KASPERSKY lab

Kaspersky Embedded Systems Security

Руководство администратора

Версия программы: 2.3.0.754

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 26.04.2019

https://www.kaspersky.ru
https://support.kaspersky.ru

Содержание

Об этом руководстве

Руководство администратора Kaspersky Embedded Systems Security 2.3 (далее также "Kaspersky Embedded Systems Security", "программа") адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Embedded Systems Security на всех защищаемых устройствах, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Embedded Systems Security.

В этом руководстве приведена информация о настройке и использовании Kaspersky Embedded Systems Security.

Также из этого руководства вы можете узнать об источниках информации о программе и способах получения технической поддержки.

В этом разделе

В этом документе

Руководство администратора Kaspersky Embedded Systems Security содержит следующие разделы:

Источники информации о Kaspersky Embedded Systems Security

Этот раздел содержит описание источников информации о программе.

Kaspersky Embedded Systems Security

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Embedded Systems Security, перечень аппаратных и программных требований Kaspersky Embedded Systems Security.

Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Embedded Systems Security.

Интерфейс программы

Этот раздел содержит информацию об элементах интерфейса Kaspersky Embedded Systems Security.

Лицензирование программы

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

Запуск и остановка Kaspersky Embedded Systems Security

Этот раздел содержит информацию о запуске и остановке Плагина управления Kaspersky Embedded Systems Security (далее также "Плагин управления") и службы Kaspersky Security.

Права доступа к функциям Kaspersky Embedded Systems Security

Этот раздел содержит информацию о правах на управление Kaspersky Embedded Systems Security и службами Windows®, которые регистрирует программа, а также инструкции по настройке этих прав.

Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Embedded Systems Security на нескольких компьютерах.

Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security, их создании, настройке параметров выполнения, запуске и остановке.

Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Embedded Systems Security в Kaspersky Security Center.

Постоянная защита компьютера

Этот раздел содержит информацию о компонентах постоянной защиты компьютера: Постоянная защита файлов, Использование KSN и Защита от эксплойтов. Также этот раздел содержит инструкции по настройке параметров задач постоянной защиты компьютера и параметров безопасности защищаемого компьютера.

Контроль активности на компьютерах

Этот раздел содержит информацию о функциях Kaspersky Embedded Systems Security, которые позволяют контролировать запуски программ и подключения внешних устройств по USB.

Контроль активности в сети

Этот раздел содержит информацию о задаче Управление сетевым экраном.

Диагностика системы

Этот раздел содержит информацию о задаче контроля файловых операций и возможностях анализа системного журнала операционной системы.

Интеграция со сторонними системами

В этом разделе описана интеграция Kaspersky Embedded Systems Security с функциями и технологиями сторонних производителей.

Работа с Kaspersky Embedded Systems Security из командной строки

Этот раздел содержит описание работы с Kaspersky Embedded Systems Security из командной строки.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Глоссарий

Этот раздел содержит список терминов, которые встречаются в тексте документа, а также определения этих терминов.

АО "Лаборатория Касперского"

Этот раздел содержит информацию об АО "Лаборатории Касперского".

Информация о стороннем коде

Этот раздел содержит информацию о стороннем коде, используемом в программе.

Уведомления о товарных знаках

В этом разделе перечислены товарные знаки сторонних правообладателей, использованные в документе.

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: …	Примеры приведены в блоках на голубом фоне под заголовком "Пример".
Обновление – это... Возникает событие *Базы устарели*.	*Курсивом* выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены **полужирным шрифтом** и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.

Пример текста	Описание условного обозначения
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены **полужирным шрифтом**.
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и символом "стрелка".
В командной строке введите текст `help` Появится следующее сообщение: Укажите дату в формате `ДД:ММ:ГГ`.	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо имени переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

Источники информации о Kaspersky Embedded Systems Security

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

В этом разделе

Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Embedded Systems Security:

- страница Kaspersky Embedded Systems Security на веб-сайте "Лаборатории Касперского";
- страница программы на веб-сайте Службы технической поддержки (База знаний);
- документация.

Если вы не нашли решение своей проблемы, обратитесь в Службу технической поддержки "Лаборатории Касперского" https://support.kaspersky.ru/.

Для использования источников информации на веб-сайтах требуется подключение к интернету.

Страница Kaspersky Embedded Systems Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Embedded Systems Security https://www.kaspersky.ru/enterprise-security/embedded-systems можно ознакомиться с общей информацией о программе, ее возможностях и особенностях работы.

Страница Kaspersky Embedded Systems Security содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить лицензию.

Страница Kaspersky Embedded Systems Security в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Embedded Systems Security в Базе знаний (https://support.kaspersky.ru/kess2/) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Embedded Systems Security, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Документация Kaspersky Embedded Systems Security

В Руководстве администратора Kaspersky Embedded Systems Security вы можете найти информацию об установке, удалении, настройке и использовании программы.

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и другими пользователями в нашем сообществе https://community.kaspersky.com/.

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Kaspersky Embedded Systems Security

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Embedded Systems Security, перечень аппаратных и программных требований Kaspersky Embedded Systems Security.

В этом разделе

О Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security защищает компьютеры и другие встроенные системы под управлением операционной системы Microsoft® Windows от вирусов и прочих угроз компьютерной безопасности. Пользователями Kaspersky Embedded Systems Security являются администраторы сети организации и сотрудники, отвечающие за антивирусную защиту сети организации.

Kaspersky Embedded Systems Security можно установить на различные встроенные системы под управлением Windows, включая устройства следующих типов:

- банковские автоматы;
- POS-терминалы.

Вы можете управлять Kaspersky Embedded Systems Security следующими способами:

- через Консоль программы, установленную на одном компьютере с Kaspersky Embedded Systems Security или на другом компьютере;
- с помощью команд командной строки;
- через Консоль администрирования Kaspersky Security Center.

Вы можете использовать программу Kaspersky Security Center для централизованного управления компьютерами с установленной программой Kaspersky Embedded Systems Security.

Вы можете просматривать счетчики производительности Kaspersky Embedded Systems Security для программы "Системный монитор", а также счетчики и ловушки SNMP.

Компоненты и функции Kaspersky Embedded Systems Security

В состав программы входят следующие компоненты:

- **Постоянная защита**. Kaspersky Embedded Systems Security проверяет объекты при обращении к ним. Kaspersky Embedded Systems Security проверяет следующие объекты:
  - файлы;
  - альтернативные потоки файловых систем (NTFS-streams);
  - Основные загрузочные записи и загрузочные секторы локальных жестких и съемных дисков.
- **Проверка по требованию**. Kaspersky Embedded Systems Security однократно проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Программа проверяет файлы, оперативную память и объекты автозапуска на защищаемом компьютере.
- **Контроль запуска программ**. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ на защищаемом компьютере.
- **Контроль устройств**. Компонент позволяет контролировать регистрацию и использование запоминающих устройств и устройств чтения CD/DVD-дисков с целью защиты компьютера от угроз безопасности, которые могут возникнуть во время файлового обмена с USB-подключаемым флеш-накопителем или внешним устройством другого типа.
- **Управление сетевым экраном**. Компонент предоставляет возможность управления брандмауэром Windows: позволяет настраивать параметры и правила сетевого экрана операционной системы и блокирует любую возможность настройки параметров сетевого экрана извне.
- **Мониторинг файловых операций**. Kaspersky Embedded Systems Security обнаруживает изменения в файлах из области мониторинга, указанной в параметрах задачи. Эти изменения могут свидетельствовать о нарушении безопасности на защищаемом компьютере.
- **Анализ журналов**. Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.

В программе реализованы следующие функции:

- **Обновление баз программы и Обновление модулей программы**. Kaspersky Embedded Systems Security загружает обновления баз и модулей программы с FTP или HTTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или других источников обновлений.
- **Карантин**. Kaspersky Embedded Systems Security перемещает объекты, которые признает возможно зараженными, из исходного местоположения в хранилище *карантина*. В целях безопасности объекты, помещённые на карантин, хранятся в зашифрованном виде.
- **Резервное хранилище**. Kaspersky Embedded Systems Security сохраняет зашифрованные копии объектов со статусом *зараженный* в *резервном хранилище* перед тем, как выполнить лечение или удаление этих объектов.
- **Уведомления администратора и пользователей**. Вы можете настроить уведомление администратора и пользователей, которые обращаются к защищаемому компьютеру, о событиях, связанных с работой Kaspersky Embedded Systems Security и состоянием антивирусной защиты компьютера.
- **Импорт и экспорт параметров**. Вы можете экспортировать параметры Kaspersky Embedded Systems Security в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Embedded Systems Security из конфигурационного файла. Вы можете сохранить в конфигурационный файл как все параметры программы, так и параметры ее отдельных компонентов.

- **Применение шаблонов**. Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов компьютера и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Embedded Systems Security.
- **Управление правами доступа к функциям Kaspersky Embedded Systems Security**. Вы можете настраивать права пользователей и групп пользователей на управление Kaspersky Embedded Systems Security и службами Windows, зарегистрированными программой.
- **Запись событий в журнал событий программы**. Kaspersky Embedded Systems Security записывает в журнал событий информацию о параметрах функциональных компонентов программы, текущем состоянии задач, событиях, возникших за время их выполнения, а также о событиях, связанных с управлением Kaspersky Embedded Systems Security, и информацию, необходимую для диагностики сбоев в работе программы.
- **Доверенная зона**. Вы можете сформировать список исключений из области защиты или проверки, который Kaspersky Embedded Systems Security будет применять в задачах проверки по требованию и постоянной защиты файлов.
- **Защита от эксплойтов**. Вы можете защищать память процессов от эксплуатации уязвимостей с помощью внедряемого в процессы Агента защиты.

Что нового

В Kaspersky Embedded Systems Security появились следующие возможности и улучшения:

- Поддержка новых версий операционных систем Microsoft Windows:

  Windows 10 Redstone 6 (x32 и x64);

- Код активации не отображается полностью в интерфейсе программы.

  Добавленный код активации частично скрыт при отображении в интерфейсе программы. Ни один из пользователей не может увидеть его полностью.

Комплект поставки

В комплект поставки входит программа-приветствие, из которой вы можете выполнить следующие действия:

- запустить мастер установки Kaspersky Embedded Systems Security;
- запустить мастер установки Консоли Kaspersky Embedded Systems Security;
- запустить мастер установки Плагина управления Kaspersky Embedded Systems Security, который позволяет управлять программой через Kaspersky Security Center;
- прочитать Руководство администратора;
- перейти на страницу Kaspersky Embedded Systems Security на веб-сайте "Лаборатории Касперского";
- перейти на веб-сайт Службы технической поддержки https://support.kaspersky.ru;
- прочитать информацию о текущем выпуске Kaspersky Embedded Systems Security.

Папка \console содержит файлы для установки Консоли программы (набор компонентов "Средства Администрирования Kaspersky Embedded Systems Security").

