedded Systems Security проверяет объекты автозапуска. Если флажок снят, Kaspersky Embedded Systems Security не проверяет объекты автозапуска. По умолчанию флажок установлен.
Устройства для проверки	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Области проверки**, в котором вы можете указать устройства, загрузочные секторы которых нужно проверять.
Использовать глобальные исключения	Флажок включает или выключает исключение точек монтирования, указанных в глобальных исключениях, во время работы приложения. Если флажок установлен, приложение исключает настроенные точки монтирования из проверки. По умолчанию флажок установлен.
Использовать исключения Защиты от файловых угроз	Флажок включает или выключает использование настроенных исключений Защиты от файловых угроз во время работы приложения. Если флажок установлен, приложение исключает из проверки объекты, указанные в исключениях для компонента Защита от файловых угроз. По умолчанию флажок установлен.

Окно Области проверки

Таблица содержит маски имен устройств, загрузочные секторы которых должно проверять приложение. По умолчанию таблица содержит маску имени устройства **/**** – все устройства.

Элементы в таблице можно добавлять, изменять и удалять.

Окно Параметры проверки

В этом окне вы можете настроить параметры проверки файлов во время работы задачи.

Параметры проверки

Параметр	Описание
Проверять архивы	Флажок включает или выключает проверку архивов. Если флажок установлен, приложение проверяет архивы. Для проверки архива приложению требуется сначала распаковать его, что может замедлить проверку. Вы можете уменьшить продолжительность проверки архивов, настроив параметры **Пропускать файл, если его проверка длится более (сек.)** и **Пропускать файл, если его размер более (МБ)** в блоке **Общие параметры проверки**. Если флажок снят, приложение не проверяет архивы. По умолчанию флажок установлен.

Параметр	Описание
Проверять самораспаковывающиеся архивы	Флажок включает или выключает проверку *самораспаковывающихся архивов*. Самораспаковывающиеся архивы – это архивы, которые имеют в своем составе исполняемый модуль-распаковщик. Если флажок установлен, приложение проверяет самораспаковывающиеся архивы. Если флажок снят, приложение не проверяет самораспаковывающиеся архивы. Флажок доступен, если снят флажок **Проверять архивы**. По умолчанию флажок установлен.
Проверять почтовые базы	Флажок включает или выключает проверку почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat! и других почтовых клиентов. Если флажок установлен, приложение проверяет файлы почтовых баз. Если флажок снят, приложение не проверяет файлы почтовых баз. По умолчанию флажок снят.
Проверять файлы почтовых форматов	Флажок включает или выключает проверку файлов сообщений электронной почты в текстовом формате. Если флажок установлен, приложение проверяет сообщения в текстовом формате. Если флажок снят, приложение не проверяет сообщения в текстовом формате. По умолчанию флажок снят.
Пропускать файл, если его проверка длится более (сек.)	Поле, в котором вы можете указать максимальное время проверки файла в секундах. После истечения указанного времени приложение прекращает проверку файла. Доступные значения: 0–9999. Если указано значение 0, время проверки не ограничено. Значение по умолчанию: 0.
Пропускать файл, если его размер более (МБ)	Поле, в котором вы можете указать максимальный размер проверяемого файла в мегабайтах. Доступные значения: 0–999999. Если установлено значение 0, приложение проверяет файлы любого размера. Значение по умолчанию: 0.
Сообщать о незараженных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectProcessed*. Если флажок установлен, приложение записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. Если флажок снят, приложение не записывает в журнал события типа *ObjectProcessed* для всех проверяемых объектов. По умолчанию флажок снят.
Сообщать о необработанных объектах	Флажок включает или выключает запись в журнал событий типа *ObjectNotProcessed*, если не удается обработать файл во время проверки. Если флажок установлен, приложение записывает в журнал события типа *ObjectNotProcessed*. Если флажок снят, приложение не записывает в журнал события типа *ObjectNotProcessed*. По умолчанию флажок снят.
Сообщать об упакованных объектах	Флажок включает или выключает запись в журнал событий типа *PackedObjectDetected* для всех обнаруженных упакованных объектов. Если флажок установлен, приложение записывает в журнал события типа *PackedObjectDetected*. Если флажок снят, приложение не записывает в журнал события типа *PackedObjectDetected*. По умолчанию флажок снят.
Использовать технологию iChecker	Флажок включает или выключает проверку только новых файлов и файлов, измененных с момента последней проверки. Если флажок установлен, приложение проверяет только новые и измененные с момента последней проверки файлы. Если флажок снят, приложение проверяет файлы, не учитывая даты создания и изменения. По умолчанию флажок установлен.
Использовать эвристический анализ	Флажок включает или выключает использование эвристического анализа при проверке файлов. По умолчанию флажок установлен.

Параметр	Описание
Уровень эвристического анализа	Если флажок **Использовать эвристический анализ** установлен, вы можете выбрать уровень эвристического анализа в раскрывающемся списке: • **Поверхностный** – наименее детализированная проверка, минимальная нагрузка на систему. • **Средний** – средняя детализация при проверке, сбалансированная нагрузка на систему. • **Глубокий** – наиболее детализированная проверка, максимальная нагрузка на систему. • **Рекомендованный** (значение по умолчанию) – оптимальный уровень, рекомендуемый специалистами "Лаборатории Касперского". Он обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых устройств.

Окно Действия при обнаружении угрозы

В этом окне вы можете настроить действия, которые приложение Kaspersky Embedded Systems 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 Embedded Systems 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.
	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**. 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 Embedded Systems 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.

Параметры задачи Проверка важных областей

Параметр	Описание	Значения
`ScanFiles`	Включение проверки файлов.	`Yes` – проверять файлы. `No` (значение по умолчанию) – не проверять файлы.
`ScanBootSectors`	Включение проверки загрузочных секторов.	`Yes` (значение по умолчанию) – проверять загрузочные секторы. `No` – не проверять загрузочные секторы.
`ScanComputerMemory`	Включение проверки памяти процессов и памяти ядра.	`Yes` (значение по умолчанию) – проверять память процессов и память ядра. `No` – не проверять память процессов и память ядра.
`ScanStartupObjects`	Включение проверки объектов автозапуска.	`Yes` (значение по умолчанию) – проверять объекты автозапуска. `No` – не проверять объекты автозапуска.
`ScanArchived`	Включение проверки архивов (включая самораспаковывающиеся архивы SFX). Приложение проверяет такие архивы, как: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Список поддерживаемых форматов архивов зависит от используемых баз приложения.	`Yes` (значение по умолчанию) – проверять архивы. Если для параметра `ActionOnThreat` указано значение `DisinfectDeleteIfNotPossible` и лечение невозможно, то в зависимости от типа архива приложение удаляет либо зараженный объект, либо целиком весь архив, содержащий угрозу. `No` – не проверять архивы.
`ScanSfxArchived`	Включение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).	`Yes` (значение по умолчанию) – проверять самораспаковывающиеся архивы. `No` – не проверять самораспаковывающиеся архивы.

Параметр	Описание	Значения
`ScanMailBases`	Включение проверки почтовых баз приложений Microsoft Outlook, Outlook Express, The Bat и других.	`Yes` – проверять файлы почтовых баз. `No` (значение по умолчанию) – не проверять файлы почтовых баз.
`ScanPlainMail`	Включение проверки сообщений электронной почты в текстовом формате (plain text).	`Yes` – проверять сообщения электронной почты в текстовом формате. `No` (значение по умолчанию) – не проверять сообщения электронной почты в текстовом формате.
`SizeLimit`	Максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, приложение пропускает объект при проверке.	0 – 999999 0 – приложение проверяет объекты любого размера. Значение по умолчанию: 0.
`TimeLimit`	Максимальная продолжительность проверки объекта (в секундах). Приложение прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.	0 – 9999 0 – продолжительность проверки объектов не ограничена. Значение по умолчанию: 0.
`ActionOnThreat`	Выбор действия, которое приложение будет выполнять над зараженными объектами.	`DisinfectDeleteIfNotPossible` (лечить; удалять, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение удаляет зараженный объект. `DisinfectInformIfNotPossible` (лечить; информировать, если лечение невозможно) – приложение пытается вылечить зараженный объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), приложение сохраняет в журнале информацию об этом. `Inform` (информировать) – приложение не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале. Значение по умолчанию: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Включение исключения из проверки объектов, указанных параметром `ExcludeMasks.item_#`.	`Yes` – исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, указанные параметром `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Исключение из проверки объектов по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате shell.
	Перед тем как указать значение этого параметра, убедитесь, что включен параметр `UseExcludeMasks`.
		Значение по умолчанию не задано.
		Пример:
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Включение исключения из проверки объектов с угрозами, указанными параметром `ExcludeThreats.item_#`.	`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`. `No` (значение по умолчанию) – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats.item_#`.

Параметр	Описание	Значения

`ExcludeThreats.item_#`	Исключение из проверки объектов по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.
	Чтобы исключить объект из проверки, укажите полное название угрозы, обнаруженной в этом объекте: строку-заключение приложения о том, что объект является зараженным.
	Например, вы используете одну из утилит для получения информации о сети. Чтобы приложение не блокировало ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.
	Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале приложения или на веб-сайте https://threats.kaspersky.com.
		Значение параметра чувствительно к регистру.
		Значение по умолчанию не задано.
		Пример:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Включение использования глобальных исключений при проверке.	`Yes` (значение по умолчанию) – использовать глобальные исключения. `No` – не использовать глобальные исключения.
`UseOASExclusions`	Включение использования исключений Защиты от файловых угроз при проверке.	`Yes` (значение по умолчанию) – использовать исключения Защиты от файловых угроз. `No` – не использовать исключения Защиты от файловых угроз.
`ReportCleanObjects`	Включение записи в журнал информации о проверенных объектах, которые приложение признало незараженными. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен приложением.	`Yes` – записывать в журнал информацию о незараженных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о незараженных объектах.
`ReportPackedObjects`	Включение записи в журнал информации о проверенных объектах, которые являются частью составных объектов. Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен приложением.	`Yes` – записывать в журнал информацию о проверке объектов в составе архивов. `No` (значение по умолчанию) – не записывать в журнал информацию о проверке объектов в составе архивов.
`ReportUnprocessedObjects`	Включение записи в журнал информации об объектах, которые по какой-то причине не были обработаны.	`Yes` – записывать в журнал информацию о необработанных объектах. `No` (значение по умолчанию) – не записывать в журнал информацию о необработанных объектах.
`UseAnalyzer`	Включение эвристического анализатора. Эвристический анализ позволяет приложению распознавать угрозы еще до того, как они станут известны вирусным аналитикам.	`Yes` (значение по умолчанию) – включить эвристический анализатор. `No` – выключить эвристический анализатор.
`HeuristicLevel`	Уровень эвристического анализа. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.	`Light` – наименее тщательная проверка, минимальная загрузка системы. `Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы. `Deep` – наиболее тщательная проверка, максимальная загрузка системы. `Recommended` (значение по умолчанию) – рекомендуемое значение.
`UseIChecker`	Включение использования технологии iChecker.	`Yes` (значение по умолчанию) – включить использование технологии iChecker. `No` – выключить использование технологии iChecker.
`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 `/`.

Параметр	Описание	Значения
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.
`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 съемных дисков

Kaspersky Embedded Systems 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 Embedded Systems 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**).

Параметры компонента Проверка съемных дисков

Параметр	Описание
Тип проверки	**Быстрая проверка**. Если выбран этот вариант, то после подключения съемного диска Kaspersky Embedded Systems Security проверяет только файлы определенных форматов, наиболее подверженные заражению, и не распаковывает составные объекты. Быстрая проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Проверка важных областей*. **Подробная проверка**. Если выбран этот вариант, то после подключения съемного диска Kaspersky Embedded Systems Security проверяет все файлы, расположенные на съемном диске. Подробная проверка выполняется с параметрами, которые заданы по умолчанию для задачи *Поиск вредоносного ПО*.
Блокировать доступ к съемному диску во время проверки	Если флажок установлен, Kaspersky Embedded Systems Security блокирует доступ к файлам на подключенном диске во время выполнения проверки.

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**).

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*.
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.

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 рекомендуется выключить другие средства управления сетевым экраном операционной системы.

При включении компонента Управление сетевым экраном приложение Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security, можно просмотреть только с помощью команд управления (команда `kess-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 динамических правилах

Приложение Kaspersky Embedded Systems 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.

Kaspersky Embedded Systems 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 `kess-control -F --query`), но не можете изменить параметры динамических правил.

О сетевых пакетных правилах

Сетевое пакетное правило представляет собой разрешающее или запрещающее действие, которое совершает Kaspersky Embedded Systems 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.

Параметры сетевого пакетного правила

Параметр	Описание
Имя правила	Поле ввода названия сетевого пакетного правила.
Приоритет	Приоритет выполнения для сетевого пакетного правила.
Действие	В раскрывающемся списке вы можете выбрать действие, которое будет выполнять компонент Управление сетевым экраном при обнаружении сетевой активности: • **Разрешать** сетевую активность (значение по умолчанию). • **Блокировать** сетевую активность.

Параметр	Описание
Направление	В раскрывающемся списке вы можете указать направление отслеживаемой сетевой активности: • **Входящее**. Если выбран этот элемент, компонент Управление сетевым экраном контролирует только входящие соединения. • **Входящее (пакет)**. Если выбран этот элемент, компонент Управление сетевым экраном контролирует только входящие пакеты. • **Входящее/Исходящее**. Если выбран этот элемент, компонент Управление сетевым экраном контролирует как входящие, так и исходящие соединения. • **Исходящее (пакет)**. Если выбран этот элемент, компонент Управление сетевым экраном контролирует только исходящие пакеты. • **Исходящее**. Если выбран этот элемент, компонент Управление сетевым экраном контролирует только исходящие соединения. • **Входящее/Исходящее (пакеты)**. Если выбран этот элемент, компонент Управление сетевым экраном контролирует как входящие, так и исходящие пакеты.
Записывать в отчет	Флажок позволяет указать, будут ли действия по сетевому правилу записываться в отчет. Если флажок установлен, приложение записывает в отчет действия по сетевому правилу. Если флажок снят, приложение не записывает в отчет действия по сетевому правилу. По умолчанию флажок снят.
Протокол	В раскрывающемся списке вы можете выбрать тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность: • **Все** • **TCP** • **UDP** • **ICMPv4** • **ICMPv6** • **IGMP** • **GRE** Если вы выбрали протокол TCP или UDP, вы можете через запятую указать номера портов устройства пользователя и удаленного устройства, соединение между которыми требуется контролировать. Если вы выбрали протокол ICMP или ICMPv6, вы можете задать тип и код ICMP-пакета.
Удаленные порты	Если в раскрывающемся списке **Протокол** выбран протокол передачи данных **TCP** или **UDP**, вы можете указать номер порта или диапазон номеров портов удаленных устройств, соединение между которыми требуется контролировать. Поле отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **TCP** или **UDP**.
Локальные порты	Если в раскрывающемся списке **Протокол** выбран протокол передачи данных **TCP** или **UDP**, вы можете указать номер порта или диапазон номеров портов локальных устройств, соединение между которыми требуется контролировать. Поле отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **TCP** или **UDP**.
ICMP-тип	Если в раскрывающемся списке **Протокол** выбран протокол передачи данных **ICMPv4** или **ICMPv6**, вы можете указать тип ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного типа, отправляемые узлом или шлюзом. Если флажок установлен, отображается поле для ввода типа ICMP.
ICMP-код	Если в раскрывающемся списке **Протокол** выбран протокол передачи данных **ICMPv4** или **ICMPv6**, вы можете указать код ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного (в поле под флажком **ICMP-тип**) типа и с указанным (в поле под флажком **ICMP-код**) кодом, отправляемые узлом или шлюзом Если флажок установлен, отображается поле для ввода кода ICMP.
Удаленные сетевые адреса	Сетевые адреса удаленных устройств, которые могут передавать и получать сетевые пакеты: • **Любой адрес**. Если выбран этот элемент, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с любым IP-адресом. • **Адрес подсети**. Если выбран этот элемент, сетевое правило контролирует сетевые пакеты, отправляемые и получаемые удаленными устройствами с IP-адресами, которые относятся к выбранному ниже типу сети: Доверенная сеть, **Публичная сеть** или **Локальная сеть**. • **Адреса из списка**. Если выбран этот элемент, сетевое правило контролирует отправку и получение сетевых пакетов удаленными устройствами с IP-адресами, указанными в таблице ниже. Вы можете указать сразу несколько адресов, в этом случае указывайте каждый адрес в новой строке для удобства их копирования.
Локальный	Сетевые адреса устройств с установленным приложением Kaspersky Embedded Systems Security, которые могут передавать и получать сетевые пакеты: • **Любой адрес**. Если выбран этот элемент, сетевое правило контролирует отправку и получение сетевых пакетов устройствами с установленным приложением Kaspersky Embedded Systems Security и любым IP-адресом. • **Адреса из списка**. Если выбран этот элемент, сетевое правило контролирует указанные в таблице ниже IP-адреса устройств с установленным приложением Kaspersky Embedded Systems Security, которые могут передавать и получать сетевые пакеты. Вы можете указать сразу несколько адресов, в этом случае указывайте каждый адрес в новой строке для удобства их копирования.