Папка \product содержит следующие файлы:

- файлы для установки компонентов Kaspersky Embedded Systems Security на сервере под управлением 32-разрядной или 64-разрядной операционной системы Microsoft Windows.
- файл для установки Плагина управления Kaspersky Embedded Systems Security через Kaspersky Security Center;
- архив антивирусных баз, актуальных на момент выпуска программы;
- файл с текстом Лицензионного соглашения и Политики конфиденциальности.

Папка \product_no_avbases содержит файлы установки компонентов Kaspersky Embedded Systems Security и Плагина управления без антивирусных баз.

Папка \setup содержит файлы, необходимые для запуска программы-приветствия.

Файлы комплекта поставки располагаются в разных папках в зависимости от их предназначения (см. таблицу ниже).

Таблица 2. Файлы комплекта поставки Kaspersky Embedded Systems Security

Файл	Назначение
autorun.inf	Файл автозапуска мастера установки Kaspersky Embedded Systems Security при установке программы с переносных носителей.
ess_admin_guide_ru.pdf	Руководство администратора.
release_notes.txt	Файл содержит информацию о версии.
setup.exe	Файл запуска программы приветствия (запускает setup.hta).
\console\esstools_x86(x64).msi	Пакет установщика Windows; устанавливает Консоль программы на защищаемый компьютер.
\console\setup.exe	Файл запуска мастера установки для набора компонентов "Средства администрирования" (включающего Консоль программы); запускает файл пакета установки esstools.msi с указанными в мастере параметрами установки.
\product\bases.cab	Архив антивирусных баз, актуальных на момент выпуска программы.
\product\setup.exe	Файл для установки Kaspersky Embedded Systems Security на защищаемом компьютере с помощью мастера установки; запускает файл пакета установки ess.msi с указанными в мастере параметрами.
\product\ess_x86(x64).msi	Пакет установщика Windows; устанавливает Kaspersky Embedded Systems Security на защищаемый компьютер.
\product\ess.kud	Файл в формате Kaspersky Unicode Definition с описанием пакета установки для удаленной установки Kaspersky Embedded Systems Security через Kaspersky Security Center.

Файл	Назначение
\product\klcfginst.exe	Программа установки Плагина управления Kaspersky Embedded Systems Security через Kaspersky Security Center. Установите Плагин управления на каждый компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, если вы планируете управлять Kaspersky Embedded Systems Security через нее.
\product\license.txt	Файл с текстом Лицензионного соглашения и Политики конфиденциальности.
\product\migration.txt	Файл с описанием перехода с предыдущих версий программы.
\setup\setup.hta	Файл запуска программы приветствия.

Аппаратные и программные требования

Перед установкой Kaspersky Embedded Systems Security требуется удалить с компьютера другие антивирусные программы.

Программные требования к защищаемому компьютеру

Вы можете установить Kaspersky Embedded Systems Security на компьютере под управлением 32-разрядной или 64-разрядной операционной системы Microsoft Windows.

Для установки и работы программы на компьютере под управлением операционной системы Windows XP требуется наличие установщика Windows версии 3.1.

Для установки и работы Kaspersky Embedded Systems Security на компьютерах со встроенной операционной системой необходим компонент "Диспетчер фильтров" (Filter Manager).

Вы можете установить Kaspersky Embedded Systems Security на компьютере под управлением одной из следующих 32- или 64-разрядных операционных систем Microsoft Windows:

- Windows XP Embedded SP3 (32-разрядная);
- Windows Embedded POSReady 2009 (32-разрядная);
- Windows XP Professional SP2 / SP3 (32-разрядная, 64-разрядная);
- Windows Embedded Standard 7 SP1 (32-разрядная, 64-разрядная);
- Windows Embedded Enterprise 7 SP1 (32-разрядная, 64-разрядная);
- Windows Embedded POSReady 7 (32-разрядная, 64-разрядная);
- Windows 7 Professional / Enterprise SP1 (32-разрядная, 64-разрядная);
- Windows Embedded 8.1 Industry Professional / Enterprise (32-разрядная, 64-разрядная);
- Windows Embedded 8.0 Standard (32-разрядная, 64-разрядная);
- Windows 8 Professional / Enterprise (32-разрядная, 64-разрядная);
- Windows 8.1 Professional / Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Professional / Enterprise (32-разрядная, 64-разрядная);
- Windows 10 IoT Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная);

- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Redstone 6 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная).

Аппаратные требования к защищаемому компьютеру

Аппаратные требования к защищаемому компьютеру различаются в разных операционных системах Windows.

- Аппаратные требования для компьютера с операционными системами Windows XP (32 / 64-разрядная), Windows 7 (32-разрядная), Windows 8 (32-разрядная), Windows Embedded XP, Windows Embedded POSReady 2009 и Windows Embedded POSReady 7:
  - Минимальная конфигурация:
    - Объем дискового пространства:
      - для установки компонента Контроль запуска программ – 50 МБ;
      - для установки всех компонентов Kaspersky Embedded Systems Security – 2 ГБ.
    - Объем оперативной памяти:
      - 256 МБ для установки только компонента Контроль запуска программ на компьютер с операционной системой Microsoft Windows;
      - 512 МБ для выполнения полной установки всех компонентов.
    - Требования к процессору:
      - для 32-разрядных операционных систем Microsoft Windows: одноядерный процессор Intel® Pentium® III, 1,4 ГГц;
      - для 64-разрядных операционных систем Microsoft Windows: одноядерный процессор Intel Pentium IV, 1,4 ГГц.
  - Рекомендуемая конфигурация:
    - Объем дискового пространства:
      - для установки компонента Контроль запуска программ – 2 ГБ;
      - для установки всех компонентов Kaspersky Embedded Systems Security – 4 ГБ.
    - Оперативная память: 2 ГБ.
    - Требования к процессору: 2,4 ГГц, четырехъядерный.
- Аппаратные требования для компьютера с операционными системами Windows 7 (64-разрядная), Windows 8 (64-разрядная), Windows 10 (64-разрядная), Windows Embedded 7 и Windows Embedded 8:
  - Минимальная конфигурация:
    - Объем дискового пространства:
      - для установки компонента Контроль запуска программ – 50 МБ;
      - для установки всех компонентов Kaspersky Embedded Systems Security – 2 ГБ.
    - Оперативная память: 1 ГБ.
    - Требования к процессору:
      - для 32-разрядных операционных систем Microsoft Windows: одноядерный процессор Intel

Pentium III, 1,4 ГГц;

- для 64-разрядных операционных систем Microsoft Windows: одноядерный процессор Intel Pentium IV, 1,4 ГГц.

- Рекомендуемая конфигурация
  - Объем дискового пространства:
    - для установки компонента Контроль запуска программ – 2 ГБ;
    - для установки всех компонентов Kaspersky Embedded Systems Security – 4 ГБ.
  - Оперативная память: 2 ГБ.
  - Требования к процессору: 2,4 ГГц, четырехъядерный.

Функциональные требования и ограничения

В этом разделе приведено описание дополнительных функциональных требований и существующих ограничений компонентов Kaspersky Embedded Systems Security.

В этом разделе

Установка и удаление

- Во время установки программы отображается предупреждение, если новый путь к папке установки Kaspersky Embedded Systems Security содержит более 150 символов. Это предупреждение не влияет на процесс установки. Программа Kaspersky Embedded Systems Security будет успешно установлена и запущена.
- Для установки компонентов, поддерживающих протокол SNMP, вам нужно перезапустить службу SNMP, если она запущена.
- Для установки и работы Kaspersky Embedded Systems Security на устройствах, управляемых встроенной операционной системой, нужно установить компонент Filter Manager.
- Установка Средств администрирования Kaspersky Embedded Systems Security невозможна средствами групповых политик Microsoft Active Directory®.
- При установке программы на компьютеры с устаревшей версией операционной системы, для которой невозможно регулярное получение обновлений, нужно проверить следующие корневые сертификаты: DigiCert Assured ID Root CA, DigiCert_High_Assurance_EV_Root_CA, DigiCertAssuredIDRootCA. Отсутствие указанных сертификатов может привести к некорректной работе программы. Рекомендуется установить указанные сертификаты любым возможным способом.

- Консоль Kaspersky Embedded Systems Security невозможно удалить из меню **Пуск**. Консоль Kaspersky Embedded Systems Security можно удалить с помощью ссылки в окне Установка / удаление программ.

Мониторинг файловых операций

По умолчанию компонент Мониторинг файловых операций не проверяет изменения в системных папках и в служебных файлах файловой системы, чтобы информация о стандартных изменениях файлов, постоянно осуществляемых операционной системой, не попадала в отчет выполнения задачи. Нельзя вручную добавить эти папки в область мониторинга.

Следующие папки и файлы исключены из области мониторинга:

- Служебные файлы NTFS с идентификатором файла от 0 до 33
- "%SystemRoot%\\Prefetch\\"
- "%SystemRoot%\\ServiceProfiles\\LocalService\\AppData\\Local\\"
- "%SystemRoot%\\System32\\LogFiles\\Scm\\"
- "%SystemRoot%\\Microsoft.NET\\Framework\\v4.0.30319\\"
- "%SystemRoot%\\Microsoft.NET\\Framework64\\v4.0.30319\\"
- "%SystemRoot%\\Microsoft.NET\\"
- "%SystemRoot%\\System32\\config\\"
- "%SystemRoot%\\Temp\\"
- "%SystemRoot%\\ServiceProfiles\\LocalService\\"
- "%SystemRoot%\\System32\\winevt\\Logs\\"
- "%SystemRoot%\\System32\\wbem\\repository\\"
- "%SystemRoot%\\System32\\wbem\\Logs\\"
- "%ProgramData%\\Microsoft\\Windows\\WER\\ReportQueue\\"
- "%SystemRoot%\\SoftwareDistribution\\DataStore\\"
- "%SystemRoot%\\SoftwareDistribution\\DataStore\\Logs\\"
- "%ProgramData%\\Microsoft\\Windows\\AppRepository\\"
- "%ProgramData%\\Microsoft\\Search\\Data\\Applications\\Windows\\"
- "%SystemRoot%\\Logs\\SystemRestore\\"
- "%SystemRoot%\\System32\\Tasks\\Microsoft\\Windows\\TaskScheduler\\"

Программа исключает папки верхнего уровня.

Компонент не осуществляет мониторинг изменений в файлах, которые происходят в обход файловой системы ReFS/NTFS (изменения, сделанные через BIOS, LiveCD и т.д.).

Управление сетевым экраном

- Работа с IP-адресами в формате IPv6 недоступна, если область указанного применяемого правила состоит из одного адреса.
- Текущие правила политики сетевого экрана обеспечивают выполнение основных сценариев взаимодействия между локальными компьютерами и Сервером администрирования. Для использования функций Kaspersky Security Center в полном объеме вам нужно вручную настроить правила для портов. Информация о номерах портов, протоколах и их функциях приведена в Базе знаний Kaspersky Security Center (статья 9297).
- Программа не контролирует изменение правил и групп правил брандмауэра Windows во время ежеминутных запросов к задаче Управление сетевым экраном, если эти правила не были добавлены в конфигурацию задачи при установке программы. Чтобы обновить статус и включить такие правила, вам нужно перезапустить задачу Управление сетевым экраном.
- При запуске задачи Управление сетевым экраном следующие типы правил автоматически удаляются из параметров сетевого экрана операционной системы:
  - запрещающие правила;
  - правила мониторинга исходящего трафика.

Прочие ограничения

Проверка по требованию и Постоянная защита файлов:

- Не поддерживается проверка при подключении для устройств, работающих по протоколу MTP.
- Проверка объектов в архивах невозможна без проверки SFX-архивов: если включена проверка архивов в параметрах защиты Kaspersky Embedded Systems Security, программа автоматически проверяет объекты как в архивах, так и в SFX-архивах. Возможна проверка SFX-архивов без проверки архивов.

Лицензирование:

- В мастере установки не поддерживается активация программы с помощью файла ключа, если файл ключа хранится на диске, созданном с помощью команды SUBST, или если указан сетевой путь к файлу ключа.

Обновления:

- После установки критических обновлений модулей Kaspersky Embedded Systems Security, по умолчанию значок программы будет скрыт.
- KLRAMDISK не поддерживается на компьютерах с операционной системой Windows XP и Windows 2003.

Интерфейс:

- При использовании фильтров в Консоли программы учитывается регистр для карантина, резервного хранилища, журнала системного аудита и журнала выполнения задач.
- При настройке области защиты и области проверки в Консоли программы можно использовать только одну маску и только в конце пути. Примеры использования маски: "C:\Temp\Temp*", "C:\Temp\Temp???.doc", "C:\Temp\Temp*.doc". Эти ограничения не распространяются на настройку доверенной зоны.

Безопасность:

- Если в операционной системе активирован Контроль учетных записей, учетные записи пользователей должны входить в группу администрирования KAVWSEE, чтобы открывать Консоль программы двойным щелчком мыши на значке программы в области уведомлений панели задач. В противном случае нужно использовать учетную запись с правами открывать Диагностическое окно или оснастку Microsoft Management Console.
- Если активирован Контроль учетных записей пользователей, недоступно удаление программы из окна Microsoft Windows **Программы и компоненты**.

Интеграция с Kaspersky Security Center:

- Сервер администрирования проверяет корректность обновлений баз программы при получении пакетов обновлений и перед отправкой обновлений на компьютеры сети. Сервер администрирования не проверяет корректность полученных обновлений модулей программы.
- Убедитесь, что установлены необходимые флажки в окне параметров взаимодействия с Сервером администрирования, при использовании компонентов, передающих динамически изменяющиеся данные в Kaspersky Security Center с помощью сетевых списков (карантин, резервное хранилище).

Защита от эксплойтов:

- Защита от эксплойтов недоступна, если библиотеки apphelp.dll не загружены в текущей конфигурации сетевого окружения.
- Компонент Защита от эксплойтов несовместим с утилитой EMET от Microsoft на компьютерах с операционной системой Microsoft Windows 10. Kaspersky Embedded Systems Security блокирует EMET, если компонент Защита от эксплойтов установлен на компьютере с установленной утилитой EMET.

Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Embedded Systems Security.

В этом разделе

Коды программных компонентов Kaspersky Embedded Systems Security для службы установщика Windows

По умолчанию файлы \product\ess_x86.msi и \product\ess_x64.msi предназначены для установки всех компонентов Kaspersky Embedded Systems Security. Вы можете установить эти компоненты при выборочной установке программы.

Файлы \console\esstools_x86.msi и \console\esstools_x64.msi устанавливают все программные компоненты набора "Средства администрирования".

В следующих разделах приведены коды компонентов Kaspersky Embedded Systems Security для службы установщика Windows. Вы можете использовать эти коды, чтобы задать список устанавливаемых компонентов при установке Kaspersky Embedded Systems Security из командной строки.

В этом разделе

Программные компоненты Kaspersky Embedded Systems Security

В следующей таблице приведены коды и описания программных компонентов Kaspersky Embedded Systems Security.

Таблица 3. Описание программных компонентов Kaspersky Embedded Systems Security

Компонент	Идентификатор	Предназначение компонента
Основная функциональность	Core	Этот компонент включает в себя набор базовых функций программы и обеспечивает их работу.
Контроль запуска программ	AppCtrl	Этот компонент отслеживает попытки запуска программ пользователями и разрешает или запрещает запуск в соответствии с заданными правилами контроля запуска программ. Компонент реализуется в задаче Контроль запуска программ.
Контроль устройств	DevCtrl	Этот компонент отслеживает попытки подключения запоминающих USB-устройств к защищаемому компьютеру и разрешает или запрещает их использование в соответствии с заданными правилами контроля устройств. Компонент реализуется в задаче Контроль устройств.
Антивирусная защита	AVProtection	Этот компонент обеспечивает антивирусную защиту и включает в себя следующие компоненты: • Проверка по требованию • Постоянная защита файлов
Проверка по требованию	Ods	Этот компонент устанавливает системные файлы Kaspersky Embedded Systems Security и выполняет задачи проверки по требованию (проверка объектов защищаемого компьютера, выполняемая по команде). Если, устанавливая Kaspersky Embedded Systems Security из командной строки, вы укажете другие компоненты Kaspersky Embedded Systems Security, не указывая компонент Core, компонент Core будет установлен автоматически.

Компонент	Идентификатор	Предназначение компонента
Постоянная защита файлов	Oas	Этот компонент обеспечивает антивирусную проверку файлов на защищаемом компьютере при обращении к этим файлам. Компонент реализует задачу Постоянная защита файлов.
Использование Kaspersky Security Network	Ksn	Этот компонент обеспечивает защиту на основе облачных технологий "Лаборатории Касперского". Компонент реализует задачу Использование KSN (отправка запросов и получение заключений от службы Kaspersky Security Network).
Мониторинг файловых операций	Fim	Этот компонент позволяет регистрировать операции, производимые над файлами в выбранной области мониторинга. Компонент реализует задачу Мониторинг файловых операций.
Защита от эксплойтов	AntiExploit	Этот компонент обеспечивает управление параметрами защиты процессов в памяти защищаемого компьютера.
Управление сетевым экраном	Firewall	Этот компонент предоставляет возможность управления сетевым экраном Windows через графический интерфейс Kaspersky Embedded Systems Security. Компонент реализует задачу Управление сетевым экраном.
Модуль интеграции с Агентом администрирования Kaspersky Security Center	AKIntegration	Этот компонент обеспечивает связь Kaspersky Embedded Systems Security с Агентом администрирования Kaspersky Security Center. Вы можете установить этот компонент на защищаемом компьютере, если вы планируете управлять программой через Kaspersky Security Center.
Анализ журналов	LogInspector	Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.

Компонент	Идентификатор	Предназначение компонента
Набор счетчиков производительности программы "Системный монитор"	PerfMonCounters	Компонент устанавливает набор счетчиков производительности программы "Системный монитор". Счетчики производительности позволяют измерять производительность Kaspersky Embedded Systems Security и находить возможные узкие места при совместной работе Kaspersky Embedded Systems Security с другими программами.
Поддержка SNMP-протокола	SnmpSupport	Этот компонент публикует счетчики и ловушки Kaspersky Embedded Systems Security через службу Simple Network Management Protocol (SNMP) Microsoft Windows. Этот компонент можно установить на защищаемом компьютере, только если на нем уже установлена служба Microsoft SNMP.
Значок Kaspersky Embedded Systems Security в области уведомлений	TrayApp	Этот компонент отображает значок Kaspersky Embedded Systems Security в области уведомлений панели задач защищаемого компьютера. Значок Kaspersky Embedded Systems Security показывает состояние защиты компьютера и позволяет открыть Консоль Kaspersky Embedded Systems Security с помощью Microsoft Management Console, если она установлена, и окно **О программе**.

Программные компоненты набора "Средства администрирования"

В следующей таблице приведены коды и описание программных компонентов набора "Средства администрирования".

Таблица 4. Описание программных компонентов набора "Средства администрирования"

Компонент	Код	Функции компонента
Оснастка Kaspersky Embedded Systems Security	MmcSnapin	Компонент устанавливает оснастку Microsoft Management Console для управления через Консоль Kaspersky Embedded Systems Security. Если при установке набора "Средства администрирования" из командной строки, вы укажете другие компоненты набора, но не укажите компонент MmcSnapin, компонент MmcSnapin будет установлен автоматически.

Компонент	Код	Функции компонента
Справка	Help	Этот компонент представляет собой chm-файл справки. Он сохраняется в папку с файлами Средств администрирования Kaspersky Embedded Systems Security. Вы можете открыть файл справки из меню **Пуск** или с помощью клавиши **F1** при открытом окне Консоли программы.
Документация	Help	Kaspersky Embedded Systems Security добавляет ярлык для перехода на веб-сайт "Лаборатории Касперского", где документ "Руководство администратора" доступен в формате PDF. Этот ярлык доступен из меню **Пуск**.

Изменения в системе после установки Kaspersky Embedded Systems Security

При совместной установке Kaspersky Embedded Systems Security и набора "Средства администрирования", включающего Консоль программы, служба установщика Windows выполняет на защищаемом компьютере следующие изменения:

- создает папки Kaspersky Embedded Systems Security на защищаемом компьютере и на компьютере, где установлена Консоль программы;
- регистрирует службы Kaspersky Embedded Systems Security;
- создает группу пользователей Kaspersky Embedded Systems Security;
- регистрирует в системном реестре ключи Kaspersky Embedded Systems Security.

Эти изменения описаны ниже.

Папки Kaspersky Embedded Systems Security на защищаемом компьютере

При установке Kaspersky Embedded Systems Security на защищаемом компьютере создаются следующие папки:

- Заданная по умолчанию папка установки Kaspersky Embedded Systems Security, содержащая исполняемые файлы Kaspersky Embedded Systems Security в зависимости от разрядности операционной системы. По умолчанию используются следующие папки установки:
  - В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
  - В 64-х разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- Файлы Management Information Base (MIB), содержащие описание счетчиков и ловушек, публикуемых Kaspersky Embedded Systems Security по протоколу SNMP.
  - %Kaspersky Embedded Systems Security%\mibs
- 64-разрядные версии исполняемых файлов Kaspersky Embedded Systems Security (папка создается только при установке Kaspersky Embedded Systems Security в 64-разрядной версии Microsoft Windows).