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 Embedded Systems 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**).

Параметры компонента Управление сетевым экраном

Параметр	Описание
Сетевые пакетные правила	Таблица сетевых пакетных правил. Сетевые пакетные правила используются для ввода ограничений на сетевые пакеты независимо от приложения. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных. В таблице представлены предустановленные сетевые пакетные правила, которые рекомендованы специалистами "Лаборатории Касперского" для оптимальной защиты сетевого трафика устройств. Компонент Управление сетевым экраном устанавливает приоритет выполнения для каждого сетевого пакетного правила и обрабатывает сетевые пакетные правила в порядке их расположения в списке сетевых пакетных правил, сверху вниз. Компонент Управление сетевым экраном находит первое по порядку подходящее для сетевого соединения сетевое пакетное правило и выполняет действие: разрешает или блокирует сетевую активность. Далее Компонент Управление сетевым экраном игнорирует все последующие сетевые пакетные правила для этого сетевого соединения. Сетевые пакетные правила имеют приоритет над сетевыми правилами приложений.

Параметр	Описание
Доступные сети	Таблица, содержащая информацию о сетевых соединениях, которые компонент Управление сетевым экраном обнаружил на устройстве 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). Приложение закрывает доступ к файлам и принтерам устройства, подключенного к такой сети. Сторонние пользователи также не могут получить доступ к информации через папки общего доступа и удаленный доступ к рабочему столу этого устройства. Компонент Управление сетевым экраном 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 устройства (например, для локальной сети организации или для домашней сети). • **Доверенная сеть**. Безопасная сеть, во время работы в которой устройство не подвергается атакам и попыткам несанкционированного доступа к данным. Для сетей с этим статусом приложение разрешает любую сетевую активность в рамках этой сети.
Всегда добавлять разрешающие правила для портов Агента администрирования	Флажок включает или выключает автоматическое добавление разрешающих правил для портов Агента администрирования.

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.
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 Embedded Systems Security, которые могут передавать и получать сетевые пакеты.
Удаленный адрес	Сетевые адреса удаленных устройств, которые могут передавать и/или получать сетевые пакеты.
Запись в отчет	В столбце указано, будет ли приложение записывать в отчет действия по сетевому пакетному правилу. Если в столбце указано **Да**, приложение записывает в журнал действия по сетевому пакетному правилу. Если в столбце указано **Нет**, приложение не записывает в журнале действия по сетевому пакетному правилу.

По умолчанию таблица сетевых пакетных правил пуста.

Сетевые пакетные правила в таблице можно добавлять, изменять, удалять, перемещать вверх и вниз.

Окно Добавление сетевого пакетного правила

В этом окне вы можете настроить параметры добавляемого сетевого пакетного правила.

Параметры сетевого пакетного правила

Параметр	Описание
Протокол	Вы можете выбрать тип протокола передачи данных, для которого вы хотите отслеживать сетевую активность: • **Любой** (значение по умолчанию) • **GRE** • **ICMP** • **ICMPv6** • **IGMP** • **TCP** • **UDP**
Направление	Вы можете указать направление отслеживаемой сетевой активности: • **Входящие пакеты**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует только входящие пакеты. • **Входящие**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует только входящие соединения. • **Входящие/Исходящие** (значение по умолчанию). Если выбран этот вариант, компонент Управление сетевым экраном контролирует как входящие, так и исходящие соединения. • **Входящие/Исходящие пакеты**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует как входящие, так и исходящие пакеты. • **Исходящие пакеты**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует только исходящие пакеты. • **Исходящие**. Если выбран этот вариант, компонент Управление сетевым экраном контролирует только исходящие соединения.
ICMP-тип	Вы можете указать тип ICMP. Компонент Управление сетевым экраном будет контролировать сообщения указанного типа, отправляемые узлом или шлюзом. Если выбран вариант **Определенный**, отображается поле для ввода типа ICMP. Окно отображается, если в раскрывающемся списке **Протокол** выбран протокол передачи данных **ICMP** или **ICMPv6**.

Параметр	Описание
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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 `kess-control -F --query`.

Параметр	Описание	Значения
DefaultIncomingAction	Действие по умолчанию, применяемое ко входящему соединению, если другие сетевые правила не применяются к этому виду соединения.	Allow (значение по умолчанию) – разрешать входящие соединения. Block – запрещать входящие соединения.
DefaultIncomingPacketAction	Действие по умолчанию, применяемое ко входящему пакету, если другие сетевые пакетные правила не применяются к этому виду соединения.	Allow (значение по умолчанию) – разрешать входящие пакеты. Block – запрещать входящие пакеты.
OpenNagentPorts	Добавление динамических правил для Агента администрирования в пакетные правила.	Yes (значение по умолчанию) – добавлять динамические правила для Агента администрирования в пакетные правила. No – не добавлять динамические правила для Агента администрирования в пакетные правила.
Секция **[PacketRules.item_#]** содержит сетевые пакетные правила для задачи Управление сетевым экраном. Вы можете указать несколько секций [PacketRules.item_#] в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания. Каждая секция [PacketRules.item_#] содержит следующие параметры:		
Name	Имя сетевого пакетного правила.	Значение по умолчанию: Packet rule #<n>, где n – это индекс.
FirewallAction	Действие, применяемое к соединениям, указанным в сетевом пакетном правиле.	Allow (значение по умолчанию) – разрешать сетевые соединения. Block – запрещать сетевые соединения.
Protocol	Тип протокола, для которого необходим мониторинг сетевой активности.	Any (значение по умолчанию) – задача Управление сетевым экраном контролирует всю сетевую активность. TCP UDP ICMP ICMPv6 IGMP GRE
RemotePorts	Номера портов удаленных устройств, соединение между которыми отслеживается. Вы можете указать значение в виде целого числа или в виде интервала. Этот параметр можно указать, только если для параметра Protocol установлено значение TCP или UDP.	Any (значение по умолчанию) – контролировать все удаленные порты. 0 – 65535.
LocalPorts	Номера портов локальных устройств, соединение между которыми отслеживается. Вы можете указать значение в виде целого числа или в виде интервала. Этот параметр можно указать, только если для параметра Protocol установлено значение TCP или UDP.	Any (значение по умолчанию) – контролировать все локальные порты. 0 – 65535.
ICMPType	Тип пакета ICMP. Этот параметр можно указать, только если для параметра Protocol установлено значение ICMP или ICMPv6.	Any (значение по умолчанию) – контролировать все типы пакетов ICMP. Целое число согласно спецификации протокола передачи данных.
ICMPCode	Код пакета ICMP. Этот параметр можно указать, только если для параметра Protocol установлено значение ICMP или ICMPv6.	Any (значение по умолчанию) – контролировать все коды пакетов ICMP. Целое число согласно спецификации протокола передачи данных.

Параметр	Описание	Значения
`Direction`	Направление отслеживаемой сетевой активности.	`IncomingOutgoing` или `InOut` (значение по умолчанию) – контролировать как входящие, так и исходящие соединения. `Incoming` или `In` – контролировать только входящие соединения. `Outgoing` или `Out` – контролировать только исходящие соединения. `IncomingPacket` или `InPacket` – контролировать только входящие пакеты. `OutgoingPacket` или `OutPacket` – контролировать только исходящие пакеты. `IncomingOutgoingPacket` или `InOutPacket` – контролировать как входящие, так и исходящие пакеты.
`RemoteAddress`	Сетевые адреса удаленных устройств, которые могут передавать и получать сетевые пакеты.	`Any` (значение по умолчанию) – контролируется отправка и / или получение сетевых пакетов удаленными устройствами с любым IP-адресом. `Trusted` – заданная сетевая зона для доверенных сетей. `Local` – заданная сетевая зона для локальных сетей. `Public` – заданная сетевая зона для публичных сетей. `d.d.d.d` – адрес версии IPv4, где d – десятичное число от 0 до 255. `d.d.d.d – d.d.d.d` – диапазон адресов версии IPv4. `d.d.d.d/p` – подсеть адресов версии IPv4, где p – число от 0 до 32. `x:x:x:x:x:x:x:x` – адрес версии IPv6, где x – шестнадцатеричное число от 0 до ffff. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` – диапазон адресов версии IPv6. x:x:x:x:x:x:x:x/p – подсеть адресов версии IPv6, где p – число от 0 до 128, можно использовать **::** для сокращения.
`LocalAddress`	Сетевые адреса устройств с установленным приложением Kaspersky Embedded Systems Security, которые могут передавать и получать сетевые пакеты.	`Any` (значение по умолчанию) – контролируется отправка и / или получение сетевых пакетов локальными устройствами с любым IP-адресом. `d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255. `d.d.d.d – d.d.d.d` – диапазон адресов версии IPv4. `d.d.d.d/p` – подсеть адресов версии IPv4, где p – число от 0 до 32. `x:x:x:x:x:x:x:x` – адрес версии IPv6, где x – шестнадцатеричное число от 0 до ffff. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` – диапазон адресов версии IPv6. x:x:x:x:x:x:x:x/p – подсеть адресов версии IPv6, где p – число от 0 до 128, можно использовать **::** для сокращения.
`LogAttempts`	Включение записи в отчет действия сетевого правила.	`Yes` – записывать действия в отчет. `No` (значение по умолчанию) – не записывать действия в отчет.
Секция **[NetworkZonesPublic]** содержит сетевые адреса, связанные с публичными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		

Параметр	Описание	Значения
`Address.item_#`	Указывает IP-адрес или IP-подсеть.	`d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255. `d.d.d.d/p` – подсеть адресов IPv4, где p – число от 0 до 32. `x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. `x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64. Значение по умолчанию: "" (в этой зоне нет сетевых адресов).
Секция **[NetworkZonesLocal]** содержит сетевые адреса, связанные с локальными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		
`Address.item_#`	Указывает IP-адрес или IP-подсеть.	`d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255. `d.d.d.d/p` – подсеть адресов IPv4, где p – число от 0 до 32. `x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. `x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64. Значение по умолчанию: `""` (в этой зоне нет сетевых адресов).
Секция **[NetworkZonesTrusted]** содержит сетевые адреса, связанные с доверенными сетями. Вы можете указать несколько IP-адресов или IP-подсетей.		
`Address.item_#`	Указывает IP-адрес или IP-подсеть.	`d.d.d.d` – адреса IPv4, где d – десятичное число от 0 до 255. `d.d.d.d/p` – подсеть адресов IPv4, где p – число от 0 до 32. `x:x:x:x:x:x:x:x` – адреса IPv6, где x – шестнадцатеричное число от 0 до ffff. `x:x:x:x::0/p` – подсеть адресов IPv6, где p – число от 0 до 64. Значение по умолчанию: `""` (в этой зоне нет сетевых адресов).

Настройка списка сетевых пакетных правил в командной строке

Чтобы добавить сетевое пакетное правило, выполните следующую команду:

```
kess-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 Embedded Systems 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:

```
kess-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:

```
kess-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:

- `kess-control --del-rule --name <название правила>`
- `kess-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:

- `kess-control --move-rule --name <название правила> --at <индекс>`
- `kess-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:

```
kess-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:

- `kess-control --del-zone <зона> --address <адрес>`
- `kess-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.

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 Embedded Systems Security анализирует активность приложений в операционной системе. Эвристический анализ может обнаружить опасные объекты, о которых нет записей в базах приложения Kaspersky Embedded Systems 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 Embedded Systems 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**).

Параметры компонента Защита от веб-угроз

Параметр	Описание
Доверенные веб-адреса	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 Embedded Systems Security поддерживает символы `*` и `?` для ввода **маски**. Использование масок для указания IP-адресов не поддерживается. 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).
Действие при обнаружении угрозы	**Информировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз информирует пользователя об обнаружении зараженного объекта в веб-трафике и позволяет загрузить объект на устройство. Также Защита от веб-угроз записывает в журнал и добавляет в список активных угроз информацию об обнаружении зараженного объекта. **Блокировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту, показывает сообщение в браузере о заблокированной попытке доступа и записывает в журнал информацию об об обнаружении зараженного объекта.

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**.
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.

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.
`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 и Защита от сетевых угроз. Компонент Защита от веб-угроз может 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 веб-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 и Защита от сетевых угроз.

Вы также можете настраивать исключения из перехвата трафика для приложения Kaspersky Embedded Systems 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.

- *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 kess_in – kess_worm_in передает сетевой трафик входящих соединений.

- Пара kess_out – kess_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**).

Параметры проверки зашифрованных соединений

Параметр	Описание
Прокси-сервер	Параметры прокси-сервера для доступа пользователей клиентских устройств в интернет. Приложение Kaspersky Embedded Systems Security использует эти параметры в работе некоторых компонентов защиты, в том числе для обновления баз и модулей приложения. По умолчанию использование прокси-сервера выключено.
Исключения для прокси-сервера	Блок параметров содержит кнопку **Настройки**, по нажатию на которую открывается окно **Исключения для прокси-сервера**, в котором вы можете выключить использование прокси-сервера для подключения к указанным адресам. 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 `?`).
Проверка защищенных соединений	По умолчанию проверка защищенных соединений включена. По нажатию на кнопку **Настройки** открывается окно **Настройки сети**, в котором вы можете настроить следующие параметры: • **Переход на домен с недоверенным сертификатом** – действие, которое приложение будет выполнять при переходе на домен с недоверенным сертификатом: • **Разрешать соединение** (значение по умолчанию) – разрешать подключение к домену с недоверенным сертификатом. • **Блокировать соединение** – блокировать подключение к домену с недоверенным сертификатом. • **Переход на домен с ошибкой проверки защищенного соединения** – действие, которое приложение будет выполнять при переходе на домен с ошибкой проверки сетевого трафика: • **Разрешать и 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 соединение** – 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.
Контролируемые порты	Режим контроля сетевых портов: • **Контролировать все сетевые порты**. Режим контроля сетевых портов, при котором приложение контролирует потоки данных, передаваемые через любые открытые сетевые порты устройства. • **Контролировать только выбранные сетевые порты** (значение по умолчанию). Режим контроля сетевых портов, при котором приложение контролирует выбранные сетевые порты устройства. По ссылке **Контролируемые порты** открывается окно **Контролируемые порты**, в котором вы можете указать сетевые порты, которые будет проверять приложение. Список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика, настроен в соответствии с рекомендациями специалистов "Лаборатории Касперского".

Параметр	Описание
Режим перехвата трафика	Режим перехвата трафика: **eBPF**. Режим перехвата трафика, при котором приложение использует для перехвата трафика технологию eBPF. **iptables** (значение по умолчанию). Режим перехвата трафика, при котором приложение использует для перехвата трафика утилиту iptables. Для изменения режима перехвата трафика требуется перезапустить приложение. Во время перезапуска происходит разрыв установленных сетевых соединений.

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 Embedded Systems Security будет считать доверенными при проверке зашифрованных соединений.
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**.

Параметр	Описание
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 Embedded Systems 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:

```
kess-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:

```
kess-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:

   ```
   kess-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:

```
kess-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:

```
kess-control -N --query user
```

Чтобы просмотреть список исключений из проверки зашифрованных соединений, добавленных приложением, выполните следующую команду:

```
kess-control -N --query auto
```

Чтобы просмотреть список исключений из проверки зашифрованных соединений, полученных из баз приложения, выполните следующую команду:

```
kess-control -N --query kl
```

Чтобы очистить список доменов, которые приложение автоматически исключило из проверки, выполните следующую команду:

```
kess-control [-N] --clear-web-auto-excluded
```

Управление списком доверенных корневых сертификатов

Чтобы добавить сертификат в список доверенных корневых сертификатов, выполните следующую команду:

```
kess-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:

```
kess-control --remove-certificate <субъект сертификата>
```

Чтобы просмотреть список доверенных корневых сертификатов, выполните следующую команду:

```
kess-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:

```
kess-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:

```
kess-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:

```
kess-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 Embedded Systems 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 Embedded Systems Security и клиентских приложений, вы можете использовать специальную разрешающую цепочку правил kess_bypass.

Цепочка kess_bypass – это специальный список правил, который приложение Kaspersky Embedded Systems Security создает в таблице mangle сетевого экрана операционной системы (iptables/ip6tables). Правила цепочки kess_bypass позволяют исключать трафик из перехвата приложением Kaspersky Embedded Systems Security. Цепочка kess_bypass добавляется первой в процесс обработки сетевых пакетов, таким образом правила kess_bypass обрабатываются в первую очередь, до всех остальных правил iptables.

Если приложение использует технологию eBPF для перехвата трафика, правила kess_bypass не применяются.

В отличие от исключений, которые вы можете настроить в параметрах Kaspersky Embedded Systems Security, цепочка kess_bypass позволяет использовать для настройки исключений не только направление трафика, IP-адрес и порт назначения, но и другие параметры соединений.

Изменение правил в цепочке kess_bypass выполняется средствами операционной системы.

Например, вы можете добавить в цепочку kess_bypass правило, выполнив следующую команду: `iptables -t mangle -I kess_bypass -m tcp -p tcp --dport http -j ACCEPT`.

Такое правило позволяет исключить из перехвата приложением Kaspersky Embedded Systems 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 и Защита от сетевых угроз.

При удалении приложения цепочка правил kess_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 Embedded Systems 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 Embedded Systems 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**).

Параметры компонента Защита от сетевых угроз

Параметр	Описание
Доверенный IP-адрес	Список IP-адресов доверенных устройств. Компонент Защита от сетевых угроз не блокирует сетевую активность с этих адресов. В список исключений можно добавить только IP-адрес в формате IPv4 или IPv6. Приложение также не заносит в отчет информацию о сетевых атаках с IP-адресов, входящих в список исключений.
Действие при обнаружении угрозы	**Блокировать**. При обнаружении угрозы компонент Защита от сетевых угроз блокирует атаку. **Блокировать атаку и атакующие устройства на (мин)**. При обнаружении угрозы 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 устройство пользователя от возможных будущих сетевых атак с этого адреса. Минимальное время, на которое атакующий компьютер можно добавить в список блокирования, составляет одну минуту. Максимальное время – 9999 минут.

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 Embedded Systems 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 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)**.

Параметры компонента Защита от атак BadUSB

Параметр	Описание
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 Embedded Systems Security покажет время блокировки USB-устройства. По истечении указанного времени, вам будет доступно 5 попыток ввода кода авторизации.
Тайм-аут при достижении максимального количества попыток (мин)	Время блокировки USB-устройства после заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).
Запрет на использование экранной клавиатуры для авторизации USB-устройств	Если переключатель включен, приложение запрещает использование экранной клавиатуры для авторизации USB-устройства, с которого невозможно ввести код авторизации.

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**).

Параметры компонента Защита от атак BadUSB

Параметр	Описание
Включить защиту от атак BadUSB	Флажок включает или выключает компонент Защита от атак BadUSB. По умолчанию компонент выключен.
Максимальное количество попыток авторизации USB-устройства	Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Embedded Systems 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.

Если защита от шифрования включена, приложение Kaspersky Embedded Systems 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.

Kaspersky Embedded Systems 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**).

Параметры компонента Защита от шифрования

Параметр	Описание
Исключения из проверки	*Исключение из проверки* – это совокупность условий, при выполнении которых Kaspersky Embedded Systems Security не проверяет объект на вирусы и другие приложения, представляющие угрозу.
Действие при обнаружении угрозы	**Информировать**. Если выбран этот вариант, то, обнаружив попытку шифрования, Kaspersky Embedded Systems Security добавляет событие о попытке шифрования в журнал событий. **Блокировать соединение на (мин)**. Если выбран этот вариант, то, обнаружив попытку шифрования, Kaspersky Embedded Systems Security блокирует сетевой трафик от устройства, которое осуществляет вредоносную деятельность, и добавляет событие о попытке шифрования в журнал событий. Вы можете указать длительность блокировки недоверенного устройства в минутах. Изменение параметра не влияет на длительность блокировки ранее заблокированных скомпрометированных устройств. Длительность блокировки не является динамическим значением и рассчитывается в момент блокировки.
Область защиты	*Область защиты* – список путей к директориям, в которых Kaspersky Embedded Systems Security отслеживает файловую активность. Kaspersky Embedded Systems Security поддерживает переменные среды и символы * и ? для ввода маски. Вы можете выбрать область защиты: **Все общие сетевые папки защищаемого устройства**. Приложение будет отслеживать файловую активность во всех директориях файловой системы сервера, доступных по протоколам Samba и NFS. **Только указанные общие папки**. Приложение будет отслеживать попытки шифрования только в указанных директориях.

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 Embedded Systems Security проверяет объекты в указанных областях в том порядке, в котором эти области перечислены в списке. Если требуется, поместите вложенную директорию выше родительской в списке, чтобы у вложенной директории параметры безопасности могли отличаться от родительской.

Окно <Новая область проверки>

В этом окне можно добавить или настроить область защиты компонента Защита от шифрования.

Параметры области защиты

Параметр	Описание
Название области	Поле ввода названия области защиты. Это название будет отображаться в таблице окна Области проверки. Поле ввода не должно быть пустым.
Использовать эту область	Флажок включает или выключает проверку этой области во время работы приложения. Если флажок установлен, приложение обрабатывает эту область защиты во время работы компонента. Если флажок снят, приложение не обрабатывает эту область защиты во время работы компонента. В дальнейшем вы можете включить эту область в параметры работы компонента, установив флажок. По умолчанию флажок установлен.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать область проверки. В раскрывающемся списке файловых систем вы можете выбрать тип файловой системы: • **Локальная** – локальные директории. • **Общая** – ресурсы файловой системы сервера, доступные по протоколу Samba или NFS. • **Все общие** (значение по умолчанию) – все ресурсы файловой системы сервера, доступные по протоколам Samba и NFS.
	Если в раскрывающемся списке файловых систем выбран тип **Общая**, то в раскрывающемся списке справа вы можете выбрать протокол удаленного доступа: • **NFS** – удаленные директории, смонтированные на устройстве по протоколу NFS. • **Samba** – удаленные директории, смонтированные на устройстве по протоколу Samba.
	Если в раскрывающемся списке файловых систем выбран тип **Локальная**, то в поле ввода вы можете указать путь к директории, которую вы хотите включить в область защиты. Для указания пути вы можете использовать **маски**. 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 Embedded Systems Security будет выполнять при обнаружении вредоносного шифрования: • **Информировать** пользователя. Kaspersky Embedded Systems Security не блокирует устройство, осуществляющее шифрование, только записывает событие об обнаружении вредоносного шифрования в журнал событий. • **Блокировать** устройство, осуществляющее шифрование (значение по умолчанию).

Параметр	Описание
Блокировать недоверенное устройство на (мин.)	Поле, в котором вы можете указать длительность блокировки недоверенного устройства в минутах. По истечении указанного времени приложение Kaspersky Embedded Systems 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**. 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 Embedded Systems 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.

Параметры 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`.

Параметр	Описание	Значения
`UseScanArea`	Включение защиты указанной области. Для выполнения задачи требуется включить защиту хотя бы одной области.	`Yes` (значение по умолчанию) – защищать указанную область. `No` – не защищать указанную область.
`AreaMask.item_#`	Ограничение области защиты. В области защиты приложение защищает только объекты, указанные с помощью масок в формате shell. Вы можете указать несколько элементов `AreaMask.item_#` в любом порядке. Приложение будет обрабатывать области по индексу в порядке возрастания.	Значение по умолчанию: `*` (защищать все объекты).
`Path`	Путь к директории с защищаемыми объектам.	`< путь к локальной директории >` – защищать локальную директорию, доступную через SMB/NFS. Для указания пути вы можете использовать **маски**. 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 Embedded Systems 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:

```
kess-control --get-blocked-hosts
```

В результате выполнения команды приложение выводит список заблокированных устройств в консоль.

Чтобы разблокировать устройства, выполните следующую команду:

```
kess-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.

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 Embedded Systems 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 Embedded Systems Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений или подписаны доверенными сертификатами Контроля приложений.

Если правила контроля приложений сформированы максимально полно, Kaspersky Embedded Systems 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 Embedded Systems Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего правилам. Kaspersky Embedded Systems Security может *применять правила* и выполнять заданные в правилах действия или *тестировать правила* и только информировать о попытке запуска приложения, удовлетворяющего правилам.

- Включать и выключать использование доверенных сертификатов в работе Контроля приложений и настраивать список доверенных сертификатов.

  При использовании собственного сертификата в случае его компрометации требуется самостоятельно переподписать защищаемые файлы и заменить сертификат в политике.

  Контроль приложений в режиме *список разрешенных* не блокирует запуск приложений и запускаемых через поддерживаемые интерпретаторы скриптов, подписанных доверенными сертификатами. Контроль приложений не контролирует запуск скриптов из интерпретаторов, не поддерживаемых приложением Kaspersky Embedded Systems Security и запуск скриптов, передаваемых интерпретатору не через командную строку. Kaspersky Embedded Systems Security поддерживает следующие интерпретаторы: Java; Perl (pl); Python (py) и sh-скрипты (ash, bash, csh, dash, ksh, sh, tcsh, zsh).

Если запуск интерпретатора разрешен правилами Контроля приложений, то Kaspersky Embedded Systems 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 Embedded Systems Security блокирует все скрипты, указанные в командной строке интерпретатора. Исключение: cat script.py | python.

- Экспортировать и импортировать настроенные параметры Контроля приложений.

Вы можете получать информацию о приложениях, установленных на защищаемых устройствах с помощью задачи Инвентаризация.

Контроль приложений не поддерживает управление запуском приложений Snap, Flatpak и AppImage.

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 Embedded Systems 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 Embedded Systems Security применяет или не применяет правило к приложению. В правилах используются включающие и исключающие условия:

  - *Включающие условия*. Kaspersky Embedded Systems Security применяет правило к приложению, если приложение соответствует хотя бы одному включающему условию.

  - *Исключающие условия*. Kaspersky Embedded Systems 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 Embedded Systems Security выполняет действие, указанное в правиле. Если параметры приложения соответствуют критериям, указанным в исключающем условии, Kaspersky Embedded Systems Security не контролирует запуск приложения.

Правила контроля приложений могут иметь один из следующих *статусов работы*:

- *Включено* – правило включено, Kaspersky Embedded Systems Security применяет это правило для контроля приложений.
- *Выключено* – правило выключено и не используется для контроля приложений.
- *Тест* – Kaspersky Embedded Systems 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.

Настройка контроля приложений в Web Console

В Web Console вы можете настраивать параметры контроля приложений в свойствах политики (**Параметры приложения** → **Контроль безопасности** → **Контроль приложений**).

Параметры компонента Контроль приложений

Параметр	Описание
Режим работы	**Разрешать все, не указанное в списке правил**. Если выбран этот режим, Контроль приложений разрешает всем пользователям запуск любых приложений, кроме приложений, запрещенных правилами Контроля приложений. **Блокировать все, не указанное в списке правил**. Если выбран этот режим, Контроль приложений запрещает всем пользователям запуск любых приложений, кроме приложений, разрешенных правилами Контроля приложений или подписанных доверенными сертификатами Контроля приложений.
Доверять приложениям, имеющим цифровую подпись	Флажок включает использование доверенных сертификатов в работе Контроля приложений. Флажок доступен, если для параметра **Режим работы** выбран режим **Блокировать все, не указанное в списке правил**. Если флажок установлен, Kaspersky Embedded Systems Security не блокирует запуск приложений и запускаемых через поддерживаемые интерпретаторы скриптов, подписанных доверенными сертификатами.
Доверенные сертификаты	На ссылке отображается количество добавленных доверенных сертификатов Контроля приложений. Ссылка доступна, если для параметра **Режим работы** выбран режим **Блокировать все, не указанное в списке правил**. По ссылке открывается окно, в котором вы можете настроить список доверенных сертификатов.
Действие	**Применять правила**. Kaspersky Embedded Systems Security управляет запуском приложений в соответствии с выбранным режимом. **Информировать**. Kaspersky Embedded Systems Security информирует о попытке запуска приложения.
Добавить правила из политики к локальным правилам	Если переключатель включен, приложение применяет правила, заданные в политике, совместно с локальными правилами, настроенными на защищаемом устройстве. Если переключатель выключен, приложение применяет только правила, заданные в политике.
Таблица правил	Правила контроля приложений, с помощью которых Kaspersky Embedded Systems Security контролирует запуск приложений на защищаемых устройствах.

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 Embedded Systems Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам: • **Применять правила** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Embedded Systems Security применяет правила контроля приложений и выполняет заданное в правилах действие. • **Тестировать правила**. При выборе этого варианта приложение Kaspersky Embedded Systems Security тестирует правила и формирует событие о попытке запуска приложения, удовлетворяющего правилам.
Режим Контроля приложений	Режим работы компонента Контроль приложений: • **Список разрешенных**. При выборе этого варианта приложение Kaspersky Embedded Systems Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений или подписаны доверенными сертификатами Контроля приложений. • **Список запрещенных** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Embedded Systems Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.

Параметр	Описание
Доверять приложениям, подписанным доверенным сертификатом	Флажок включает или выключает использование списка доверенных сертификатов в работе компонента Контроль приложений. Если флажок установлен, Контроль приложений в режиме *список разрешенных* не блокирует запуск приложений, подписанных доверенными сертификатами. Флажок доступен, если для параметра **Режим Контроля приложений** выбран вариант **Список разрешенных**. По кнопке **Настроить** открывается окно, в котором вы можете настроить список доверенных сертификатов 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 Embedded Systems 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.

Окно Доверенные сертификаты Контроля приложений

Вы можете настроить список сертификатов, которые компонент Контроль приложений будет считать доверенными. Контроль приложений разрешает запуск приложений, подписанных сертификатами из этого списка.

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**.

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 Embedded Systems Security, то при изменении параметров задачи с помощью конфигурационного файла или с помощью ключей командной строки требуется запускать команду `kess-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.
- Настраивать список доверенных сертификатов 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.

Параметр	Описание	Значения
`AppControlMode`	Режим работы компонента Контроль приложений.	`AllowList` – Kaspersky Embedded Systems Security запрещает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений или подписаны доверенными сертификатами Контроля приложений. `DenyList` (значение по умолчанию) – Kaspersky Embedded Systems Security разрешает всем пользователям запуск любых приложений, кроме тех, которые указаны в правилах контроля приложений.
`UseTrustedCustomCerts`	Включение использования доверенных сертификатов в работе Контроля приложений.	`Yes` (значение по умолчанию) – использовать доверенные сертификаты в работе компонента Контроль приложений. Контроль приложений в режиме *список разрешенных* не блокирует запуск приложений, подписанных доверенными сертификатами. Вы можете настроить список доверенных сертификатов Контроля приложений с помощью команд приложения. `No` – не учитывать список доверенных сертификатов в работе компонента Контроль приложений.
`AppControlRulesAction`	Действие, которое приложение Kaspersky Embedded Systems Security будет выполнять при обнаружении попытки запуска приложения, удовлетворяющего настроенным правилам.	`ApplyRules` (значение по умолчанию) – Kaspersky Embedded Systems Security применяет правила контроля приложений и выполняет заданное в правилах действие. `TestRules` – Kaspersky Embedded Systems Security тестирует правила и формирует событие об обнаружении приложения, удовлетворяющего правилу.
Секция **[Categories.item_#]** содержит следующие параметры:		
`Name`	Название категории приложений, для которой будет применяться правило.	
`UseIncludes`	Использование включающих условий для срабатывания правила.	`Yes` – применять правило к приложению, если приложение соответствует хотя бы одному включающему условию. `No` (значение по умолчанию) – не применять правило к приложению, даже если приложение соответствует включающему условию.
`IncludeFileNames.item_#`	Имя исполняемого файла, на которое срабатывает правило.	Для указания имени файла вы можете использовать **маски**. 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.

Параметр	Описание	Значения
`UseExcludes`	Использование исключающих условий для срабатывания правила.	`Yes` – не применять правило к приложению, если приложение соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию. `No` (значение по умолчанию) – применять правило к приложению, даже если приложение соответствует исключающему условию.
`ExcludeFileNames.item_#`	Имя исполняемого файла, на которое срабатывает правило.	Для указания имени файла вы можете использовать **маски**. 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.
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 Embedded Systems Security применяет это правило для контроля приложений. `Off` – правило не используется для контроля приложений. `Test` – Kaspersky Embedded Systems 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.