    - %Kaspersky Embedded Systems Security%\x64
- Служебные файлы Kaspersky Embedded Systems Security:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Data\
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Settings\
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Dskm\
- Файлы с параметрами источников обновлений:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Update\
- Обновления баз и программных модулей, загруженные с помощью задачи Копирование обновлений (папка создается при первой загрузке обновлений с помощью задачи Копирование обновлений).
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Update\Distribution\
- Журналы выполнения задач и журнал системного аудита.
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports\
- Набор используемых баз данных:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Current\
- Резервные копии баз; перезаписывается при каждом обновлении баз.
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Backup\
- Временные файлы, создаваемые при выполнении задач обновления.
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Temp\
- Объекты на карантине (папка по умолчанию).
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Quarantine\
- Объекты в резервном хранилище (папка по умолчанию).
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Backup\
- Объекты, восстановленные из резервного хранилища и карантина (папка по умолчанию для восстановленных объектов).
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored\

Папка, создаваемая при установке Консоли программы

Заданная по умолчанию папка установки Консоли программы, содержащая файлы набора "Средства администрирования", зависит от разрядности операционной системы. По умолчанию используются следующие папки установки:

- В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\
- В 64-х разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\

Службы Kaspersky Embedded Systems Security

Следующие службы Kaspersky Embedded Systems Security запускаются под системной учетной записью "Локальная система" (SYSTEM).

- Kaspersky Security Service (KAVFS) – это основная служба Kaspersky Embedded Systems Security, которая управляет задачами и рабочими процессами Kaspersky Embedded Systems Security.
- Служба Kaspersky Security Management (KAVFSGT) – это служба, предназначенная для управления Kaspersky Embedded Systems Security через Консоль программы.
- Служба Kaspersky Security Exploit Prevention (KAVFSSLP) – это служба, исполняющая роль посредника при передаче параметров безопасности внешним агентам безопасности и при получении данных о событиях безопасности.

Группа Kaspersky Embedded Systems Security

ESS Administrators – это группа на защищаемом компьютере, пользователи которой имеют полный доступ к службе Kaspersky Security Management и ко всем функциям Kaspersky Embedded Systems Security.

Ключи системного реестра

При установке Kaspersky Embedded Systems Security создаются следующие ключи системного реестра:

- Свойства Kaspersky Embedded Systems Security: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Параметры журнала событий Kaspersky Embedded Systems Security (Kaspersky Event Log): [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Свойства службы управления Kaspersky Embedded Systems Security: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Параметры счетчиков производительности:
  - В 32-х разрядной версии Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - В 64-х разрядной версии Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- Параметры компонента Поддержка SNMP-протокола:
  - В 32-х разрядной версии Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\SnmpAgent]
  - В 64-х разрядной версии Microsoft Windows:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\SnmpAgent]

- Параметры файла дампа:
  - В 32-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\CrashDump]
  - В 64-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\CrashDump]
- Параметры файла трассировки:
  - В 32-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
  - В 64-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace]
- Параметры задач и функций программы:
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Environment]

Процессы Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security запускает процессы, описанные в таблице ниже.

Таблица 5. Процессы Kaspersky Embedded Systems Security

Имя файла	Назначение
kavfswp.exe	Рабочий процесс Kaspersky Embedded Systems Security
kavtray.exe	Процесс значка области уведомлений
kavfsmui.exe	Процесс компонента Диагностическое окно
kavshell.exe	Процесс утилиты командной строки
kavfsrcn.exe	Процесс удаленного управления Kaspersky Embedded Systems Security
kavfs.exe	Процесс службы Kaspersky Security
kavfsgt.exe	Процесс службы Kaspersky Security Management
kavfswh.exe	Процесс службы Kaspersky Security Exploit Prevention

Параметры установки и удаления и ключи командной строки для службы установщика Windows

В этом разделе описаны параметры установки и удаления Kaspersky Embedded Systems Security, их значения по умолчанию, указаны ключи для изменения параметров установки и возможные значения этих

ключей. Вы можете использовать эти ключи вместе со стандартными ключами команды `msiexec` службы установщика Windows при установке Kaspersky Embedded Systems Security из командной строки.

Параметры установки и ключи командной строки для установщика Windows

- Согласие с условиями Лицензионного соглашения: необходимо принять условия для установки Kaspersky Embedded Systems Security.

  Возможны следующие значения ключа командной строки `EULA=<значение>`:

  - `0` – вы отклоняете условия Лицензионного соглашения (значение по умолчанию).
  - `1` – вы принимаете условия Лицензионного соглашения.

- Согласие с условиями Политики конфиденциальности: необходимо принять условия для установки Kaspersky Embedded Systems Security.

  Возможны следующие значения ключа командной строки `PRIVACYPOLICY=<значение>`:

  - `0` – вы отклоняете условия Политики конфиденциальности (значение по умолчанию).
  - `1` – вы принимаете условия Политики конфиденциальности.

- Установка Kaspersky Embedded Systems Security с предварительной проверкой активных процессов и загрузочных секторов локальных дисков.

  Возможны следующие значения ключа командной строки `PRESCAN=<значение>`:

  - `0` – не выполнять предварительную проверку активных процессов и загрузочных секторов локальных дисков во время установки (значение по умолчанию).
  - `1` – выполнить предварительную проверку активных процессов и загрузочных секторов локальных дисков во время установки.

- Папка, в которую будут сохранены файлы Kaspersky Embedded Systems Security при установке. Вы можете указать другую папку.

  Значение по умолчанию для ключа командной строки `INSTALLDIR=<полный путь к папке>`:

  - Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - Средства администрирования: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
  - В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%

- Задача Постоянная защита файлов запускается сразу после запуска Kaspersky Embedded Systems Security. Включите этот параметр, чтобы запустить Постоянную защиту файлов при запуске Kaspersky Embedded Systems Security (рекомендуется).

  Возможны следующие значения ключа командной строки `RUNRTP=<значение>`:

  - `1` – запустить (значение по умолчанию).
  - `0` – не запускать.

- Исключения из области защиты, рекомендуемые корпорацией Microsoft. В задаче Постоянная защита файлов: исключать из области защиты объекты на компьютере, которые рекомендует исключать корпорация Microsoft. Некоторые программы на компьютере могут работать нестабильно, когда антивирусная программа перехватывает или изменяет файлы, используемые этими программами. К таким программам корпорация Microsoft относит, например, некоторые программы

контроллеров доменов.

Возможны следующие значения ключа командной строки ADDMSEXCLUSION=<значение>:

- 1 – исключить (значение по умолчанию).
- 0 – не исключать.

- Объекты, исключаемые из области защиты в соответствии с рекомендациями "Лаборатории Касперского". В задаче Постоянная защита файлов: исключать из области защиты объекты на компьютере, которые рекомендует исключать "Лаборатория Касперского".

  Возможны следующие значения ключа командной строки ADDKLEXCLUSION=<значение>:

  - 1 – исключить (значение по умолчанию).
  - 0 – не исключать.

- Разрешить удаленное подключение к Консоли программы По умолчанию удаленное подключение к Консоли программы, установленной на защищаемом компьютере, не разрешено. Во время установки можно разрешить подключение. Kaspersky Embedded Systems Security создаст разрешающие правила для процесса kavfsgt.exe по протоколу TCP для всех портов.

  Возможны следующие значения ключа командной строки ALLOWREMOTECON=<значение>:

  - 1 – разрешить.
  - 0 – запретить (значение по умолчанию).

- Путь к файлу ключа. По умолчанию установщик Windows пытается найти файл с расширением .key в папке \product комплекта поставки. Если в папке \product имеется несколько файлов ключа, установщик Windows выбирает файл ключа с самой поздней датой истечения срока действия. Можно предварительно сохранить файл ключа в папке \product или указать другой путь к файлу ключа с помощью параметра **Добавление ключа**. Вы можете добавить ключ после установки Kaspersky Embedded Systems Security с помощью выбранного вами средства администрирования, например, через Консоль программы. Если вы не добавите ключ программы во время его установки, после установки Kaspersky Embedded Systems Security не будет функционировать.

- Путь к конфигурационному файлу. Kaspersky Embedded Systems Security импортирует параметры из указанного конфигурационного файла, созданного в программе. Kaspersky Embedded Systems Security не импортирует из конфигурационного файла пароли, например пароли учетных записей для запуска задач или пароли для соединения с прокси-сервером. После импорта параметров вам нужно ввести все пароли вручную. Если вы не укажете конфигурационный файл, после установки программа начнет работать с параметрами по умолчанию.

  Значение по умолчанию для параметра CONFIGPATH=<имя конфигурационного файла> не указано.

- Включение сетевых соединений для Консоли программы. Используйте этот параметр, если вы устанавливаете Kaspersky Embedded Systems Security не на защищаемом компьютере. Вы можете удаленно управлять защитой компьютера с другого компьютера, на котором установлена Консоль Kaspersky Embedded Systems Security. В брандмауэре Microsoft Windows будет открыт TCP-порт 135, разрешены сетевые соединения для исполняемого файла kavfsrcn.exe для удаленного управления Kaspersky Embedded Systems Security и предоставлен доступ к DCOM-программам. После завершения установки добавьте пользователей, которые будут управлять программой удаленно, в группу ESS Administrators и разрешите сетевые подключения компьютера к службе Kaspersky Security Management (файл kavfsgt.exe). Вы можете подробнее прочитать о дополнительной настройке при установке Консоли программы на другом компьютере (см. раздел "Дополнительная настройка после установки Консоли программы на другом компьютере" на стр. 51).

Возможны следующие значения ключа командной строки ADDWFEXCLUSION=<значение>:

- 1 – разрешить.
- 0 – запретить (значение по умолчанию).

- Отключение проверки на наличие несовместимого программного обеспечения. Используйте этот параметр, чтобы включить или выключить проверку на наличие несовместимого программного обеспечения при установке программы на компьютер в фоновом режиме. Независимо от значения этого параметра, при установке Kaspersky Embedded Systems Security программа всегда предупреждает о других версиях программы, установленных на этом компьютере.

  Возможны следующие значения ключа командной строки SKIPINCOMPATIBLESW=<значение>:

  - 0 – выполняется проверка на несовместимое программное обеспечение (значение по умолчанию).
  - 1 – проверка на наличие несовместимого программного обеспечения не выполняется.

Параметры удаления и ключи командной строки для установщика Windows

- Восстановление содержимого карантина.

  Возможны следующие значения ключа командной строки RESTOREQTN=<значение>:

  - 0 – удалить содержимое карантина (значение по умолчанию).
  - 1 – восстановить содержимое карантина в папку, указанную в качестве значения параметра RESTOREPATH, во вложенную подпапку \Quarantine.

- Восстановление содержимого резервного хранилища.

  Возможны следующие значения ключа командной строки RESTOREBCK=<значение>:

  - 0 – удалить содержимое резервного хранилища (значение по умолчанию).
  - 1 – восстановить содержимое резервного хранилища в папку, указанную в качестве значения параметра RESTOREPATH, во вложенную папку \Backup.

- Ввод текущего пароля для подтверждения операции удаления (при включенной функции защиты паролем).

  Значение по умолчанию для ключа UNLOCK_PASSWORD=<указанный пароль> не задано.

- Папка для восстановленных объектов. Восстановленные объекты будут сохранены в указанной папке.

  Значение по умолчанию для ключа командной строки RESTOREPATH=<полный путь к папке> – %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored.

Журналы установки и удаления Kaspersky Embedded Systems Security

Если вы выполняете установку или удаление Kaspersky Embedded Systems Security с помощью мастера установки (удаления), служба установщика Windows создает журнал установки (удаления). Файл журнала с именем ess_install_<uid>.log (где <uid> – это уникальный восьмизначный идентификатор журнала)

сохраняется в папку %temp% пользователя, с правами учетной записи которого был запущен файл setup.exe.

Если в меню **Пуск** вы выбрали пункт **Изменение или удаление Средств администрирования Kaspersky Embedded Systems Security 2.3** для Консоли программы или для Kaspersky Embedded Systems Security, в папке %temp% будет автоматически создан файл журнала с именем ess_2.3_maintenance.log.

Если вы выполняете установку или удаление Kaspersky Embedded Systems Security из командной строки, по умолчанию файл журнала установки не создается.

► *Чтобы установить Kaspersky Embedded Systems Security и создать файл журнала на диске C:\, выполните одну из следующих команд:*

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

Планирование установки

В этом разделе описаны средства администрирования Kaspersky Embedded Systems Security, особенности установки и удаления Kaspersky Embedded Systems Security с помощью мастера установки (см. раздел "Установка и удаление программы с помощью мастера" на стр. 47), из командной строки (см. раздел "Установка и удаление программы из командной строки" на стр. 60), через Kaspersky Security Center (см. раздел "Установка и удаление программы через Kaspersky Security Center" на стр. 65) и через групповые политики Active Directory (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. 70).

Перед началом установки Kaspersky Embedded Systems Security составьте план основных этапов установки.

1. Выберите средства администрирования, которые вы будете использовать для управления Kaspersky Embedded Systems Security и его настройки.
2. Определите, какие программные компоненты требуется установить (см. раздел "Коды программных компонентов Kaspersky Embedded Systems Security для службы установщика Windows" на стр. 33).
3. Выберите способ установки.

В этом разделе

Выбор средств администрирования

Определите, какие средства администрирования вы будете использовать для настройки параметров и управления Kaspersky Embedded Systems Security. В качестве средств администрирования Kaspersky Embedded Systems Security вы можете использовать Консоль программы, утилиту командной строки и Консоль администрирования Kaspersky Security Center.

Консоль Kaspersky Embedded Systems Security

Консоль Kaspersky Embedded Systems Security представляет собой самостоятельную оснастку, которая добавляется в Microsoft Management Console. Вы можете управлять Kaspersky Embedded Systems Security через Консоль программы, установленную на защищаемом компьютере или на другом компьютере в сети организации.

Вы можете добавить несколько оснасток Kaspersky Embedded Systems Security в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких компьютеров, на которых установлена программа Kaspersky Embedded Systems Security.

Консоль программы входит в набор компонентов "Средства администрирования".

Утилита командной строки

Вы можете управлять Kaspersky Embedded Systems Security из командной строки защищаемого компьютера.

Утилита командной строки входит в набор программных компонентов Kaspersky Embedded Systems Security.

Kaspersky Security Center

Если вы используете Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации, вы можете управлять Kaspersky Embedded Systems Security через Консоль администрирования Kaspersky Security Center.

Вам потребуется установить следующие компоненты:

- **Модуль интеграции с Агентом администрирования Kaspersky Security Center**. Этот компонент входит в группу программных компонентов Kaspersky Embedded Systems Security. Он позволяет Kaspersky Embedded Systems Security взаимодействовать с Агентом администрирования. Установите модуль интеграции с Агентом администрирования Kaspersky Security Center на защищаемый компьютер.
- **Агент администрирования Kaspersky Security Center**. Установите этот компонент на каждый защищаемый компьютер. Этот компонент будет обеспечивать взаимодействие между программой Kaspersky Embedded Systems Security, установленной на компьютере, и Консолью администрирования Kaspersky Security Center. Файл установки Агента администрирования входит в комплект поставки Kaspersky Security Center.
- **Плагин управления Kaspersky Embedded Systems Security 2.3**. Дополнительно на компьютере, на котором установлен Сервер администрирования Kaspersky Security Center, установите Плагин управления Kaspersky Embedded Systems Security для работы через Консоль администрирования. Плагин обеспечивает интерфейс управления программой через Kaspersky Security Center. Файл установки Плагина управления \product\klcfginst.exe входит в комплект поставки Kaspersky Embedded Systems Security.

Выбор способа установки

После определения программных компонентов для установки Kaspersky Embedded Systems Security (см. раздел "Коды программных компонентов Kaspersky Embedded Systems Security для службы установщика Windows" на стр. 33) нужно выбрать способ установки программы.

Выберите способ установки в зависимости от архитектуры сети и следующих условий:

- потребуется ли вам задать специальные параметры установки Kaspersky Embedded Systems Security или вы будете использовать рекомендуемые параметры установки (см. раздел "Параметры

установки и удаления и ключи командной строки для службы установщика Windows" на стр. 40);

- будут ли параметры установки едиными для всех компьютеров или индивидуальными для каждого компьютера.

Вы можете установить Kaspersky Embedded Systems Security как с помощью мастера установки, так и в режиме без взаимодействия с пользователем, указав параметры установки в командной строке. Вы можете выполнить централизованную удаленную установку Kaspersky Embedded Systems Security: через групповые политики Active Directory или с помощью задачи удаленной установки Kaspersky Security Center.

Вы можете установить и настроить Kaspersky Embedded Systems Security на отдельном компьютере и сохранить его параметры в конфигурационный файл, чтобы затем использовать созданный файл для установки Kaspersky Embedded Systems Security на другие компьютеры. Однако это невозможно при установке программы через групповые политики Active Directory.

Запуск мастера установки

С помощью мастера установки вы можете установить:

- компоненты Kaspersky Embedded Systems Security (см. раздел "Программные компоненты Kaspersky Embedded Systems Security" на стр. 34) на защищаемом компьютере из файла \product\setup.exe, входящего в комплект поставки;
- Консоль Kaspersky Embedded Systems Security (см. раздел "Установка Консоли Kaspersky Embedded Systems Security" на стр. 50) из файла \console\setup.exe, входящего в комплект поставки, на защищаемом компьютере или другом компьютере в локальной сети.

Запуск из командной строки файла инсталляционного пакета с параметрами установки

Запустив файл инсталляционного пакета без ключей, вы установите Kaspersky Embedded Systems Security с параметрами установки по умолчанию. С помощью ключей Kaspersky Embedded Systems Security вы можете изменять параметры установки.

Вы можете установить Консоль программы на защищаемом компьютере или на рабочем месте администратора.

Вы также можете использовать команды для установки Kaspersky Embedded Systems Security и Консоли программы (см. раздел "Установка и удаление программы из командной строки" на стр. 60).

Централизованная установка через Kaspersky Security Center

Если вы используете Kaspersky Security Center для управления антивирусной защитой компьютеров сети, вы можете установить Kaspersky Embedded Systems Security на нескольких компьютерах с помощью задачи удаленной установки.

Компьютеры, на которых вы хотите установить Kaspersky Embedded Systems Security через Kaspersky Security Center (см. раздел "Установка и удаление программы с помощью Kaspersky Security Center" на стр. 65), могут находиться как в одном домене с Kaspersky Security Center, так и в другом домене или вообще не принадлежать ни одному домену.

Централизованная установка через групповые политики Active Directory

С помощью групповых политик Active Directory можно установить Kaspersky Embedded Systems Security на защищаемом компьютере. Вы можете установить Консоль программы на защищаемом компьютере или рабочем месте администратора.

Вы можете установить Kaspersky Embedded Systems Security, используя лишь параметры установки по умолчанию.

Компьютеры, на которых программа Kaspersky Embedded Systems Security установлена с помощью

групповых политик Active Directory (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. 70), должны находиться в том же домене и в том же подразделении организации. Установка выполняется при запуске компьютера, перед входом в Microsoft Windows.

Установка и удаление программы с помощью мастера

В этом разделе описана установка и удаление Kaspersky Embedded Systems Security и Консоли программы с помощью мастера установки, а также приведена информация о дополнительных параметрах Kaspersky Embedded Systems Security и действиях при установке.

В этом разделе

Установка с помощью мастера установки

В следующих разделах содержится информация об установке Kaspersky Embedded Systems Security и Консоли программы.

► *Чтобы установить и начать использовать Kaspersky Embedded Systems Security, выполните следующие действия:*

1. Установите Kaspersky Embedded Systems Security на защищаемом компьютере.
2. На компьютерах, с которых вы планируете управлять Kaspersky Embedded Systems Security, установите Консоль программы.
3. Если вы установили Консоль программы не на защищаемом компьютере, а на другом компьютере сети, выполните дополнительную настройку, чтобы пользователи Консоли программы могли удаленно управлять Kaspersky Embedded Systems Security.
4. Выполните действия после установки Kaspersky Embedded Systems Security.

В этом разделе

Установка Kaspersky Embedded Systems Security

Перед установкой Kaspersky Embedded Systems Security выполните следующие действия:

Убедитесь, что на компьютере не установлены другие антивирусные программы.

- Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на защищаемом компьютере.

После выполнения описанных выше действий, перейдите к процедуре установки. Следуя инструкциям мастера установки, задайте параметры установки Kaspersky Embedded Systems Security. Вы можете прервать установку Kaspersky Embedded Systems Security на любом шаге мастера установки. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Подробнее о параметрах установки (удаления) можно прочитать в разделе "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. 40.

► *Чтобы установить Kaspersky Embedded Systems Security с помощью мастера установки, выполните следующие действия:*

1. На компьютере запустите файл setup.exe.
2. В открывшемся окне в блоке **Установка** перейдите по ссылке **Установить защиту на основе антивирусных баз** или по ссылке **Установить защиту на основе белых списков**.
3. В открывшемся окне приветствия мастера установки Kaspersky Embedded Systems Security нажмите на кнопку **Далее**.

   Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.
4. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности.
5. Если вы согласны с условиями Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки, свидетельствующие, что вы принимаете **положения и условия настоящего Лицензионного соглашения** и **Политику конфиденциальности, которая описывает обработку данных**.

   Если вы не принимаете Лицензионное соглашение и Политику конфиденциальности, установка будет прервана.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Быстрая проверка компьютера перед началом установки**.
7. В окне **Быстрая проверка компьютера перед началом установки** установите флажок **Проверить компьютер на вирусы**, чтобы проверить на наличие угроз системную память и загрузочные секторы локальных дисков компьютера. Нажмите на кнопку **Далее**. По окончании проверки откроется окно с результатами проверки.

   Вы можете просмотреть информацию о проверенных объектах на компьютере: общее количество проверенных объектов, количество обнаруженных угроз, количество обнаруженных зараженных и возможно зараженных объектов, количество опасных или подозрительных процессов, которые программа Kaspersky Embedded Systems Security удалила из памяти, и количество опасных или подозрительных процессов, которые программе не удалось удалить.