Параметр	Описание	Значения
`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 Embedded Systems Security применяет это правило для контроля приложений. `Off` – правило не используется для контроля приложений. `Test` – Kaspersky Embedded Systems 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 kess --set-settings и конфигурационного файла параметров задачи Контроль приложений (Application_Control);
- с помощью команды kess --set-categories и конфигурационного файла параметров категории.

Чтобы создать категории приложений, выполните следующую команду:

```
kess-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:

```
kess-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 `kess-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:

```
kess-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 Embedded Systems 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:

```
kess-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:

```
kess-control --get-settings 21 [--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.

Kaspersky Embedded Systems 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:

```
kess-control --set-settings 21 [--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 список категорий приложений и правил контроля приложений, выполните следующую команду:

```
kess-control --set-settings 21 --set-to-default
```

Управление списком доверенных сертификатов Контроля приложений

Чтобы добавить сертификат в список доверенных сертификатов Контроля приложений, выполните следующую команду:

```
kess-control --add-app-control-trust-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 сертификатов Контроля приложений, выполните следующую команду:

```
kess-control --remove-app-control-trust-certificate <серийный номер сертификата>
```

Чтобы просмотреть список доверенных сертификатов Контроля приложений, выполните следующую команду:

```
kess-control --query-app-control-trust-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.

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 Embedded Systems 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.

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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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.

Параметр	Описание
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 Embedded Systems 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.

Параметр	Описание	Значения
`AreaMask.item_#`	Ограничение области инвентаризации. В области инвентаризации приложение проверяет только файлы, указанные с помощью масок в формате shell. Если параметр не указан, приложение проверяет все объекты в области инвентаризации. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (проверять все объекты).
`Path`	Путь к директории с проверяемыми объектами.	`< путь к локальной директории >` – проверять объекты в указанной директории. Значение по умолчанию: `/usr/bin`
Секция **[ExcludedFromScanScope.item_#]** содержит следующие параметры.		
`AreaDesc`	Описание области исключения из инвентаризации.	Значение по умолчанию не задано.
`UseScanArea`	Исключение указанной области из инвентаризации.	`Yes` (значение по умолчанию) – исключать указанную область. `No` – не исключать указанную область.
`AreaMask.item_#`	Ограничение области исключения из инвентаризации по маскам в формате shell. Если параметр не указан, приложение исключает все объекты в области инвентаризации. Вы можете указать несколько значений этого параметра.	Значение по умолчанию: `*` (исключать все объекты).
`Path`	Путь к директории с исключаемыми объектами.	`< путь к локальной директории >` – исключать из проверки объекты в указанной директории. Для указания пути вы можете использовать **маски**. 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:

```
kess-control --get-app-list [--json]
```

где `--json` – выводить данные в формате JSON.

Kaspersky Embedded Systems 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 `kess-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 Embedded Systems 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**).

Параметры компонента Контроль устройств

Параметр	Описание
Доверенные устройства	Список доверенных устройств и пользователей, которым разрешен доступ к этим устройствам. Kaspersky Embedded Systems Security поддерживает символы `*` и `?` для ввода маски.
Шаблоны сообщений	**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.
Разрешить запрашивать временный доступ	Если флажок установлен, то пользователь может запрашивать временный доступ к заблокированному устройству в графическом интерфейсе или командной строке приложения.
Режим работы	Kaspersky Embedded Systems Security выполнит выбранное действие при попытке доступа к устройству, к которому запрещен доступ в соответствии с параметрами Контроля устройств: **Информировать**. При выборе этого действия приложение Kaspersky Embedded Systems Security тестирует выбранный режим доступа и формирует событие об обнаружении попытки доступа к устройству. **Блокировать**. При выборе этого действия приложение Kaspersky Embedded Systems Security применяет режим доступа, заданный для устройства или шины.

Параметр	Описание
Устройства и сети Wi-Fi	Список всех возможных типов устройств по классификации компонента Контроль устройств и режим доступа к ним.
Шины подключения	Список всех возможных шин подключения по классификации компонента Контроль устройств и режим доступа к ним. Kaspersky Embedded Systems Security разрешает или запрещает доступ к устройствам по шине подключения, если для устройства выбран режим **Зависит от шины**.

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.
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 Embedded Systems Security тестирует выбранный режим доступа и формирует событие об обнаружении попытки доступа к устройству. • **Блокировать** (значение по умолчанию). При выборе этого варианта приложение Kaspersky Embedded Systems 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	Имя 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 добавить устройство 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 импортировать список устройств из файла по кнопке **Дополнительно** → **Импортировать** и экспортировать список добавленных устройств в файл в формате JSON по кнопке **Дополнительно** → **Экспортировать выбранное** или **Дополнительно** → **Экспортировать все**. При импорте вам будет предложено заменить список доверенных устройств или добавить устройства к уже существующему списку.

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

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).

Параметр	Описание
Разрешать доступ пользователям и/или группам пользователей	Поле, в котором отображается имя пользователя и/или название группы пользователей, для которых устройство является доверенным. По умолчанию указано значение **\Everyone** (все пользователи).
Настроить	По нажатию на кнопку открывается окно **Доступ к доверенному устройству**.

Окно Устройства на клиентских устройствах

В этом окне вы можете добавить устройство в список доверенных, выбрав его в списке устройств, обнаруженных на управляемых клиентских устройствах.

Информация о существующих устройствах доступна, если создана активная политика и выполнена синхронизация с Агентом администрирования (выполняется с частотой, указанной в политике Агента администрирования, по умолчанию – каждые 15 минут).

При создании новой неактивной политики список будет пустым.

Добавление устройств из списка устройств, обнаруженных на управляемых клиентских устройствах

Параметр	Описание
Имя клиентского устройства	Поле ввода имени или маски имени управляемого устройства, для которого вы хотите найти подключенные устройства. По умолчанию указана маска * – все управляемые устройства.
Тип устройства	В раскрывающемся списке вы можете выбрать тип подключенного устройства для поиска (например, Жесткие диски или Устройства чтения смарт-карт). По умолчанию выбран элемент **Все устройства**.
Идентификатор устройства	Поле для ввода идентификатора или маски идентификатора устройства, которое вы хотите найти. По умолчанию указана маска * – все устройства.
Поиск на устройствах	По нажатию на кнопку приложение выполняет поиск устройств с указанными параметрами. Результаты поиска отображаются в таблице ниже.
Список обнаруженных устройств	Таблица содержит следующие столбцы: • **Имя клиентского устройства** – имя клиентского устройства, к которому подключено найденное устройство. • **Тип устройства** – тип найденного устройства (например, Жесткий диск или Устройство чтения смарт-карт). • **Имя устройства** – имя найденного устройства. • **Идентификатор устройства** – идентификатор найденного устройства.

Окно Список устройств на основе событий Контроля устройств

В этом окне вы можете сформировать список устройств, которые обнаружены в событиях Контроля устройств в Kaspersky Security Center. Устройства из этого списка вы можете затем добавить в список доверенных устройств.

Вы можете выбрать одно или несколько устройств для добавления в список доверенных устройств.

Информация об устройствах доступна, если включен Контроль устройств, существует активная политика и выполнена синхронизация с Агентом администрирования (выполняется с частотой, указанной в политике Агента администрирования, по умолчанию – каждые 15 минут).

При создании новой неактивной политики список будет пустым.

Добавление устройств из списка устройств, обнаруженных в событиях Kaspersky Security Center

Параметр	Описание
Типы событий	Вы можете выбрать с помощью флажков типы событий Контроля устройств, отправленные в Kaspersky Security Center. В список попадают устройства, обнаруженные в событиях указанного типа. По умолчанию все флажки установлены.
Группа администрирования	Поле для ввода названия группы администрирования, содержащей клиентские устройства, к которым подключены обнаруженные устройства. В список попадают только устройства, подключенные к клиентским устройствам из указанной группы администрирования. Вы можете указать часть названия группы. По умолчанию в список попадают устройства, подключенные к клиентским устройствам из любой группы администрирования.
Период формирования событий	В раскрывающемся списке вы можете выбрать период времени, в течение которого произошли события. В список попадают устройства, которые обнаружены в событиях, отправленных в Kaspersky Security Center в указанный период. По умолчанию в список попадают устройства, обнаруженные в событиях за последний месяц.
Поиск устройств	По нажатию на кнопку приложение выполняет поиск устройств с указанными параметрами. Результаты поиска отображаются в таблице ниже.
Найденные устройства	Таблица содержит следующие столбцы: • **Тип устройства** – тип найденного устройства (например, Жесткий диск или Устройство чтения смарт-карт). • **Идентификатор устройства** – идентификатор найденного устройства. • **Имя устройства** – имя найденного устройства. • **Имя клиентского устройства** – имя клиентского устройства, к которому подключено найденное устройство. • **Дата подключения** – дата подключения найденного устройства. • **Группа администрирования** – название группы администрирования, содержащей клиентское устройство, к которому подключено найденное устройство.
Комментарий	Поле ввода комментария к устройству, которое вы хотите добавить в список доверенных устройств (необязательное).
Разрешать доступ пользователям и/или группам пользователей	Поле, в котором отображается имя пользователя и/или название группы пользователей, для которых устройство является доверенным. По умолчанию указано значение **\Everyone** (все пользователи).
Настроить	По нажатию на кнопку открывается окно **Доступ к доверенному устройству**.

Окно Доступ к доверенному устройству

В этом окне вы можете настроить доступ пользователей или групп пользователей к выбранному доверенному устройству.

Доступ к доверенному устройству

Параметр	Описание
Пользователи и/или группы пользователей	Список пользователей и групп, для которых добавляемое устройство будет доверенным. По умолчанию таблица содержит элемент **\Everyone** (все пользователи). Вы можете добавлять, изменять и удалять пользователей и группы пользователей.

Окно Пользователь или группа

В этом окне вы можете указать пользователя или группу пользователей, для которых устройство будет доверенными.

Параметры доверенного устройства

Параметр	Описание
Тип	**Пользователь** или **Группа**, для которых устройство будет доверенным.
Имя пользователя или группы	Имя локального или доменного пользователя (без указания полного имени с доменом, если система допускает ввод имен пользователей в таком формате, или в формате <имя домена>\<имя пользователя> или <имя пользователя>@<имя домена>) или название группы пользователей, для которых устройство будут доверенным.

Окно Тип устройства

В этом окне вы можете настроить режим доступа для различных типов устройств.

Режим доступа для типов устройств

Параметр	Описание
Тип устройства	Тип устройства (например, Жесткие диски, Принтеры).
Режим доступа	Режим доступа к устройству. При нажатии на правую кнопку мыши открывается контекстное меню, в котором вы можете выбрать один из следующих пунктов: • **Разрешать** – разрешать доступ к устройствам выбранного типа. • **Блокировать** – запрещать доступ к устройствам выбранного типа. • **Зависит от шины** (значение по умолчанию) – разрешать или запрещать доступ к устройствам в зависимости от режима доступа для шины подключения. • **По правилам** – разрешать или запрещать доступ к устройствам в зависимости от правила доступа и расписания. Этот пункт меню доступен только для устройств хранения данных (Жесткие диски, Съемные диски, Дискеты, CD/DVD-приводы). • **Только чтение** – разрешать доступ к устройствам выбранного типа только на чтение. Этот пункт меню доступен только для устройств хранения данных (Жесткие диски, Съемные диски, Дискеты, CD/DVD-приводы).

Вы можете настроить правила доступа и расписания доступа в окне **Настройка правила доступа к устройствам**, которое открывается двойным щелчком мыши по названию типа устройства.

Окно Настройка правила доступа к устройствам

В этом окне вы можете настроить правила доступа и расписания для выбранного типа устройств.

Окно открывается по двойному щелчку на названии типа устройства в окне **Тип устройства**.

Правила доступа и расписания для устройств

Параметр	Описание
Пользователи и/или группы пользователей	Список пользователей и групп, для которых можно настроить расписание доступа. По умолчанию таблица содержит элемент **\Everyone** (все пользователи). Вы можете добавлять, изменять и удалять пользователей и группы пользователей.
Правила доступа к устройствам	Таблица содержит расписания доступа для пользователей и групп и состоит из следующих столбцов: • **Расписание доступа** – названия существующих расписаний доступа. Флажок рядом с расписанием показывает, используется ли это расписание в работе компонента. • **Доступ** – тип доступа для расписания: **Разрешать** (предоставить доступ к устройствам выбранного типа) или **Блокировать** (запретить доступ к устройствам выбранного типа). Расписания можно настраивать только для жестких дисков, съемных дисков, дискет и CD/DVD-приводов. По умолчанию таблица содержит расписание доступа **По умолчанию**, которое обеспечивает полный доступ к устройствам для всех пользователей (выбран элемент **\Everyone** в списке **Пользователи и/или группы пользователей**) в любое время, если для этого типа устройства разрешен доступ по шине подключения. Вы можете добавлять, изменять и удалять расписания доступа для выбранных пользователей. Расписание **По умолчанию** невозможно изменить или удалить.

Окно Пользователь или группа

В этом окне вы можете указать пользователя или группу пользователей, на которых распространяется правило доступа к устройствам.

Настройка правила доступа к устройствам

Параметр	Описание
Тип	**Пользователь** или **Группа**, на которых распространяется правило.
Имя пользователя или группы	Имя локального 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 16.2 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.		

Параметр	Описание	Значения
`HardDrive`	Режим доступа к жестким дискам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к жестким дискам. `DependsOnBus` (значение по умолчанию) – доступ к жесткому диску зависит от режима доступа для шины подключения, по которой подключен диск. `Block` – пользователям запрещен доступ ко всем жестким дискам (за исключением системных жестких дисков, которые Контроль устройств не блокирует). `ByRule` – доступ к жестким дискам зависит от правил доступа. `ReadOnly` – пользователям разрешен доступ к жестким дискам только на чтение, запись запрещена.
`RemovableDrive`	Режим доступа к съемным дискам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к съемным дискам. `DependsOnBus` (значение по умолчанию) – доступ к съемному диску зависит от режима доступа для шины подключения, по которой подключен диск. `Block` – пользователям запрещен доступ к съемным дискам. `ByRule` – доступ к съемным дискам зависит от правил доступа. `ReadOnly` – пользователям разрешен доступ к съемным дискам только на чтение, запись запрещена.
`FloppyDrive`	Режим доступа к дискетам, подключенным к клиентскому устройству. Приложение не блокирует дискеты, подключенные к клиентскому устройству с помощью шины ISA.	`Allow` – пользователям разрешен доступ к дискетам. `DependsOnBus` (значение по умолчанию) – доступ к дискете зависит от режима доступа для шины подключения, по которой подключена дискета. `Block` – пользователям запрещен доступ к дискетам. `ByRule` – доступ к дискетам зависит от правил доступа. `ReadOnly` – пользователям разрешен доступ к дискетам только на чтение, запись запрещена.
`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.

Параметр	Описание	Значения
`Printer`	Режим доступа к принтерам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к принтерам. `DependsOnBus` (значение по умолчанию) – доступ к принтеру зависит от режима доступа для шины подключения, по которой подключен принтер. `Block` – пользователям запрещен доступ к принтерам.
`Modem`	Режим доступа к модемам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к модемам. `DependsOnBus` (значение по умолчанию) – доступ к модему зависит от режима доступа для шины подключения, по которой подключен модем. `Block` – пользователям запрещен доступ к модемам.
`TapeDrive`	Режим доступа к стримерам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к стримерам. `DependsOnBus` (значение по умолчанию) – доступ к стримеру зависит от режима доступа для шины подключения, по которой подключен стример. `Block` – пользователям запрещен доступ к стримерам.
`MultifuncDevice`	Режим доступа к мультифункциональным устройствам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к мультифункциональным устройствам. `DependsOnBus` (значение по умолчанию) – доступ к мультифункциональному устройству зависит от режима доступа для шины подключения, по которой подключено устройство. `Block` – пользователям запрещен доступ к мультифункциональным устройствам.
`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.

Параметр	Описание	Значения
`BluetoothDevice`	Режим доступа к Bluetooth-устройствам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к Bluetooth-устройствам. `DependsOnBus` (значение по умолчанию) – доступ к Bluetooth-устройству зависит от режима доступа для шины подключения, по которой подключено устройство. `Block` – пользователям запрещен доступ к Bluetooth-устройствам.
`ImagingDevice`	Режим доступа к устройствам обработки изображений, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к устройствам обработки изображений. `DependsOnBus` (значение по умолчанию) – доступ к устройству обработки изображений зависит от режима доступа для шины подключения, по которой подключено устройство. `Block` – пользователям запрещен доступ к устройствам обработки изображений.
`SoundAdapter`	Режим доступа к звуковым адаптерам, подключенным к клиентскому устройству.	`Allow` – пользователям разрешен доступ к звуковым адаптерам. `DependsOnBus` (значение по умолчанию) – доступ к звуковому адаптеру зависит от режима доступа для шины подключения, по которой подключено устройство. `Block` – пользователям запрещен доступ к звуковым адаптерам.
`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:

```
kess-control --get-device-list [--all] [--json]
```

где:

- `--all` – выводить список всех подключенных устройств.
- `--json` – выводить список подключенных устройств в формате JSON.