   Чтобы посмотреть, какие именно объекты были проверены, нажмите на кнопку **Список обработанных объектов**.

8. В окне **Быстрая проверка компьютера перед началом установки** нажмите на кнопку **Далее**.

   Откроется окно **Выборочная установка**.

9. Выберите компоненты, которые вы хотите установить.

   По умолчанию в список рекомендуемых к установке объектов включены все компоненты Kaspersky Embedded Systems Security, за исключением компонента Управление сетевым экраном.

   > Компонент Поддержка SNMP-протокола отображается в списке устанавливаемых компонентов Kaspersky Embedded Systems Security, только если на компьютере установлена служба Microsoft Windows SNMP.

10. Чтобы отменить все изменения, в окне **Выборочная установка** нажмите на кнопку **Сбросить**. Нажмите на кнопку **Далее**.
11. В окне **Выбор папки назначения** выполните следующие действия:

    - Если требуется, укажите папку, в которой будут сохранены файлы Kaspersky Embedded Systems Security.
    - Если требуется, нажмите на кнопку **Диск** для просмотра информации о доступном пространстве на локальных жестких дисках.

    Нажмите на кнопку **Далее**.

12. В окне **Дополнительные параметры установки** настройте следующие параметры установки:

    - **Включить постоянную защиту после установки программы**
    - **Добавить к исключениям файлы, рекомендованные Microsoft**
    - **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**

      Нажмите на кнопку **Далее**.

13. В окне **Импорт параметров из конфигурационного файла** выполните следующие действия:

    a. Если вы хотите импортировать параметры Kaspersky Embedded Systems Security из существующего конфигурационного файла, созданного в любой предыдущей совместимой версии программы, укажите конфигурационный файл.

    b. Нажмите на кнопку **Далее**.

14. В окне **Активация программы** выполните одно из следующих действий:

    - Если вы хотите активировать программу, укажите файл ключа Kaspersky Embedded Systems Security для активации программы.
    - Если вы хотите активировать программу позже, нажмите на кнопку **Далее**.
    - Если вы предварительно сохранили файл ключа в папке \product комплекта поставки, имя этого файла отобразится в поле **Ключ**.

      > Чтобы добавить ключ с помощью файла ключа, который хранится в другой папке, укажите файл ключа.

      После добавления файла ключа в окне отобразится информация о лицензии. В Kaspersky Embedded Systems Security отображается расчетная дата истечения срока действия лицензии. Срок действия лицензии отсчитывается с момента добавления ключа, а истекает не позднее

даты окончания срока действия файла ключа.

Нажмите на кнопку **Далее**, чтобы добавить файл ключа в программу.

15. В окне **Готовность к установке** нажмите на кнопку **Установить**. Мастер приступит к установке компонентов Kaspersky Embedded Systems Security.
16. По завершении установки откроется окно **Установка завершена**.
17. Установите флажок **Прочитать информацию о релизе**, чтобы просмотреть информацию о версии после завершения работы мастера установки.
18. Нажмите на кнопку **Готово**.

Работа мастера установки будет завершена. По завершении установки Kaspersky Embedded Systems Security будет готов к работе, если вы добавили ключ активации программы.

Установка Консоли Kaspersky Embedded Systems Security

Следуя инструкциям мастера установки, настройте параметры установки Консоли программы. Вы можете прервать установку на любом шаге мастера. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

► *Чтобы установить Консоль программы, выполните следующие действия:*

1. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на компьютере.
2. На компьютере запустите файл setup.exe.

   Откроется окно программы-приветствия.
3. Перейдите по ссылке **Установить Консоль Kaspersky Embedded Systems Security**.

   Откроется окно приветствия мастера установки.
4. Нажмите на кнопку **Далее**.
5. В открывшемся окне ознакомьтесь с условиями Лицензионного соглашения и, чтобы продолжить установку, установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Лицензионного соглашения**.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Дополнительные параметры установки**.
7. В окне **Дополнительные параметры установки** выполните следующие действия:
   - Если вы планируете с помощью Консоли программы управлять программой Kaspersky Embedded Systems Security, установленной на удаленном компьютере, установите флажок **Разрешить удаленный доступ**.
   - Чтобы открыть окно **Выборочная установка** и выбрать компоненты, выполните следующие действия:
     a. Нажмите на кнопку **Дополнительно**.

        Откроется окно **Выборочная установка**.
     b. В списке выберите набор компонентов "Средства администрирования".

        По умолчанию устанавливаются все компоненты.

c. Нажмите на кнопку **Далее**.

> Подробнее о компонентах Kaspersky Embedded Systems Security можно прочитать в разделе "Коды программных компонентов Kaspersky Embedded Systems Security для службы установщика Windows" на стр. 33.

8. В окне **Выбор папки назначения** выполните следующие действия:
   a. Если требуется, укажите другую папку, в которой будут сохранены устанавливаемые файлы.
   b. Нажмите на кнопку **Далее**.
9. В окне **Готовность к установке** нажмите на кнопку **Установить**.

   Мастер приступит к установке выбранных компонентов.
10. Нажмите на кнопку **Готово**.

Работа мастера установки будет завершена. Консоль программы будет установлена на защищаемый компьютер.

Если вы установили набор "Средства администрирования" не на защищаемом компьютере, а на другом компьютере сети, выполните дополнительную настройку (см. раздел "Дополнительная настройка после установки Консоли программы на другом компьютере" на стр. 51).

Дополнительная настройка после установки Консоли программы на другом компьютере

Если вы установили Консоль программы не на защищаемом компьютере, а на другом компьютере сети, выполните следующие действия для того, чтобы пользователи могли удаленно управлять Kaspersky Embedded Systems Security:

- Добавьте пользователей Kaspersky Embedded Systems Security в группу ESS Administrators на защищаемом компьютере.
- Включите сетевые соединения для службы Kaspersky Security Management (kavfsgt.exe) (см. раздел "О правах доступа к службе Kaspersky Security Management" на стр. 233), если на защищаемом компьютере используется брандмауэр Windows или сетевой экран стороннего поставщика.
- Если во время установки Консоли программы на компьютер под управлением Microsoft Windows не был установлен флажок **Разрешить удаленный доступ**, необходимо вручную включить сетевые соединения для Консоли программы через сетевой экран компьютера.

Консоль программы на удаленном компьютере использует протокол DCOM для получения информации о событиях Kaspersky Embedded Systems Security, например, о проверенных объектах или о завершении задач, от службы Kaspersky Security Management на защищаемом компьютере. Необходимо разрешить сетевые соединения для Консоли программы в параметрах брандмауэра Windows, чтобы устанавливать соединения между Консолью программы и службой Kaspersky Security Management.

На удаленном компьютере, на котором установлена Консоль программы, выполните следующие действия:

- Убедитесь, что разрешен анонимный удаленный доступ к программам COM (но не удаленный запуск и активация программ COM).
- В параметрах брандмауэра Windows откройте порт TCP 135 и разрешите сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Embedded Systems Security – kavfsrcn.exe.

Клиентский компьютер, на котором установлена Консоль программы, обменивается информацией с защищаемым компьютером через порт TCP 135.

- Чтобы разрешить подключение, настройте правило исходящего подключения для брандмауэра Windows.

  В отличие от стандартных служб TCP/IP и UDP/IP, где для каждого протокола имеется фиксированный порт, DCOM динамически назначает порты удаленным COM-объектам. Если между клиентским устройством (на котором установлена Консоль программы) и DCOM-устройством (защищаемым компьютером) имеется сетевой экран, вам нужно открыть широкий диапазон портов.

Аналогичные шаги следует выполнить для настройки любого другого программного или аппаратного сетевого экрана.

► *Если Консоль программы открыта во время настройки соединения между защищаемым компьютером и компьютером, на котором установлена Консоль программы, выполните следующие действия:*

1. Закройте Консоль программы.
2. Дождитесь завершения процесса удаленного управления Kaspersky Embedded Systems Security – kavfsrcn.exe.
3. Перезапустите Консоль программы.

   Будут применены новые параметры соединения.

В этом разделе

Разрешение анонимного удаленного доступа к программам COM

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы разрешить анонимный удаленный доступ к программам COM, выполните следующие действия:*

1. На удаленном компьютере, на котором установлена Консоль Kaspersky Embedded Systems Security, откройте консоль Службы компонентов.
2. Выберите **Пуск** → **Выполнить**.
3. Введите команду `dcomcnfg`.
4. Нажмите на кнопку **OK**.

5. В консоли **Службы компонентов** компьютера разверните узел **Компьютеры**.
6. Откройте контекстное меню узла **Мой компьютер**.
7. Выберите пункт **Свойства**.
8. В окне **Свойства** на закладке **Безопасность COM** нажмите на кнопку **Изменить ограничения** в блоке параметров **Права доступа**.
9. В окне **Разрешение на доступ** убедитесь, что для пользователя ANONYMOUS LOGON установлен флажок **Разрешить удаленный доступ**.
10. Нажмите на кнопку **OK**.

Разрешение сетевых соединений для процесса удаленного управления Kaspersky Embedded Systems Security

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы открыть TCP-порт 135 в брандмауэре Windows и разрешить сетевые соединения для процесса удаленного управления Kaspersky Embedded Systems Security, выполните следующие действия:*

1. На удаленном компьютере закройте Консоль Kaspersky Embedded Systems Security.
2. Выполните одно из следующих действий:
   - В Microsoft Windows XP с пакетом обновлений 2 или выше:
     a. Выберите **Пуск** > **Брандмауэр Windows**.
     b. В окне **Брандмауэр Windows** (или Параметры брандмауэра Windows) на закладке **Исключения** нажмите на кнопку **Добавить порт**.
     c. В поле **Имя** укажите имя порта RPC (TCP/135) или задайте другое имя, например, DCOM Kaspersky Embedded Systems Security, а в поле **Номер порта** укажите номер порта: 135.
     d. Выберите протокол **TCP**.
     e. Нажмите на кнопку **OK**.
     f. На закладке **Исключения** нажмите на кнопку **Добавить программу**.
   - В Microsoft Windows 7 и выше:
     a. Выберите **Пуск** > **Панель управления** > **Брандмауэр Windows**.
     b. В окне **Брандмауэр Windows** выберите пункт **Разрешить запуск программы или компонента через брандмауэр Windows**.
     c. В окне **Разрешить связь программ через брандмауэр Windows** нажмите на кнопку **Разрешить другую программу**.
3. В окне **Добавление программы** укажите файл kavfsrcn.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке Консоли Kaspersky Embedded Systems Security с помощью Microsoft Management Console.
4. Нажмите на кнопку **OK**.
5. Нажмите на кнопку **OK** в окне **Брандмауэр Windows (Параметры брандмауэра Windows)**.