Приложение Kaspersky Embedded Systems 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:

```
kess-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:

```
kess-control --trusted-devices --list
```

Чтобы добавить устройство в список доверенных устройств, выполните следующую команду:

```
kess-control --trusted-devices --add <идентификатор>
```

где `<идентификатор>` – идентификатор устройства или маска идентификатора устройства.

Чтобы удалить устройство из списка доверенных устройств, выполните следующую команду:

```
kess-control --trusted-devices --delete <идентификатор>
```

где `<идентификатор>` – идентификатор устройства или маска идентификатора устройства.

Чтобы импортировать список доверенных устройств из файла, выполните следующую команду:

```
kess-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 16.2 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 16.2 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 `kess-control --request-temporary-device-access`.

Чтобы запросить временный доступ к заблокированному устройству, выполните следующую команду:

```
kess-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 `kess-control --upload-temporary-device-access-key`, чтобы получить временный доступ к устройству.

Чтобы получить временный доступ к заблокированному устройству, выполните следующую команду:

```
kess-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.

Контроль целостности системы

Приложение Kaspersky Embedded Systems 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 Embedded Systems 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/kess/).

  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**).

Параметры компонента Контроль целостности системы

Параметр	Описание
Области мониторинга	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	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	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.

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**.
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/kess/).

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 Embedded Systems 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.

Параметр	Описание
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/kess.
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 Embedded Systems 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 Embedded Systems 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/kess/
`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.

Параметр	Описание	Значения
`UseScanArea`	Исключение указанной области из мониторинга.	`Yes` (значение по умолчанию) – исключать указанную область из мониторинга. `No` – не исключать указанную область из мониторинга.
`Path`	Путь к директории с объектами, исключаемыми из мониторинга.	Для указания пути вы можете использовать **маски**. 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 Embedded Systems 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/kess/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.

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	Таблица, содержащая области мониторинга, проверяемые задачей. По умолчанию таблица содержит область мониторинга **Внутренние объекты "Лаборатории Касперского"** (/opt/kaspersky/kess/). 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 Embedded Systems 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/kess/).

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 Embedded Systems 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/kess.
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 Embedded Systems 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 Embedded Systems 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/kess/
`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 Embedded Systems Security может завершать процесс приложения, осуществляющего вредоносную активность.

Компонент Анализ поведения включается автоматически с параметрами по умолчанию при запуске приложения Kaspersky Embedded Systems 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 Embedded Systems 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 компонентом MDR.

  Приложение автоматически исключает из проверки активность процесса Watchdog-сервера. Это исключение удалить нельзя.

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**).

Параметры компонента Анализ поведения

Параметр	Описание
Доверенные приложения	*Список доверенных приложений* – это список приложений, у которых Kaspersky Embedded Systems Security не контролирует файловую и сетевую активности (в том числе и вредоносную). По умолчанию Kaspersky Embedded Systems 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 Embedded Systems Security перестает контролировать активность приложения.
Добавить приложение	Вы можете добавить приложение в список доверенных приложений по пути или маске пути к приложению. Дополнительно вы можете исключить из проверки активность дочерних приложений, а также исключить приложение из проверки при работе компонента Managed Detection and Response.
Действие при обнаружении угрозы	**Информировать**. Если выбрано это действие, то при обнаружении вредоносной активности приложение Kaspersky Embedded Systems Security не завершает процесс, осуществляющий вредоносную активность, а только записывает событие об обнаружении вредоносной активности в журнал событий. **Блокировать** Если выбрано это действие, то при обнаружении вредоносной активности приложение Kaspersky Embedded Systems Security завершает процесс, осуществляющий вредоносную активность, и записывает в журнал событий информацию об обнаруженной вредоносной активности.

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 Embedded Systems Security будет выполнять при обнаружении вредоносной активности в операционной системе: • **Блокировать** приложение, осуществляющее вредоносную активность (значение по умолчанию). Kaspersky Embedded Systems Security завершает процесс, осуществляющий вредоносную активность, и записывает в журнал событий информацию об обнаруженной вредоносной активности. • **Информировать** пользователя. Kaspersky Embedded Systems 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

Таблица содержит области исключения по процессам. Область исключения по процессам позволяет настроить исключение активности указанного процесса из проверки. По умолчанию таблица пуста.

Параметры области исключения по процессам

Параметр	Описание
Название области исключения	Название области исключения.
Путь	Полный путь к исключаемому процессу.
Статус	Статус показывает, используется ли это исключение в работе приложения.

Элементы в таблице можно добавлять, изменять и удалять.

Вы также можете импортировать список исключений из файла по кнопке **Дополнительно → Импортировать** и экспортировать список добавленных исключений в файл по кнопке **Дополнительно → Экспортировать выбранное** или **Дополнительно → Экспортировать все**. При импорте вам будет предложено заменить список исключений или добавить исключения к уже существующему списку.

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	Флажок включает или выключает исключение процесса из телеметрии, которую собирает компонент MDR. 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.

Параметры 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 Embedded Systems 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.	

Параметр	Описание	Значения
`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.
`UseTrustedProgramForMDR`	Исключение активности процесса из телеметрии, которую собирает компонент MDR.	`Yes` – исключать активность указанного процесса из телеметрии, которую собирает компонент MDR. `No` (значение по умолчанию) – не исключать активность указанного процесса из телеметрии компонента MDR.
`TelemetrySource`	Дополнительный параметр сбора телеметрии, отправляемой решению Managed Detection and Response при интеграции с ним.	`Default` (значение по умолчанию) – использовать для сбора телеметрии технологию eBPF и службу auditd. `OnlyEBPF` – использовать для сбора телеметрии только технологию eBPF.
`UseTelemetryMonopolyMode`	Дополнительный параметр сбора телеметрии, отправляемой решению Managed Detection and Response при интеграции с ним. Параметр `UseTelemetryMonopolyMode` применяется, только если для параметра `TelemetrySource` установлено значение `Default`.	`True` (значение по умолчанию) – приложение Kaspersky Embedded Systems Security использует службу auditd в монопольном режиме. `False` – служба auditd используется в режиме многоадресной рассылки.

Использование Kaspersky Security Network

Функциональность KSN может быть недоступна в приложении на территории США.

Для повышения эффективности защиты устройств и данных пользователей приложение Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security не отправляет анонимную статистику и данные о типах и источниках угроз.

Вы можете в любой момент выбрать другой вариант использования Kaspersky Security Network.

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 веб-сайте "Лаборатории Касперского". Файл с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения.

Облачный режим работы Kaspersky Embedded Systems Security

Облачный режим – это режим работы приложения Kaspersky Embedded Systems 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 вы используете KSN в работе приложения, вы можете включать облачный режим работы приложения.

Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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.

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.

Настройка параметров прокси-сервера KSN с помощью командной строки 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)**.

Параметры использования Kaspersky Security Network

Параметр	Описание
Использование Kaspersky Security Network включено / выключено	Если флажок установлен, вы принимаете условия использования Kaspersky Security Network. Вы сможете получать информацию из базы знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Если флажок снят, вы отказываетесь от использования Kaspersky Security Network.
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.
Использовать расширенный режим KSN	Если флажок установлен, 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. Флажок недоступен, если вы используете инфраструктурное решение *Kaspersky Private Security Network (KPSN)*.

Параметр	Описание
Использовать облачный режим	Если флажок установлен, то Kaspersky Embedded Systems Security использует облегченную версию баз приложения, за счет чего снижается нагрузка на ресурсы операционной системы. Kaspersky Embedded Systems Security загружает облегченную версию баз приложения в ходе ближайшего обновления после того, как флажок был установлен. Если флажок снят, то Kaspersky Embedded Systems Security использует полную версию баз приложения. Kaspersky Embedded Systems Security загружает полную версию баз приложения в ходе ближайшего обновления после того, как флажок был снят. 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.
Использовать Сервер администрирования как прокси-сервер KSN	Если флажок установлен, приложение Kaspersky Embedded Systems Security взаимодействует с серверами KSN с помощью службы прокси-сервера KSN на Сервере администрирования. Вы можете настроить параметры службы прокси-сервера KSN в свойствах Сервера администрирования.
Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен	Если флажок установлен, приложение Kaspersky Embedded Systems Security взаимодействует с серверами KSN напрямую, когда служба прокси-сервера KSN недоступна. Флажок доступен, если установлен флажок **Использовать Сервер администрирования как прокси-сервер KSN**.

Настройка использования Kaspersky Security Network в Консоли администрирования

В Консоли администрирования вы можете настраивать использование Kaspersky Security Network в работе приложения Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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	Описание
Использовать Сервер администрирования как прокси-сервер KSN	Если флажок установлен, приложение Kaspersky Embedded Systems Security взаимодействует с серверами KSN с помощью службы прокси-сервера KSN на Сервере администрирования. По умолчанию флажок установлен.
Использовать серверы KSN, если прокси-сервер KSN недоступен	Если флажок установлен, приложение Kaspersky Embedded Systems 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**.

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:

```
kess-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/kess/doc/.

Чтобы выключить использование Kaspersky Security Network с помощью ключей командной строки, выполните следующую команду:

```
kess-control --set-app-settings UseKSN=No
```

Чтобы включить или выключить использование Kaspersky Security Network с помощью конфигурационного файла, выполните следующую команду:

```
kess-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 Embedded Systems 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 Embedded Systems 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:

```
kess-control --app-info
```

В строке **Использование Kaspersky Security Network** отображается статус подключения к Kaspersky Security Network:

- Если отображается статус `Расширенный режим KSN`, приложение Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security, при котором используется облегченная версия баз вредоносного ПО.

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 и задач Поиск вредоносного ПО, Проверка важных областей 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.
- Включение и выключение проверки пространств имен.
- Отмена запуска запланированных задач на устройстве, работающем от аккумулятора.
- 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 Embedded Systems Security может использовать прокси-сервер для подключения к серверам активации "Лаборатории Касперского", к источникам обновлений баз и модулей приложения, к Kaspersky Security Network, а также 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 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** и **Параметры приложения → Общие настройки → Интеграция с KSC**).

Параметры прокси-сервера в разделе Настройки сети

Параметр	Описание
Прокси-сервер	Параметры прокси-сервера для доступа пользователей клиентских устройств в интернет. Приложение Kaspersky Embedded Systems Security использует эти параметры в работе некоторых компонентов защиты, в том числе для обновления баз и модулей приложения.
Использование прокси-сервера включено / выключено	Переключатель включает или выключает использование прокси-сервера в работе приложения.
Адрес прокси-сервера	Поле для ввода IP-адреса или доменного имени прокси-сервера.
Порт прокси-сервера	Поле для ввода порта прокси-сервера. Значение по умолчанию: 3128.
Использовать аутентификацию на прокси-сервере	Если флажок установлен, приложение использует аутентификацию с помощью имени пользователя и пароля при соединении с прокси-сервером. 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 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.
Исключения для прокси-сервера	Блок параметров содержит кнопку **Настройки**, по нажатию на которую открывается окно **Исключения для прокси-сервера**, в котором вы можете выключить использование прокси-сервера для подключения к указанным адресам. 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 `?`).

Параметры прокси-сервера в разделе Интеграция с KSC

Параметр	Описание
Использовать Kaspersky Security Center в качестве прокси-сервера для активации	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.

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**.
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.
Исключения для прокси-сервера	Блок параметров содержит кнопку **Настроить**, по нажатию на которую открывается окно **Исключения для прокси-сервера**, в котором вы можете указать список адресов, для подключения к которым не будет использоваться прокси-сервер. В качестве адреса вам нужно указать IP-адрес или DNS-имя, для подключения к которому не будет использоваться прокси-сервер. Для указания адреса вы можете использовать маски (символы * и ?).

Настройка параметров прокси-сервера в командной строке

В командной строке вы можете включать и выключать использование прокси-сервера компонентами приложения с помощью параметров `UseProxy`, `ProxyServer` и `ProxyBypass` 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 также 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 \).

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 и Проверка важных областей. Исключение точек монтирования позволяет исключать из перехвата файловых операций локальные или удаленные директории, смонтированные на устройстве. Кроме того, глобальные исключения влияют на работу 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** → **Доверенные точки монтирования**).

Список доверенных точек монтирования. Они исключаются из перехвата файловых операций для компонентов Защита от файловых угроз и Защита от шифрования, а также из проверки задачами Поиск вредоносного ПО и Проверка важных областей.

Точки монтирования требуется указывать точно так же, как они отображаются в выводе команды mount.

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**).

По ссылке **Настроить исключение памяти процессов из проверки** в блоке **Дополнительные настройки** открывается окно, в котором вы можете сформировать список исключений. Укажите путь к процессам, которые приложение исключит 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.

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. Элементы в списке можно добавлять, изменять и удалять.

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 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**, 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 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.

Обнаружение 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 обнаружение легальных приложений, которые злоумышленники могут использовать для нанесения вреда устройствам или данным, в свойствах политики (**Параметры приложения** → **Общие настройки** → **Настройки обнаружения**, блок **Обнаружение других типов объектов**).

Флажок **Легальные приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя** включает или выключает обнаружение легальных приложений, через которые злоумышленники могут навредить устройству или данным пользователя. По умолчанию флажок снят.

В разделе **Настройки обнаружения** в Web Console вы также можете настроить режим перехвата файловых операций.

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать 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 настраивать 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 Embedded Systems 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**, блок **Дополнительные настройки**).

Флажок **Включить мониторинг стабильности работы приложения** включает или выключает отслеживание состояния работы приложения Kaspersky Embedded Systems 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 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 Embedded Systems 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 Embedded Systems Security с помощью параметров `TrackProductCrashes`, `ProductHealthLogFile`, `WarnThreshold`, `WarnAfter_#_crash` и `WarnRemovingThreshold` в конфигурационном файле kess.ini.

Параметр `TrackProductCrashes` позволяет включить отправку статуса устройства от приложения Kaspersky Embedded Systems Security в Kaspersky Security Center при нестабильной работе приложения. Параметр может принимать следующие значения:

- `Yes/true` – включить отправку статуса устройства от приложения Kaspersky Embedded Systems Security в Kaspersky Security Center.
- `No/false` – выключить отправку статуса устройства от приложения Kaspersky Embedded Systems 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/kess/private/kess_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**, блок **Настройки запуска приложения**).

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 kess будет перезапущен. Значение по умолчанию: 3.

В разделе **Взаимодействие с пользователем** в Web Console вы также можете настроить разрешение на просмотр и управление задачами.

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 kess 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 kess.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 kess 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**, блок **Дополнительные настройки**).

В блоке **Дополнительные настройки** по ссылке **Дополнительные настройки** открывается окно, в котором вы можете настроить ограничение на использование резидентной памяти (см. таблицу ниже).

Параметры

Параметр	Описание
Ограничить использование памяти приложением	Флажок включает ограничение на использование резидентной памяти приложнием. По умолчанию флажок установлен.
Метод расчета ограничения	В раскрывающемся списке вы можете выбрать метод ограничения на использование резидентной памяти: • **Без ограничений**. При выборе этого элемента списка использование резидентной памяти не ограничивается. • **Задать точное значение (%)**. При выборе этого элемента списка становится доступно поле **Точное значение (%)**, в котором вы можете указать нужное значение в процентах. • **Задать точное значение (МБ)**. При выборе этого элемента списка становится доступно поле **Точное значение (МБ)**, в котором вы можете указать нужное значение в мегабайтах. • **Использовать меньшее из двух значений (% или МБ)**. При выборе этого элемента списка становятся доступны поля **Точное значение (%)** и **Точное значение (МБ)**, в которых вы можете указать нужные значения. • **Использовать большее из двух значений (% или МБ)**. При выборе этого элемента списка становятся доступны поля **Точное значение (%)** и **Точное значение (МБ)**, в которых вы можете указать нужные значения. • **Ограничивать автоматически (рекомендуется)**. При выборе этого элемента списка использование резидентной памяти ограничивается автоматически (значение по умолчанию).

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).

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 kess.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. Потребление ресурсов устройства при проверке приложением Kaspersky Embedded Systems Security может увеличить нагрузку на центральный процессор. Это может замедлить работу других приложений. Для оптимизации производительности приложения вы можете ограничить использование ресурсов процессора. 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* и *Инвентаризация*, 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**.

В блоке **Ограничить потребление ресурсов процессора для задач проверки** с помощью переключателя вы можете включить или выключить ограничение на использование ресурсов процессора для задач *Поиск вредоносного ПО*, *Проверка важных областей* и *Инвентаризация*.

Если флажок установлен, максимальная нагрузка на все ядра процессора при работе этих задач не превышает значения, указанного в поле **Максимальное значение (%)**. Значение в поле должно быть целым числом и находиться в пределах от 10 до 100.

В блоке **Дополнительные настройки** в поле ввода **Ограничение на использование памяти для задач проверки (МБ)** вы можете задать ограничение на использование памяти для задач проверки (в мегабайтах). Значение по умолчанию: 8192.

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* и *Инвентаризация*. Если флажок установлен, максимальная нагрузка на все ядра процессора при работе этих задач не превышает значения, указанного в поле справа (в процентах). Значение в поле должно быть целым числом и находиться в пределах от 10 до 100. По умолчанию флажок снят.
Ограничение на использование памяти для задач проверки (МБ)	Поле ввода ограничения на использование памяти для задач проверки (в мегабайтах). Значение по умолчанию: 8192.

Настройка ограничения в командной строке

В командной строке вы можете настраивать ограничение на использование ресурсов процессора для задач типа *ODS* 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* 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* и *InventoryScan*. Значение в поле 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* и *InventoryScan* с помощью параметра `ScanMemoryLimit` в конфигурационном файле kess.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 Embedded Systems Security> → закладка **Параметры приложения** → раздел **Параметры хранилищ**, блок **Параметры передачи данных на Сервер администрирования**).

Параметры передачи данных на Сервер администрирования

Параметр	Описание
Передача данных на Сервер администрирования	Категории событий на клиентских устройствах, информация о которых должна передаваться на Сервер администрирования. Вы можете выключить передачу некоторых данных для оптимизации дискового пространства на Сервере администрирования. Приложение передает следующие категории событий: • **О файлах карантина**. • **О файлах в резервном хранилище**. • **О необработанных файлах**. • **Об установленных устройствах**. • **О запускаемых приложениях**.

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.

Параметр	Описание
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 просмотр локальных задач, созданных в приложении Kaspersky Embedded Systems Security. Если политика Kaspersky Security Center запрещает пользователям просматривать и изменять локальные задачи, информация о задачах Scan_My_Computer, Critical_Areas_Scan, Inventory_Scan, Update и Rollback недоступна.

- разрешение на просмотр на клиентских устройствах задач, созданных 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**, блок **Разрешенные действия**).

Параметры управления задачами

Параметр	Описание
Доступ к локальным задачам	Флажок разрешает или запрещает пользователям просмотр локальных задач, созданных в приложении Kaspersky Embedded Systems 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.
Управление групповыми задачами	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.

В разделе **Взаимодействие с пользователем** в Web Console вы также можете настроить параметры запуска приложения.

Настройка в Консоли администрирования

В Консоли администрирования вы можете настраивать разрешение на просмотр задач 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 Embedded Systems 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 пользователям 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.

Включение и выключение проверки пространств имен

Вы можете включать и выключать использование системного механизма пространств имен. Этот механизм применяется в системах контейнеризации и сессиях с мандатным разграничением доступа в операционных системах Astra Linux.

Настройка проверки пространств имен в Web Console

В Web Console вы можете включать и выключать использование механизма пространств имен в свойствах политики (**Параметры приложения** → **Общие настройки** → **Проверка контейнеров**).

Переключатель **Проверка пространств имен включена / выключена** включает или выключает использование механизма пространств имен в поддерживаемых операционных системах.

По умолчанию переключатель включен.

Настройка проверки пространств имен в Консоли администрирования

В Консоли администрирования вы можете включать и выключать использование механизма пространств имен в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Общие параметры** → **Параметры проверки контейнеров**).

Флажок **Включить проверку пространств имен и контейнеров** включает или выключает использование механизма пространств имен в поддерживаемых операционных системах.

По умолчанию флажок установлен.

Настройка проверки пространств имен в командной строке

В командной строке вы можете включать и выключать использование механизма пространств имен с помощью параметра `NamespaceMonitoring` 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 `NamespaceMonitoring` может принимать следующие значения:

- `Yes` (значение по умолчанию) – включить использование механизма пространств имен.
- `No` – выключить использование механизма пространств имен.

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 Embedded Systems Security отменяет запуск по расписанию следующих задач:

- всех задач проверки (выборочная проверка, проверка важных областей, поиск вредоносного ПО);
- инвентаризации;
- обновления баз и модулей приложения;
- 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**).

Флажок **Откладывать или пропускать задачи по расписанию при работе от аккумулятора** включает или выключает отмену запуска задач, для которых настроено расписание.

Если функция включена, приложение переходит в режим энергосбережения при работе от аккумулятора и отменяет выполнение задач, для которых задан запуск по расписанию.

Если флажок снят, на устройстве запускаются все запланированные по расписанию задачи, независимо от источника питания, к которому подключено устройство (сеть или аккумулятор).

По умолчанию флажок установлен.

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 дополнительных параметров телеметрии

Вы можете настраивать следующие дополнительные параметры сбора телеметрии, отправляемой решению Kaspersky Managed Detection and Response при интеграции с ним:

- Источник телеметрии. Для сбора телеметрии можно использовать технологию eBPF и службу auditd или только технологию eBPF.
- Режим использования службы auditd. Приложение Kaspersky Embedded Systems 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**, блок **Настройки телеметрии**).

Дополнительные параметры сбора телеметрии

Параметр	Описание
Источник телеметрии	Источник, который использует приложение Kaspersky Embedded Systems Security 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.

Параметр	Описание
Режим работы auditd	Режим использования службы auditd: • **Монопольный**. Если выбран этот вариант, приложение Kaspersky Embedded Systems Security использует службу auditd в монопольном режиме. • **Режим многоадресной рассылки**. Если выбран этот вариант, служба auditd используется в режиме многоадресной рассылки. Параметр применяется, только если для параметра **Источник телеметрии** выбран вариант **По умолчанию**.

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 Embedded Systems Security для сбора телеметрии: • **Использовать только eBPF** – использовать для сбора телеметрии только технологию eBPF. • **Использовать eBPF и auditd** (значение по умолчанию) – использовать для сбора телеметрии технологию eBPF и службу auditd.
Использование auditd	Режим использования службы auditd: • **В монопольном режиме** (значение по умолчанию) – приложение Kaspersky Embedded Systems 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 `kess-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 Embedded Systems 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`.

Доверенная зона

Доверенная зона – это сформированный администратором системы список объектов и приложений, которые приложение не проверяет и не контролирует в процессе работы.

Администратор системы формирует доверенную зону самостоятельно в зависимости от особенностей объектов, с которыми требуется работать, а также от приложений, установленных на устройстве. Включение объектов и приложений в доверенную зону может потребоваться, например, если приложение блокирует доступ к какому-либо объекту или приложению, в то время как вы уверены, что этот объект или приложение безвредны.

Вы можете добавить в доверенную зону следующие объекты:

- Исключения из проверки Защитой от файловых угроз.
- Доверенные веб-адреса для Защиты от веб-угроз.
- Доверенные IP-адреса для Защиты от сетевых угроз.
- Сетевые порты, которые будет проверять приложение.
- Доверенные корневые сертификаты.
- Доверенные домены, которые исключаются из проверки приложением.
- Доверенные точки монтирования (глобальные исключения) – точки монтирования, исключенные из перехвата файловых операций для компонентов Защита от файловых угроз, Защита от шифрования и задач Поиск вредоносного ПО, Проверка важных областей и Проверка съемных дисков.
- Исключения из перехвата трафика.
- Исключения процессов из проверки Анализом поведения.
- Доверенные устройства – устройства, полный доступ к которым разрешен в любое время для указанных пользователей.

Резервное хранилище

Если во время проверки защищенного устройства приложение Kaspersky Embedded Systems 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/kess/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 Embedded Systems Security> → закладка **Параметры приложения** → раздел **Параметры хранилищ**).

Параметры резервного хранилища

Параметр	Описание
Удалять объекты через (дни)	Если флажок установлен, то максимальный срок хранения файлов ограничен заданным интервалом времени. По истечении максимального срока хранения приложение удаляет наиболее старые файлы из резервного хранилища. Если флажок снят, период хранения объектов в резервном хранилище не ограничен. Значение по умолчанию: 30.
Ограничить размер резервного хранилища до (МБ)	Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. После достижения максимального размера резервного хранилища приложение автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения. Если флажок снят, размер резервного хранилища не ограничен. Доступные значения: 1–4000. 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: 1–4000. 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 – 4000 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/kess/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:

```
kess-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 отобразит 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:

```
kess-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:

```
kess-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.

Удаление объектов из резервного хранилища

Чтобы удалить выбранные объекты из резервного хранилища, выполните следующую команду:

```
kess-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:

```
kess-control -B --mass-remove --query "ObjectId == '15'"
```

Чтобы удалить объекты, в названии которых или в пути к которым содержится "test":

```
kess-control -B --mass-remove --query "FileName like '%test%'"
```

Чтобы удалить все объекты из резервного хранилища, выполните следующую команду:

```
kess-control -B --mass-remove
```

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 Embedded Systems 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 Embedded Systems 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 путем добавления лицензионного ключа MDR с помощью файла ключа или кода активации.

Лицензию, которая позволяет активировать функциональность Kaspersky Managed Detection and Response, требуется предварительно зарегистрировать на портале MDR.

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 Embedded Systems Security**

   Убедитесь, что включены и работают следующие компоненты приложения Kaspersky Embedded Systems 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**

   Убедитесь, что вы добавили в приложение лицензионный ключ MDR.

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.

О действиях по реагированию

При интеграции с решением Kaspersky Managed Detection and Response приложение Kaspersky Embedded Systems Security может выполнять действия по реагированию, направленные на обеспечение функций безопасности.

Приложение Kaspersky Embedded Systems Security может выполнять следующие действия по реагированию:

- Сетевая изоляция устройства.

  Включение и выключение сетевой изоляции выполняется на стороне решения Kaspersky Managed Detection and Response. Вы можете вручную выключать сетевую изоляцию устройства в командной строке.

- Помещение файла на карантин.

  Действие выполняется с помощью задачи помещения файла на карантин (*Quarantine file*). Задача создается и запускается на стороне решения Kaspersky Managed Detection and Response. Вы также можете вручную помещать файлы на карантин с помощью командной строки.

- Восстановление файла из карантина.

  Действие по реагированию формируется на стороне решения Kaspersky Managed Detection and Response. Вы также можете вручную восстановить файл из карантина с помощью Kaspersky Security Center или командной строки.

- 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. Задача создается и запускается на стороне решения Kaspersky Managed Detection and Response.

- 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. Задача создается и запускается на стороне решения Kaspersky Managed Detection and Response.

- 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. Задача создается и запускается на стороне решения Kaspersky Managed Detection and Response.

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 Embedded Systems 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**).

Для интеграции с Kaspersky Managed Detection and Response должны быть включены компоненты Защита от файловых угроз и Анализ поведения. Рекомендуется также включить компоненты Защита от веб-угроз и Защита от сетевых угроз.

Для активации компонента MDR требуется лицензионный ключ MDR.

Параметры интеграции с MDR

Параметр	Описание
Managed Detection and Response включен / выключен	Переключатель включает или выключает компонент MDR, необходимый для интеграции приложения Kaspersky Embedded Systems Security с решением Kaspersky Managed Detection and Response. По умолчанию компонент выключен. Для активации компонента MDR требуется включить использование Kaspersky Security Network в расширенном режиме.

Настройка интеграции с Kaspersky Managed Detection and Response в Консоли администрирования

В Консоли администрирования вы можете включать и выключать компонент MDR в свойствах политики (Управление политиками в Консоли администрирования, Создание политики с помощью Консоли администрирования) (**Detection and Response → Managed Detection and Response**).

Для активации компонента MDR требуется лицензионный ключ MDR.

Параметры интеграции с MDR

Параметр	Описание
Включить Managed Detection and Response	Флажок включает или выключает компонент MDR, необходимый для интеграции приложения Kaspersky Embedded Systems 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.

Настройка интеграции с Kaspersky Managed Detection and Response в командной строке

В командной строке вы можете:

- Включать и выключать компонент MDR.
- Добавлять и удалять лицензионный ключ для активации компонента MDR (ключ MDR) с помощью команд управления лицензионными ключами.
- Изменять время запуска служебной задачи *Mdr_Autostart_Scan*, которая создается автоматически после интеграции Kaspersky Embedded Systems Security с Managed Detection and Response. задача *Mdr_Autostart_Scan* создается 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.

Настройку интеграции приложения Kaspersky Embedded Systems 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.

Сетевая изоляция устройства

При интеграции с решением Kaspersky Managed 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 Embedded Systems Security.
- Соединений, инициированных Агентом администрирования Kaspersky Security Center.
- Соединений с KSN.

Сетевая изоляция может применяться, только если включена интеграция приложения Kaspersky Embedded Systems Security с решением Kaspersky Managed Detection and Response и активирован компонент MDR.

Включение и выключение сетевой изоляции устройства, а также настройка исключений из сетевой изоляции выполняется на стороне решения Kaspersky Managed Detection and Response. Подробнее см. в справке Kaspersky Managed Detection and Response.

Если требуется, вы можете вручную выключать сетевую изоляцию устройства в командной строке. Выключение сетевой изоляции вручную доступно вне зависимости от того, включена ли интеграция с решением Kaspersky Managed Detection and Response, а также вне зависимости от того, распространяется ли на устройство действие политики. Вы можете проверять статус сетевой изоляции устройства в командной строке.

Ограничения сетевой изоляции

При использовании сетевой изоляции настоятельно рекомендуется ознакомиться с описанными ограничениями.

Для работоспособности сетевой изоляции требуется, чтобы приложение Kaspersky Embedded Systems Security было запущено. Во время сбоя в работе приложения Kaspersky Embedded Systems Security (когда приложение не запущено), блокировка трафика при включении сетевой изоляции решением Kaspersky Managed 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 Embedded Systems Security не сможет получить к нему доступ.

Прокси-сервер не добавляется автоматически в исключения из сетевой изоляции, поэтому требуется добавить его в исключения вручную, чтобы приложение Kaspersky Embedded Systems 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.

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.

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 решением Kaspersky Managed Detection and Response для выполнения рекомендуемых действий по реагированию на угрозы. 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/kess/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.
- 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 Embedded Systems Security.

Помещение файла на карантин возможно, только если включена интеграция приложения Kaspersky Embedded Systems Security с Kaspersky Managed Detection and Response и активирован компонент MDR.

Директория для хранения объектов карантина должна быть доступна для записи.

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.

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 и удаление из карантина доступно вне зависимости от того, включена ли интеграция с Kaspersky Managed 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/kess/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.

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 Embedded Systems Security> → закладка **Параметры приложения** → раздел **Параметры хранилищ**).

Параметры карантина

Параметр	Описание
Максимальный размер карантина (МБ)	Если флажок установлен, то максимальный размер карантина ограничен заданным значением (в мегабайтах). Если флажок снят, размер карантина не ограничен. Доступные значения: 1–4000. Значение по умолчанию: 200.
Уведомлять при заполнении карантина на (%)	Если флажок установлен, то при заполнении карантина до указанного значения в (процентах) 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: 1–4000. Значение по умолчанию: 200.