Добавление правила исходящего подключения для брандмауэра Windows

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы добавить правило исходящего подключения для брандмауэра Windows, выполните следующие действия:*

1. Выберите **Пуск** > **Панель управления** > **Брандмауэр Windows**.
2. В окне **Брандмауэр Windows** перейдите по ссылке **Дополнительные параметры**.

   Откроется окно **Брандмауэр Windows в режиме повышенной безопасности**.
3. Выберите вложенный узел **Правила для исходящего подключения**.
4. На панели **Действия** выберите пункт **Создать правило**.
5. В открывшемся окне **Мастер создания правила для нового исходящего подключения** выберите параметр **Порт** и нажмите на кнопку **Далее**.
6. Выберите протокол **TCP**.
7. В поле **Определенные удаленные порты** укажите следующий диапазон портов, чтобы разрешить исходящие подключения: 1024–65535.
8. В окне **Действие** выберите пункт **Разрешить подключение**.
9. Сохраните созданное правило и закройте окно **Брандмауэр Windows в режиме повышенной безопасности**.

Брандмауэр Windows не разрешает установку сетевых соединений между Консолью программы и службой Kaspersky Security Management.

Действия после установки Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Embedded Systems Security был установлен флажок **Включить постоянную защиту после установки программы** (по умолчанию), программа проверяет объекты файловой системы компьютера при доступе к ним. Каждую пятницу в 20:00 Kaspersky Embedded Systems Security выполняет задачу Проверка важных областей.

После установки Kaspersky Embedded Systems Security рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз программы. После установки Kaspersky Embedded Systems Security проверяет объекты с использованием баз, которые входили в состав программы при поставке.

  Рекомендуется сразу же обновить базы Kaspersky Embedded Systems Security, так как базы могли устареть.

  Далее программа будет обновлять базы каждый час согласно расписанию, установленному в задаче по умолчанию.

- Выполнить Проверку важных областей, если перед установкой Kaspersky Embedded Systems Security на защищаемом компьютере не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.
- Настроить уведомления администратора о событиях Kaspersky Embedded Systems Security.

В этом разделе

Запуск и настройка задачи Обновление баз программы

► *Чтобы обновить базы программы после установки, выполните следующие действия:*

1. В свойствах задачи обновления баз программы настройте соединение с источником обновлений – HTTP- или FTP-серверами обновлений "Лаборатории Касперского".
2. Запустите задачу Обновление баз программы.

В вашей сети может быть не настроен протокол Web Proxy Auto-Discovery Protocol (WPAD) для автоматического распознавания параметров прокси-сервера в локальной сети. В этом случае может потребоваться проверка подлинности при доступе к прокси-серверу.

► *Чтобы указать дополнительные параметры прокси-сервера и параметры проверки подлинности для доступа к прокси-серверу, выполните следующие действия:*

1. Откройте контекстное меню узла **Kaspersky Security**.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.
3. Выберите закладку **Параметры соединения**.
4. В разделе **Параметры прокси-сервера** установите флажок **Использовать параметры указанного прокси-сервера**.
5. В поле **Адрес** укажите адрес прокси-сервера, а в поле **Порт** укажите номер порта прокси-сервера.
6. В разделе **Параметры аутентификации на прокси-сервере** выберите требуемый метод аутентификации из раскрывающегося списка:
   - **Использовать NTLM-аутентификацию**, если прокси-сервер поддерживает встроенную проверку подлинности Microsoft Windows (NTLM-аутентификацию). Kaspersky Embedded Systems Security будет использовать для доступа к прокси-серверу учетную запись, указанную в параметрах задачи. По умолчанию задача запускается под учетной записью **Локальная система** (**SYSTEM**).
   - **Использовать NTLM-аутентификацию с именем пользователя и паролем**, если прокси-сервер поддерживает встроенную проверку подлинности Microsoft Windows. Kaspersky

Embedded Systems Security будет использовать указанную учетную запись для доступа к прокси-серверу. Введите имя и пароль пользователя или выберите пользователя в списке.

- **Использовать имя пользователя и пароль**, чтобы выбрать обычную проверку подлинности. Введите имя и пароль пользователя или выберите пользователя в списке.

7. В окне **Параметры программы** нажмите на кнопку **OK**.

► *Чтобы настроить соединение с серверами обновлений "Лаборатории Касперского" в задаче обновления баз программы, выполните следующие действия:*

1. Запустите Консоль программы одним из следующих способов:
   - Откройте Консоль программы на защищаемом компьютере. Для этого в меню **Пуск** выберите **Все программы**> **Kaspersky Embedded Systems Security** > **Средства администрирования** > **Консоль Kaspersky Embedded Systems Security 2.3**.
   - Если Консоль программы запущена не на защищаемом компьютере, подключитесь к защищаемому компьютеру:
     a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security**.
     b. Выберите пункт **Подключиться к другому компьютеру**.
     c. В окне **Выбор компьютера** выберите вариант **Другой компьютер** и в поле ввода укажите сетевое имя защищаемого компьютера.

   Если учетная запись, которую вы использовали для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management (см. раздел "О правах доступа к службе Kaspersky Security Management" на стр. 233), укажите учетную запись, которая обладает этими правами.

   Откроется окно Консоли программы.
2. В дереве Консоли программы разверните узел **Обновление**.
3. Выберите вложенный узел **Обновление баз программы**.
4. В панели результатов перейдите по ссылке **Свойства**.
5. В открывшемся окне **Параметры задачи** выберите закладку **Параметры соединения**.
6. Выберите **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.
7. В окне **Параметры задачи** нажмите на кнопку **OK**.

Параметры соединения с источником обновлений в задаче Обновление баз программы будут сохранены.

► *Чтобы запустить задачу Обновление баз программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. В контекстном меню вложенного узла **Обновление баз программы** выберите пункт **Запустить**.

Задача Обновление баз программы будет запущена.

После успешного завершения задачи можно посмотреть дату выпуска последних установленных обновлений баз в панели результатов узла **Kaspersky Security**.

Проверка важных областей

После того как вы обновили базы Kaspersky Embedded Systems Security, проверьте компьютер на наличие вредоносных программ с помощью задачи Проверка важных областей.

► *Чтобы запустить задачу Проверка важных областей, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. В контекстном меню вложенного узла **Проверка важных областей** выберите команду **Запустить**.

Задача будет запущена; в панели результатов отобразится статус задачи **Выполняется**.

► *Чтобы просмотреть журнал выполнения задачи,*

в панели результатов узла **Проверка важных областей** перейдите по ссылке **Открыть журнал выполнения**.

Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security

Вы можете добавлять или удалять компоненты Kaspersky Embedded Systems Security. Вам нужно предварительно остановить задачу Постоянная защита файлов, если вы хотите удалить компонент Постоянная защита файлов. В остальных случаях останавливать задачу Постоянная защита файлов или службу Kaspersky Security не требуется.

Если доступ к управлению программой защищен паролем, Kaspersky Embedded Systems Security запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов в мастере установки.

► *Чтобы изменить состав компонентов Kaspersky Embedded Systems Security, выполните следующие действия:*

1. В меню **Пуск** выберите **Все программы** > **Kaspersky Embedded Systems Security** > **Изменение или удаление Kaspersky Embedded Systems Security**.

   Откроется окно мастера установки программы **Изменение, восстановление или удаление**.
2. Выберите **Изменение состава компонентов программы**. Нажмите на кнопку **Далее**.

   Откроется окно **Выборочная установка**.
3. В списке доступных компонентов в окне **Выборочная установка** выберите компоненты, которые требуется добавить или удалить из состава Kaspersky Embedded Systems Security. Для этого выполните следующие действия:
   - Чтобы изменить состав компонентов, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите:
     - пункт **Компонент будет установлен на локальный жесткий диск**, если требуется установить отдельный компонент;
     - пункт **Компонент и его подкомпоненты будут установлены на локальный жесткий диск**, если требуется установить группу компонентов.

- Чтобы удалить установленные ранее компоненты, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите пункт **Компонент будет недоступен**.

Нажмите на кнопку **Далее**.

4. В окне **Готовность к установке** подтвердите изменение состава компонентов программы, нажав на кнопку **Установить**.
5. В окне, открывшемся по завершении установки, нажмите на кнопку **ОК**.

Состав компонентов Kaspersky Embedded Systems Security будет изменен в соответствии с заданными параметрами.

Если в работе Kaspersky Embedded Systems Security возникли проблемы (Kaspersky Embedded Systems Security завершается аварийно, задачи завершаются аварийно или не запускаются), можно попробовать восстановить Kaspersky Embedded Systems Security. Вы можете выполнить восстановление с сохранением текущих значений параметров Kaspersky Embedded Systems Security или выбрать режим, при котором все параметры Kaspersky Embedded Systems Security примут значения по умолчанию.

► *Чтобы восстановить Kaspersky Embedded Systems Security после аварийного завершения работы программы или задач, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы**.
2. Выберите **Kaspersky Embedded Systems Security**.
3. Выберите **Изменение или удаление Kaspersky Embedded Systems Security**.

   Откроется окно мастера установки программы **Изменение, восстановление или удаление**.
4. Выберите вариант **Восстановление установленных компонентов**. Нажмите на кнопку **Далее**.

   Откроется окно **Восстановление установленных компонентов**.
5. В окне **Восстановление установленных компонентов** установите флажок **Восстановить рекомендуемые параметры работы программы**, если вы хотите сбросить параметры программы и восстановить Kaspersky Embedded Systems Security с параметрами по умолчанию. Нажмите на кнопку **Далее**.
6. В окне **Готовность к восстановлению** подтвердите операцию восстановления программы, нажав на кнопку **Установить**.
7. В окне, открывшемся по завершении операции восстановления, нажмите на кнопку **ОК**.

Программа Kaspersky Embedded Systems Security будет восстановлена с указанными параметрами.

Удаление с помощью мастера установки

В этом разделе приведены инструкции по удалению Kaspersky Embedded Systems Security и Консоли программы с защищаемого компьютера с помощью мастера установки / удаления.

В этом разделе

Удаление Kaspersky Embedded Systems Security

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Kaspersky Embedded Systems Security с защищаемого компьютера с помощью мастера установки / удаления.

После удаления Kaspersky Embedded Systems Security с защищаемого компьютера может потребоваться перезагрузка. Перезагрузку можно отложить.

Удаление, восстановление и установка программы через панель управления Windows невозможна, если операционная система использует функцию Контроль учетных записей (User Account Control) или если доступ к управлению программой защищен паролем.

Если доступ к управлению программой защищен паролем, Kaspersky Embedded Systems Security запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов в мастере установки.

► *Чтобы удалить Kaspersky Embedded Systems Security, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы**.
2. Выберите **Kaspersky Embedded Systems Security**.
3. Выберите **Изменение или удаление Kaspersky Embedded Systems Security**.

   Откроется окно мастера установки программы **Изменение, восстановление или удаление**.
4. Выберите пункт **Удаление компонентов программы**. Нажмите на кнопку **Далее**.