Параметр	Описание
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.
`QuarantineSizeLimit`	Максимальный размер карантина (в мегабайтах). При достижении максимального размера карантина приложение удаляет самые старые файлы. Чтобы снять ограничение на размер карантина, укажите значение 0.	0 – 4000 0 – размер карантина не ограничен. Значение по умолчанию: 200.
`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/kess/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.
- 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:

```
kess-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.

Просмотр информации о файлах на карантине

Чтобы просмотреть информацию о файлах карантина, выполните следующую команду:

```
kess-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:

```
kess-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:

```
kess-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:

```
kess-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":

```
kess-control -Q --mass-remove --query "FileName like '%test%'"
```

Чтобы удалить все файлы из карантина, выполните следующую команду:

```
kess-control -Q --mass-remove
```

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 Embedded Systems 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/kess/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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 и идентификаторы устройств;
- веб-адреса репозиториев;
- имена файлов, пути к файлам и хеш-суммы исполняемых файлов приложений;
- 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 `kess-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 `kess-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 Embedded Systems 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 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/kess/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 Embedded Systems Security отображается в Web Console и в Консоли администрирования.

События, возникающие в работе приложения Kaspersky Embedded Systems 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:

```
kess-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:

```
kess-control --start-task <идентификатор/имя задачи> -W
```

Пример:
Включить вывод текущих событий запущенной задачи с ID=1:

```
kess-control --start-task 1 -W
```

Чтобы вывести в консоль информацию о текущих событиях, соответствующих условиям фильтра, выполните следующую команду:

```
kess-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:

```
kess-control -W --query "EventType == 'TaskStateChanged'"
```

Вывести события TaskSettingsChanged, инициированных пользователем User:

```
kess-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:

```
kess-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/kess/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 `kess-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:

```
kess-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:

```
kess-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

С помощью графического пользовательского интерфейса приложения Kaspersky Embedded Systems 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 сетевых угроз.
  - Контроль устройств.
  - Защита от атак BadUSB.
  - Анализ поведения.
  - Контроль приложений.
  - Контроль целостности системы.
- Запускать и останавливать задачи проверки:
  - Поиск вредоносного ПО.
  - Проверка важных областей.
- Запускать выборочную проверку файлов и директорий.
- Запускать и останавливать задачи обновления и отката обновления баз.
- 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 компонент и/или задача приложения работает в информирующем режиме, в графическом интерфейсе приложения для компонента и/или задачи отображается предупреждение *Выбран информирующий режим работы*.

Графический пользовательский интерфейс

Значок приложения в области уведомлений

Значок приложения Kaspersky Embedded Systems 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 Embedded Systems Security 4.0 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* и *Проверка важных областей*. 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 приложения 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

С помощью графического пользовательского интерфейса вы можете запускать выборочную проверку файлов и директорий.

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 Embedded Systems Security 4.0 для Linux** в качестве приложения для проверки файла или директории.

   В зависимости от среды рабочего стола названия элементов контекстного меню могут отличаться.

Задача выборочной проверки и ход ее выполнения отобразятся в графическом пользовательском интерфейсе.

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

С помощью графического пользовательского интерфейса вы можете просматривать отчеты приложения. В отчеты записывается информация о работе компонентов и задач приложения. 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 сетевых угроз.
  - Защита от атак BadUSB.
  - Управление сетевым экраном.
  - Анализ поведения.
  - Контроль приложений.
  - Контроль устройств.
  - Контроль целостности системы.
- **Задачи по требованию**. Этот отчет содержит информацию о событиях, зарегистрированных в журнале во время выполнения задач проверки, задач обновления и задач проверки целостности системы.

Чтобы просмотреть отчет:

1. Откройте главное окно 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 пользовательского 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.

Вы можете активировать приложение, добавив активный лицензионный ключ.

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

Для активации приложения Kaspersky Embedded Systems Security на защищенном устройстве требуется добавить лицензионный ключ в приложение. Также для приложения Kaspersky Embedded Systems Security предусмотрен отдельный лицензионный ключ для активации интеграции с Kaspersky Managed Detection and Response – ключ 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 MDR. Процедуры добавления резервного основного ключа и ключа MDR не отличаются.

Чтобы добавить в приложение резервный основной ключ или ключ MDR:

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 ключ MDR, то он добавляется как активный, если ранее в приложение не был добавлен ключ MDR. Новый ключ MDR добавляется как резервный, если в приложение уже добавлен ключ MDR.

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/kess/.

Проверка целостности компонентов приложения

Приложение Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security;
- MMC-плагин управления Kaspersky Embedded Systems 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:

- Для проверки пакета приложения, пакета графического пользовательского интерфейса и Агента администрирования: /opt/kaspersky/kess/bin/integrity_checker.
- Для проверки MMC-плагина управления Kaspersky Embedded Systems Security:
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kess_<номер версии>.plg\integrity_checker.exe – для 32-битных операционных систем;
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kess_<номер версии>.plg\integrity_checker.exe – для 64-битных операционных систем.

- Для проверки веб-плагина управления Kaspersky Embedded Systems Security:
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\integrity_checker.exe – на устройствах с операционными системами Windows;
  - /var/opt/kaspersky/ksc-web-console/integrity_checker – на устройствах с операционными системами Linux.

Файлы манифеста расположены по следующим путям:

- Для проверки целостности пакета приложения: /opt/kaspersky/kess/bin/integrity_check.xml.
- Для проверки целостности пакета графического пользовательского интерфейса – /opt/kaspersky/kess/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 Embedded Systems Security:
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kess_<версия плагина>.plg\integrity_check.xml – для 32-битных операционных систем;
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kess_<версия плагина>.plg\integrity_check.xml – для 64-битных операционных систем.
- Для проверки веб-плагина управления Kaspersky Embedded Systems Security:
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\server\plugins\kess_<номер версии>\integrity_check.xml – на устройствах с операционными системами Windows;
  - /var/opt/kaspersky/ksc-web-console/server/plugins/kess_<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 и пакета графического пользовательского интерфейса:

  ```
  integrity_checker [<путь к файлу манифеста>] --signature-type kds-with-filename
  ```

- для проверки целостности MMC-плагина управления Kaspersky Embedded Systems Security:

  ```
  integrity_checker.exe [<путь к файлу манифеста>]
  ```

- для проверки целостности веб-плагина управления Kaspersky Embedded Systems Security и Агента администрирования на устройствах с операционными системами Linux:

  ```
  integrity_checker [<путь к файлу манифеста>]
  ```

- для проверки целостности веб-плагинов управления Kaspersky Embedded Systems Security на устройствах с операционными системами Windows:

  ```
  integrity_checker.exe [<путь к файлу манифеста>]
  ```

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).
- `--version` – отобразить версию утилиты.
- `--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-with-filename` – тип проверяемой сигнатуры (этот параметр является обязательным для проверки пакета приложения, пакета графического пользовательского интерфейса и Агента администрирования).
- `--single-file <файл>` – проверить только один файл, входящий в состав манифеста, остальные объекты манифеста игнорировать.

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 Embedded Systems 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 Embedded Systems Security.

Kaspersky предоставляет поддержку Kaspersky Embedded Systems 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 Embedded Systems 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/kess/. 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 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 Embedded Systems Security через Kaspersky Security Center, вы можете настраивать параметры трассировки приложения в параметрах политики Kaspersky Embedded Systems 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**, блок **Настройки файла трассировки**).

Параметры трассировки

Параметр	Описание
Путь к папке трассировки	Поле ввода пути к директории, в которой хранятся файлы трассировки. Значение по умолчанию: /var/log/kaspersky/kess. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, под которой работает Kaspersky Embedded Systems Security. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права.
Максимальное количество файлов трассировки	Поле ввода максимального количества файлов трассировки приложения. Значение по умолчанию: 10.
Максимальный размер файла трассировки (МБ)	Поле ввода максимального размера файла трассировки приложения (в мегабайтах). Значение по умолчанию: 500.

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

Параметр	Описание
Путь к директории с файлами трассировки	Поле ввода пути к директории, в которой хранятся файлы трассировки. Значение по умолчанию: /var/log/kaspersky/kess. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, под которой работает Kaspersky Embedded Systems Security. Для доступа к директории хранения файлов трассировки, заданной по умолчанию, требуются root-права.
Максимальный размер файла трассировки (МБ)	Поле ввода максимального размера файла трассировки приложения (в мегабайтах). Значение по умолчанию: 500.
Максимальное количество файлов трассировки	Поле ввода максимального количества файлов трассировки приложения. Значение по умолчанию: 10.

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/kess. Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись только для учетной записи, под которой работает Kaspersky Embedded Systems 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 Embedded Systems Security вы используете Консоль администрирования, информация о событиях, возникающих во время работы MMC-плагина управления, может записываться в файл трассировки MMC-плагина Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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/kess/common/dumps (файлы дампов процесса kess);
- /var/opt/kaspersky/kess/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 kess. 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 Embedded Systems Security через Kaspersky Security Center, вы можете настраивать параметры записи дампов в параметрах политики Kaspersky Embedded Systems 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 kess.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**, блок **Отладочная информация**).

Параметры записи дампов

Параметр	Описание
Запись дампа включена / выключена	Если запись дампов включена, Kaspersky Embedded Systems Security создает файл дампа при сбое в работе приложения. По умолчанию флажок снят.
Путь к файлу дампа	Поле ввода пути к директории, в которой хранятся файлы дампа. Размер поля ввода ограничен 128 символами. Значение по умолчанию: /var/opt/kaspersky/kess/common/dumps.

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/kess/common/dumps.

Для применения параметров записи дампов требуется перезапустить приложение.

Настройка записи дампов в командной строке

Чтобы настроить запись дампов с помощью конфигурационного файла kess.ini:

1. Остановите Kaspersky Embedded Systems Security.
2. Откройте файл /var/opt/kaspersky/kess/common/kess.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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 приложением

Управление приложением Kaspersky Embedded Systems Security в командной строке выполняется с помощью команд управления Kaspersky Embedded Systems Security.

Вы можете посмотреть справку по командам управления с помощью команды:

```
kess-control --help <префикс группы команд>
```

где <префикс группы команд> может принимать следующие значения:

- -A – команды управления контролем приложений.
- -B – команды управления резервным хранилищем.
- -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.
- -N – команды управления параметрами проверки сетевого трафика.
- -Q – команды управления карантином.
- -R – команды управления сетевой изоляции устройства.
- -S – команды статистики.
- -T – команды управления задачами и параметрами приложения.
- -U – команды управления пользователями и ролями пользователей.
- -W – команды вывода событий (Просмотр событий в командной строке, Просмотр событий в Kaspersky Security Center).

Команды управления параметрами и задачами приложения

-T – префикс, указывающий, что команда принадлежит к группе команд управления параметрами и задачами приложения.

Команда kess-control --export-settings

Команда позволяет вывести в консоль или экспортировать в конфигурационный файл все параметры приложения (включая параметры проверки защищенных соединений, общие параметры приложения и параметры задач).

Синтаксис команды

```
kess-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 kess-control --import-settings

Команда позволяет импортировать из конфигурационного файла все параметры приложения (включая параметры проверки защищенных соединений, общие параметры приложения и параметры задач).

Синтаксис команды

```
kess-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 kess-control --update-application

Команда позволяет установить загруженное обновление модулей приложения.

Синтаксис команды

```
kess-control [-T] --update-application
```

Команды управления общими параметрами приложения

Команда kess-control --get-app-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения общих параметров приложения.

Синтаксис команды

```
kess-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 kess-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:

```
kess-control [-T] --set-app-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kess-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 kess-control --get-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения параметров указанной задачи.

Синтаксис команды

```
kess-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 kess-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:

```
kess-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:

```
kess-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 kess-control --set-to-default

Команда позволяет восстановить значения по умолчанию для параметров указанной задачи.

Синтаксис команды

```
kess-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 kess-control --get-schedule

Команда позволяет вывести в консоль или в конфигурационный файл текущее расписание запуска указанной задачи.

Синтаксис команды

```
kess-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 kess-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:

```
kess-control [-T] --set-schedule <идентификатор/имя задачи> <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kess-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 kess-control --get-task-list

Команда позволяет вывести список существующих задач приложения.

Синтаксис команды

```
kess-control [-T] --get-task-list [--json]
```

Аргументы и ключи

`--json` – выводить параметры в формате JSON.

Команда kess-control --get-task-state

Команда позволяет вывести состояние указанной задачи.

Синтаксис команды

```
kess-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 kess-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:

```
kess-control [-T] --create-task <имя задачи> --type <тип задачи>
```

Создать задачу с параметрами из конфигурационного файла:

```
kess-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 kess-control --delete-task

Команда позволяет удалить задачу.

Синтаксис команды

```
kess-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 kess-control --start-task

Команда позволяет запустить задачу.

Синтаксис команды

```
kess-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 kess-control --stop-task

Команда позволяет остановить задачу.

Синтаксис команды

```
kess-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 kess-control --suspend-task

Команда позволяет приостановить задачу.

Синтаксис команды

```
kess-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 kess-control --resume-task

Команда позволяет возобновить выполнение задачи.

Синтаксис команды

```
kess-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 kess-control --scan-file

Команда позволяет создать и запустить задачу выборочной проверки.

Синтаксис команды

```
kess-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.

Команды управления параметрами проверки сетевого трафика

-N – префикс, указывающий, что команда принадлежит к группе команд управления параметрами проверки сетевого трафика.

Команда kess-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

```
kess-control -N --query user

kess-control -N --query auto

kess-control -N --query kl
```

Команда kess-control --clear-web-auto-excluded

Команда позволяет очистить список доменов, которые приложение автоматически исключило из проверки.

Синтаксис команды

```
kess-control -N --clear-web-auto-excluded
```

Команда kess-control --get-net-settings

Команда позволяет вывести в консоль или в конфигурационный файл текущие значения параметров проверки сетевого трафика.

Синтаксис команды

```
kess-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 kess-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:

```
kess-control [-N] --set-net-settings <имя параметра>=<значение параметра> [<имя параметра>=<значение параметра>]
```

Задать параметры с помощью конфигурационного файла:

```
kess-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 kess-control --list-certificates

Команда позволяет вывести список доверенных корневых сертификатов.

Синтаксис команды

```
kess-control [-N] --list-certificates
```

Команда kess-control --add-certificate

Команда позволяет добавить сертификат в список доверенных корневых сертификатов.

Синтаксис команды

```
kess-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 kess-control --remove-certificate

Команда позволяет удалить сертификат из списка доверенных корневых сертификатов.

Синтаксис команды

```
kess-control [-N] --remove-certificate <субъект сертификата>
```

Команда kess-control --add-bypass-endpoints

Команда позволяет добавить исключение из перехвата трафика.

Синтаксис команды

```
kess-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 kess-control --list-bypass-endpoints

Команда позволяет просмотреть список настроенных исключений из перехвата трафика.

Синтаксис команды

```
kess-control [-N] --list-bypass-endpoints
```

Команда kess-control --remove-bypass-endpoints

Команда позволяет удалить исключение из перехвата трафика.

Синтаксис команды

```
kess-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 kess-control --app-info

Команда позволяет вывести информацию о приложении.

Синтаксис команды

```
kess-control [-S] --app-info [--json]
```

Аргументы и ключи

--json – выводить параметры в формате JSON.

Команда kess-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

```
kess-control [-S] --supported-tech-info [--json]
```

Аргументы и ключи

`--json` – выводить функции в формате JSON.

Команда kess-control --get-statistic

Команда позволяет вывести статистику о работе приложения и список точек монтирования, обнаруженных на устройстве.

Синтаксис команды

```
kess-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 Embedded Systems 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 Embedded Systems 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.

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 kess-control --omsinfo

Команда позволяет создать файл формата JSON для интеграции с Microsoft Operations Management Suite.

Синтаксис команды

```
kess-control [-S] --omsinfo --file <путь к файлу>
```

Команды вывода событий

Команда kess-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

```
kess-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 kess-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

```
kess-control -E
```

Команда kess-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

```
kess-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/kess/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.

Команда kess-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 MDR. Указывать тип ключа в команде не требуется.

Синтаксис команды

```
kess-control [-L] --add-active-key < путь к файлу ключа >
```

```
kess-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:

```
kess-control --add-active-key /home/test/00000001.key
```

Команда kess-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 MDR. Указывать тип ключа в команде не требуется.

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

Синтаксис команды

```
kess-control [-L] --add-reserve-key <путь к файлу ключа>

kess-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:

```
kess-control --add-reserve-key /home/test/00000002.key
```

Команда kess-control --remove-active-key

Команда позволяет удалить активный лицензионный ключ.

Синтаксис команды

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

Аргументы и ключи

`--mdr` – удалить активный лицензионный ключ MDR. Если вы не укажете ключ `--mdr`, будет удален основной активный ключ.

Команда kess-control --remove-reserve-key

Команда позволяет удалить резервный лицензионный ключ.

Синтаксис команды

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

Аргументы и ключи

`--mdr` – удалить резервный лицензионный ключ MDR. Если вы не укажете ключ `--mdr`, будет удален основной резервный ключ.

Команда kess-control -L --query

Команда `-L --query` позволяет вывести информацию о лицензии, по которой активировано приложение, и об используемых лицензионных ключах.

Синтаксис команды

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

Аргументы и ключи

`--json` – выводить данные в формате JSON.

Команды управления сетевым экраном

-F – префикс, указывающий, что команда принадлежит к группе команд управления сетевым экраном.

Команда kess-control --add-rule

Команда позволяет добавить новое сетевое пакетное правило.

Синтаксис команды

```
kess-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 Embedded Systems 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 kess-control --del-rule

Команда позволяет удалить сетевое пакетное правило с указанным названием или с указанным индексом в списке правил.

Синтаксис команды

```
kess-control [-F] --del-rule --name <название правила>

kess-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 kess-control --move-rule

Команда позволяет изменить приоритет выполнения сетевого пакетного правила.

Синтаксис команды

```
kess-control [-F] --move-rule --name <название правила> --at <индекс>

kess-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 kess-control --add-zone

Команда позволяет добавить адрес в сетевую зону.

Синтаксис команды

```
kess-control [-F] --add-zone --zone <зона> --address <адрес>
```

Аргументы и ключи

`--zone <зона>` – предустановленное имя сетевой зоны.

`--address <адрес>` – сетевой адрес или подсеть.

Команда kess-control --del-zone

Команда позволяет удалить адрес из сетевой зоны.

Синтаксис команды

```
kess-control [-F] --del-zone --zone <зона> --address <адрес>

kess-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 kess-control -F --query

Команда позволяет посмотреть правила сетевого экрана, созданные с помощью приложения Kaspersky Embedded Systems Security.

Синтаксис команды

```
kess-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 kess-control --get-blocked-hosts

Команда позволяет вывести в консоль список заблокированных устройств.

Синтаксис команды

```
kess-control [-H] --get-blocked-hosts
```

Команда kess-control --allow-hosts

Команда позволяет разблокировать заблокированные устройства.

Синтаксис команды

```
kess-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 kess-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

```
kess-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 kess-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

```
kess-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 kess-control --request-temporary-device-access

Команда позволяет создать файл запроса доступа, чтобы запросить временный доступ к заблокированному устройству.

Синтаксис команды

```
kess-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 kess-control --upload-temporary-device-access-key

Команда позволяет загрузить ключ доступа, чтобы получить временный доступ к заблокированному устройству.

Синтаксис команды

```
kess-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 kess-control --get-app-list

Команда позволяет вывести список приложений, обнаруженных на клиентском устройстве во время выполнения задачи Инвентаризация.

Синтаксис команды

```
kess-control [-A] --get-app-list [--json]
```

Аргументы и ключи

`--json` – выводить данные в формате JSON.

Команда kess-control --get-categories

Команда позволяет вывести список созданных категорий контроля приложений.

Синтаксис команды

```
kess-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 kess-control --set-categories

Команда позволяет создать или изменить список созданных категорий контроля приложений.

Синтаксис команды

```
kess-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 kess-control --get-settings 21

Команда позволяет вывести список созданных правил контроля приложений.

Синтаксис команды

```
kess-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 kess-control --set-settings 21

Команда позволяет изменить список созданных категорий приложений и правил контроля приложений.

Синтаксис команды

```
kess-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 kess-control --set-to-default 21

Команда позволяет удалить список категорий приложений и правил контроля приложений.

Синтаксис команды

```
kess-control --set-settings 21 --set-to-default
```

Команда kess-control ---add-app-control-trust-certificate

Команда позволяет добавить сертификат в список доверенных сертификатов Контроля приложений.

Синтаксис команды

```
kess-control [-A] --add-app-control-trust-certificate <путь к сертификату>
```

Аргументы и ключи

`<путь к сертификату>` – путь к файлу сертификата, который вы хотите добавить, в формате PEM или DER.

Команда kess-control --remove-app-control-trust-certificate

Команда позволяет удалить сертификат из списка доверенных сертификатов Контроля приложений.

Синтаксис команды

```
kess-control [-A] --remove-app-control-trust-certificate <серийный номер сертификата>
```

Команда kess-control --query-app-control-trust-certificates

Команда позволяет вывести список доверенных сертификатов Контроля приложений.

Синтаксис команды

```
kess-control [-A] --query-app-control-trust-certificates
```

Команды управления резервным хранилищем

-B – префикс, указывающий, что команда принадлежит к группе команд управления резервным хранилищем.

Команда kess-control -B --mass-remove

Команда позволяет удалить из резервного хранилища все или только указанные объекты.

Синтаксис команды

Удалить все объекты:

```
kess-control -B --mass-remove
```

Удалить объекты, соответствующие условиям фильтра:

```
kess-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 kess-control -B --query

Команда позволяет вывести информацию об объектах резервного хранилища.

Синтаксис команды

Вывести информацию обо всех объектах резервного хранилища:

```
kess-control -B --query [-n <количество>] [--json] [--reverse]
```

Вывести информацию об объектах резервного хранилища, соответствующих условиям фильтра:

```
kess-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 kess-control -B --restore

Команда позволяет восстановить объект из резервного хранилища.

Синтаксис команды

```
kess-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 kess-control -Q --mass-remove

Команда позволяет удалить из карантина все или только указанные файлы.

Синтаксис команды

Удалить все файлы:

```
kess-control -Q --mass-remove
```

Удалить файлы, соответствующие условиям фильтра:

```
kess-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 kess-control --put

Команда позволяет поместить файл на карантин.

Синтаксис команды

```
kess-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 kess-control -Q --query

Команда позволяет вывести информацию о файлах на карантине.

Синтаксис команды

Вывести информацию обо всех файлах на карантине:

```
kess-control -Q --query [-n < количество >] [--json]
```

Вывести информацию о файлах на карантине, соответствующих условиям фильтра:

```
kess-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 kess-control -Q --restore

Команда позволяет восстановить файл из карантина.

Синтаксис команды

```
kess-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/kess/common/restored/. Вы можете вручную переместить файл из этой директории в нужную директорию.

Команды управления сетевой изоляцией устройства

-R – префикс, указывающий, что команда принадлежит к группе команд управления сетевой изоляцией устройства. Сетевая изоляция устройств применяется как действие по реагированию на обнаружение угрозы при интеграции с решением Kaspersky Managed Detection and Response.

Команда kess-control --isolation-stat

Команда позволяет вывести в консоль текущее состояние сетевой изоляции: включена или выключена.

Синтаксис команды

```
kess-control [-R] --isolation-stat
```

Команда kess-control --isolation-off

Команда позволяет временно выключить сетевую изоляцию устройства.

Синтаксис команды

```
kess-control [-R] --isolation-off
```

Команды управления пользователями и ролями

-U – префикс, указывающий, что команда принадлежит к группе команд управления пользователями и ролями.

Команда kess-control --get-user-list

Команда позволяет вывести список пользователей и ролей.

Синтаксис команды

```
kess-control [-U] --get-user-list
```

Команда kess-control --grant-role

Команда позволяет назначить роль определенному пользователю.

Синтаксис команды

```
kess-control [-U] --grant-role <роль> <пользователь>
```

Команда kess-control --revoke-role

Команда позволяет отозвать роль у определенного пользователя.

Синтаксис команды

```
kess-control [-U] --revoke-role <роль> <пользователь>
```

Команды управления сбором метрик о состоянии системы

Команда kess-control --export-metrics

Команда позволяет настроить сбор метрик о состоянии операционной системы.

Синтаксис команды

```
kess-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 Embedded Systems 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 Embedded Systems 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/kess/common/agreements.ini

  Конфигурационный файл agreements.ini содержит параметры, связанные с Лицензионным соглашением, Политикой конфиденциальности и Положением о Kaspersky Security Network.

- /var/opt/kaspersky/kess/common/kess.ini

  Конфигурационный файл kess.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 под руководством специалистов Службы технической поддержки по полученным от них инструкциям.

Параметр	Описание	Значения
Секция **[General]** содержит следующие параметры:		
`Locale`	Языковой стандарт, используемый для локализации текстов, передаваемых приложением Kaspersky Embedded Systems Security в Kaspersky Security Center (события, уведомления, результаты выполнения задач и другие). Локализация графического интерфейса и командной строки приложения зависит от локализации, указанной в переменной окружения `LANG`. Если в переменной окружения `LANG` указана локализация, которую не поддерживает приложение Kaspersky Embedded Systems Security, то графический интерфейс и командная строка отображаются в английской локализации.	Языковой стандарт в формате, определенном в RFC 3066. Если параметр `Locale` не указан, устанавливается язык локализации операционной системы. Если приложению не удалось определить язык локализации операционной системы или эта локализация операционной системы не поддерживается, устанавливается значение по умолчанию `en_US.utf8`.
`PackageType`	Формат установленного пакета приложения. Не рекомендуется изменять значение этого параметра вручную. Значение параметра 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.
`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.
`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/kess/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.

Параметр	Описание	Значения
`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 kess-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.
`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.
Секция **[Network]** содержит следующие параметры:		
`WtpFwMark`	Метка в правилах утилиты iptables для перенаправления трафика в приложение для обработки компонентом Защита от веб-угроз. Вам может потребоваться изменить эту метку, если на одном устройстве с установленным приложением работает другое ПО, которое использует девятый бит маски TCP-пакета, и возникает конфликт.	Значение задается десятеричным или шестнадцатеричным числом с префиксом 0x. Значение по умолчанию: 0x100. Во избежание цикличной проверки трафика при работе приложения на узлах, используемых в составе распределенных систем, таких как Kubernetes, требуется изменить значения меток сетевых пакетов, используя более старшие биты. Например: 0x1000 или 0x10000 (значение метки ограничено 32-битным целым числом).

Параметр	Описание	Значения
`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 исключить запись о них 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 компонентами Защита от файловых угроз и Анализ поведения.	`true/yes` (значение по умолчанию) – включить подсчет статистики проверки файлов и процессов. `false/no` – не включать подсчет статистики проверки файлов и процессов.
`StatCollectionPeriod`	Интервал времени, в течение которого приложение считает статистику проверки файлов и процессов компонентами Защита от файловых угроз и Анализ поведения, перед сохранением в файл трассировки и в отчеты.	Значение по умолчанию: 10 минут.
`StatCollectionCount`	Количество файлов и 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 **[Watchdog]** содержит следующие параметры:		

Параметр	Описание	Значения
`TimeoutAfterHeadshot`	Максимальное время ожидания завершения процесса kess от момента отправки сигнала HEADSHOT Watchdog-сервером процессу kess.	Значение по умолчанию: 2 минуты.
`StartupTimeout`	Максимальное время ожидания запуска приложения (в минутах), после которого Watchdog-сервер начинает процедуру перезапуска процесса kess.	Значение по умолчанию: 3 минуты.
`TimeoutAfterKill`	Максимальное время ожидания завершения управляемого процесса kess от момента отправки сигнала SIGKILL Watchdog-сервером процессу kess. Если по истечении этого времени процесс kess 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 (в миллисекундах).	Значение по умолчанию: 2000.
`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 kess.	Значение по умолчанию: 2 минуты.
`ConnectTimeout`	Максимальный интервал времени от момента запуска процесса kess до момента установления приложением соединения с Watchdog-сервером. Если приложение не успевает создать соединение за этот интервал времени, Watchdog-сервер начинает процедуру перезапуска процесса kess.	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 kess от момента отправки сигнала SHUTDOWN Watchdog-сервером процессу kess.	Значение по умолчанию: 2 минуты.
`MaxMemory`	Ограничение на использование резидентной памяти процесса kess. Если резидентная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру перезапуска процесса kess.	`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`.

Параметр	Описание	Значения
`MaxVirtualMemory`	Ограничение на использование виртуальной памяти процесса kess. Если виртуальная память управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру перезапуска процесса kess.	`off` (значение по умолчанию) – использование виртуальной памяти не ограничено. `< значение >MB` – значение в мегабайтах.
`MaxSwapMemory`	Ограничение на размер swap-файла управляемого процесса kess. Если swap-файл управляемого процесса превышает это ограничение, Watchdog-сервер начинает процедуру перезапуска процесса kess.	`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 мониторинга стабильности работы приложения. Если мониторинг стабильности работы приложения включен, Watchdog-сервер отслеживает количество нештатных остановок приложения.	`true/yes` – включить мониторинг стабильности работы приложения. `false/no` (значение по умолчанию) – выключить мониторинг стабильности работы приложения.
`ProductHealthLogFile`	Путь к файлу, с помощью которого осуществляется мониторинг стабильности приложения.	Значение по умолчанию: /var/opt/kaspersky/kess/private/kess_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.
`WarnAfter_#_crash`	Количество нештатных остановок приложения, необходимых для отображения уведомления 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.
`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 kess.	Значение по умолчанию: 32 секунды.
`DumpSuspendPeriod`	Максимальное время ожидания завершения создания файла дампа приложения, в течение которого Watchdog-сервер приостанавливает проверку активности приложения (в минутах). Если по истечении этого времени создание файла дампа не завершилось, Watchdog-сервер начинает процедуру перезапуска процесса kess.	Возможные значения: 1 – 30 минут. Значение по умолчанию: 2.

Параметр	Описание	Значения
`TimeoutAfterCoredump`	Максимальный интервал времени, в течение которого Watchdog-сервер приостанавливает отправку других сигналов процессу kess 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.

Если параметр отсутствует в файле или указано некорректное значение параметра, то приложение будет использовать значение по умолчанию.

Параметры задач командной строки по умолчанию

Этот раздел содержит параметры по умолчанию всех предустановленных задач, которые предусмотрены для управления приложением Kaspersky Embedded Systems 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/kess/

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 задачи Behavior_Detection (ID:20)

```
UseTrustedPrograms=No

TaskMode=Block

UseTelemetryMonopolyMode=Yes

TelemetrySource=Default
```

Параметры по умолчанию задачи Application_Control (ID:21)

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules

UseTrustedCustomCerts=Yes
```

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 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.

Общие параметры приложения

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.

Параметр	Описание	Значения
`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/kess. 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.
`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.

Параметр	Описание	Значения
`NamespaceMonitoring`	Включение использования механизма пространств имен, который в том числе обеспечивает проверку файлов в контейнерах и мандатных сессиях операционной системы Astra Linux. Приложение не проверяет пространства имен и контейнеры, если в операционной системе не установлены компоненты для работы с ними.	`Yes` (значение по умолчанию) – включить использование механизма пространств имен. `No` – выключить использование механизма пространств имен.
`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 и Контроль устройств 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.
`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.	`Yes` – включить режим работы, при котором приложение Kaspersky Embedded Systems 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.

Параметр	Описание	Значения
`UseProxy`	Включение использования прокси-сервера компонентами приложения Kaspersky Embedded Systems Security.	`Yes` – включить использование прокси-сервера. `No` (значение по умолчанию) – выключить использование прокси-сервера.
`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 `\`).
`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.
`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/kess/private/storage/events.db.

Параметр	Описание	Значения
`ExcludedMountPoint.item_#`	Точка монтирования, которую требуется исключить из области проверки. Исключение применяется в работе компонентов Защита от файловых угроз, Защита от шифрования и задачи Проверка съемных дисков, а также настраивается в работе задач проверки с типом ODS. 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* и *InventoryScan*.	`Yes` – включить ограничение потребления ресурсов процессора для задач типа *ODS* 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* 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 – 4000 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. В качестве резервного хранилища 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/kess/common/objects-backup/ Для доступа к заданной по умолчанию директории требуются root-права.

Параметр	Описание	Значения
`QuarantineFillingNotification`	Процент заполнения карантина, при котором формируется событие о заполнении карантина. Чтобы выключить формирование событий о заполнении карантина, укажите значение 0.	0 – 100 0 – формирование событий о заполнении карантина выключено. Значение по умолчанию: 90.
`QuarantineSizeLimit`	Максимальный размер карантина (в мегабайтах). При достижении максимального размера карантина приложение удаляет самые старые файлы. Чтобы снять ограничение на размер карантина, укажите значение 0.	0 – 4000 0 – размер карантина не ограничен. Значение по умолчанию: 200.
`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).

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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security не запущено;

66 – базы приложения не загружены (используется только командой `kess-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 обнаружены угрозы;

73 – попытка задать параметры задачи Контроль приложений, влияющие на работу приложения Kaspersky Security Network, без их подтверждения с помощью ключа `--accept`.

74 – требуется перезапуск приложения Kaspersky Embedded Systems 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;

80 – операция скачивания обновлений завершилась с ошибкой из-за сетевых проблем;

128 – неизвестная ошибка;

65 – все остальные ошибки.

Приложение 4. Параметры для взаимодействия с внешними службами

Приложение Kaspersky Embedded Systems 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: Any 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.

Источники информации о Kaspersky Embedded Systems Security

Страница Kaspersky Embedded Systems Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Embedded Systems Security вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

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

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.

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.

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.

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.

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.

EulerOS является товарным знаком Huawei Technologies Co., Ltd.

Core является товарным знаком Intel Corporation или ее дочерних компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Outlook, Visual C++ и Windows являются товарными знаками группы компаний Microsoft.

Oracle, Java, 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 – 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.