   Откроется окно **Дополнительные параметры удаления программы**.
5. Если требуется, в окне **Дополнительные параметры удаления программы** выполните следующие действия:
   a. Установите флажок **Экспортировать объекты на карантине**, чтобы программа Kaspersky Embedded Systems Security экспортировала объекты, помещенные на карантин. По умолчанию флажок снят.
   b. Установите флажок **Экспортировать объекты резервного хранилища**, чтобы экспортировать объекты из резервного хранилища Kaspersky Embedded Systems Security. По умолчанию флажок снят.
   c. Нажмите на кнопку **Сохранить в** и укажите папку, в которую требуется экспортировать объекты. По умолчанию экспорт объектов осуществляется в папку %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall.

      Нажмите на кнопку **Далее**.
6. В окне **Готовность к удалению** подтвердите удаление, нажав на кнопку **Удалить**.

7. В окне, открывшемся по завершении удаления, нажмите на кнопку **OK**.

Программа Kaspersky Embedded Systems Security будет удалена с защищаемого компьютера.

Удаление Консоли Kaspersky Embedded Systems Security

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Консоль программы с компьютера с помощью мастера установки / удаления.

После удаления Консоли программы перезагрузка компьютера не требуется.

► *Чтобы удалить Консоль программы, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы**.
2. Выберите **Kaspersky Embedded Systems Security**.
3. Выберите **Изменение или удаление Средств администрирования Kaspersky Embedded Systems Security 2.3**.

   Откроется окно мастера **Изменение, восстановление или удаление**.
4. Выберите пункт **Удаление компонентов программы** и нажмите на кнопку **Далее**.
5. Откроется окно **Готовность к удалению**. Нажмите на кнопку **Удалить**.

   Откроется окно **Удаление завершено**.
6. Нажмите на кнопку **OK**.

Операция удаления будет завершена; окно мастера установки будет закрыто.

Установка и удаление программы из командной строки

Этот раздел содержит описание особенностей установки и удаления Kaspersky Embedded Systems Security из командной строки, примеры команд для установки и удаления Kaspersky Embedded Systems Security из командной строки, примеры команд для добавления и удаления компонентов Kaspersky Embedded Systems Security из командной строки.

В этом разделе

Об установке и удалении Kaspersky Embedded Systems Security из командной строки

Вы можете устанавливать и удалять Kaspersky Embedded Systems Security, добавлять или удалять компоненты, запустив из командной строки файлы пакета установки \product\ess_x86(x64).msi и указав параметры установки с помощью ключей.

Вы можете установить набор "Средства администрирования" на защищаемом компьютере или другом компьютере в сети, чтобы работать с Консолью программы локально или удаленно. Для этого используйте пакет установки \console\esstools.msi.

Выполняйте установку с правами учетной записи, входящей в группу администраторов на компьютере, на котором установлена программа.

Если вы запустите на защищаемом компьютере один из файлов \product\ess_x86.msi или \product\ess_x64.msi без дополнительных ключей, программа Kaspersky Embedded Systems Security будет установлена с рекомендуемыми параметрами установки.

Вы можете задать набор устанавливаемых компонентов с помощью ключа ADDLOCAL, перечислив в качестве его значений коды выбранных компонентов или наборов компонентов.

Примеры команд установки Kaspersky Embedded Systems Security

В этом разделе приводятся примеры команд для установки Kaspersky Embedded Systems Security.

На компьютере под управлением Microsoft Windows 32-разрядной версии запускайте файлы с суффиксом x86 из комплекта поставки. На компьютере под управлением Microsoft Windows 64-разрядной версии запускайте файлы с суффиксом x64 из комплекта поставки.

Подробная информация об использовании стандартных команд и ключей установщика Windows содержится в документации, предоставляемой корпорацией Microsoft.

Примеры установки Kaspersky Embedded Systems Security из файла setup.exe

► *Чтобы установить Kaspersky Embedded Systems Security с параметрами по умолчанию без взаимодействия с пользователем, выполните следующую команду:*

```
\product\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

Можно установить Kaspersky Embedded Systems Security со следующими параметрами:

- установить только компоненты Постоянная защита файлов и Проверка по требованию;
- не запускать Постоянную защиту файлов при запуске Kaspersky Embedded Systems Security;
- не исключать из проверки файлы, рекомендованные к исключению корпорацией Microsoft.

Для этого выполните следующую команду:

```
\product\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

Примеры команд для установки: запуск msi-файла

- *Чтобы установить Kaspersky Embedded Systems Security с параметрами по умолчанию без взаимодействия с пользователем, выполните следующую команду:*

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

- *Чтобы установить Kaspersky Embedded Systems Security с параметрами по умолчанию и показать интерфейс установки, выполните следующую команду:*

```
msiexec /i ess.msi /qf EULA=1 PRIVACYPOLICY=1
```

- *Чтобы установить Kaspersky Embedded Systems Security и активировать его с помощью файла ключа C:\0000000A.key, выполните следующую команду:*

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1
PRIVACYPOLICY=1
```

- *Чтобы установить Kaspersky Embedded Systems Security с предварительной проверкой активных процессов и загрузочных секторов локальных дисков, выполните следующую команду:*

```
msiexec /i ess.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

- *Чтобы установить Kaspersky Embedded Systems Security в папку установки C:\ESS, выполните следующую команду:*

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

- *Чтобы установить Kaspersky Embedded Systems Security и сохранить файл журнала установки с именем ess.log в папку, где хранится msi-файл Kaspersky Embedded Systems Security, выполните следующую команду:*

```
msiexec /i ess.msi /l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

- *Чтобы установить Консоль Kaspersky Embedded Systems Security, выполните следующую команду:*

```
msiexec /i esstools.msi /qn EULA=1
```

- *Чтобы установить и активировать Kaspersky Embedded Systems Security с помощью файла ключа C:\0000000A.key, а также настроить Kaspersky Embedded Systems Security в соответствии с параметрами в конфигурационном файле C:\settings.xml, выполните следующую команду:*

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key
CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

► *Чтобы установить исправление программы, если Kaspersky Embedded Systems Security защищен паролем, выполните следующую команду:*

```
msiexec /p "<msp путь к имени файла>" UNLOCK_PASSWORD=<пароль>
```

Действия после установки Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Embedded Systems Security был установлен флажок **Включить постоянную защиту после установки программы**, программа проверяет объекты файловой системы компьютера при доступе к ним. Каждую пятницу в 20:00 Kaspersky Embedded Systems Security выполняет задачу Проверка важных областей.

После установки Kaspersky Embedded Systems Security рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз Kaspersky Embedded Systems Security. После установки Kaspersky Embedded Systems Security проверяет объекты с использованием баз, которые входили в его состав при поставке. Рекомендуется сразу же обновить базы Kaspersky Embedded Systems Security. Для этого вам нужно запустить задачу Обновление баз программы. Далее обновление баз будет выполняться каждый час согласно расписанию, установленному по умолчанию.

  Например, вы можете запустить задачу Обновление баз программы, выполнив следующую команду:

  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456

  При этом обновления баз Kaspersky Embedded Systems Security будут загружены с серверов обновлений "Лаборатории Касперского". Соединение с источником обновлений происходит через прокси-сервер (адрес прокси-сервера: proxy.company.com, порт: 8080) с использованием для доступа к серверу встроенной проверки подлинности Microsoft Windows (NTLM-authentication) с учетной записью (имя пользователя: inetuser; пароль: 123456).

- Выполнить Проверку важных областей на компьютере, если перед установкой Kaspersky Embedded Systems Security на защищаемом компьютере не было установлено антивирусной программы с функцией постоянной защиты файлов.

► *Чтобы выполнить задачу Проверка важных областей с помощью командной строки, выполните следующую команду:*

  KAVSHELL SCANCRITICAL /W:scancritical.log

  Эта команда сохраняет журнал выполнения задачи в файле scancritical.log в текущей папке.

- Настроить уведомления администратора о событиях Kaspersky Embedded Systems Security.

Добавление и удаление компонентов. Примеры команд

Компонент Проверка по требованию устанавливается автоматически. Вам не нужно указывать его в списке значений ключа ADDLOCAL, добавляя или удаляя компоненты Kaspersky Embedded Systems Security.

► *Чтобы добавить компонент Контроль запуска программ к ранее установленным компонентам, выполните следующую команду:*

```
msiexec /i ess.msi ADDLOCAL=Oas,AppCtrl /qn
```

или

```
\product\setup.exe /s /p "ADDLOCAL=Oas,AppCtrl"
```

Если вы перечислите не только компоненты, которые требуется установить, но и уже установленные компоненты, Kaspersky Embedded Systems Security переустановит указанные установленные компоненты.

► *Чтобы удалить установленные компоненты, выполните следующую команду:*

```
msiexec /i ess.msi
"ADDLOCAL=Oas,Ods,Ksn,AntiExploit,DevCtrl,Firewall,AntiCryptor,LogInspecto
r,AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVProtection,Ram
Disk REMOVE=AppCtrl,Fim" /qn
```

Удаление Kaspersky Embedded Systems Security. Примеры команд

► *Чтобы удалить Kaspersky Embedded Systems Security с защищаемого компьютера, выполните следующую команду:*

```
msiexec /x ess.msi /qn
```

или

- Для 32-разрядной операционной системы:

```
msiexec /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} /qn
```

- Для 64-разрядной операционной системы:

```
msiexec /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} /qn
```

► *Чтобы удалить Консоль Kaspersky Embedded Systems Security, выполните следующую команду:*

```
msiexec /x esstools.msi /qn
```

или

- Для 32-разрядной операционной системы:

```
msiexec /x {26E7C356-E535-4434-9AB1-F1EA4E8A70F4} /qn
```

- Для 64-разрядной операционной системы:

```
msiexec /x {7EC1A40D-52F4-4F8F-93BA-F6E68B152C26} /qn
```

► *Чтобы удалить Kaspersky Embedded Systems Security с защищаемого компьютера, на котором установлен пароль, выполните следующую команду:*

- Для 32-разрядной операционной системы:

```
msiexec /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} UNLOCK_PASSWORD=*** /qn
```

- Для 64-разрядной операционной системы:

```
msiexec /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} UNLOCK_PASSWORD=*** /qn
```

Коды возврата

В таблице ниже приведено описание кодов возврата командной строки.

Таблица 6. Коды возврата

Код	Описание
1324	Имя папки назначения содержит недопустимые символы.
25001	Недостаточно прав для установки Kaspersky Embedded Systems Security. Чтобы установить программу, запустите мастер установки с правами локального администратора.
25003	Kaspersky Embedded Systems Security не может быть установлен на компьютер под управлением этой версии Microsoft Windows. Пожалуйста, запустите мастер установки программы, предназначенный для 64-разрядной версии Microsoft Windows.
25004	Обнаружено несовместимое программное обеспечение. Чтобы продолжить установку, удалите следующее программное обеспечение: <список несовместимого программного обеспечения>.
25010	Указанный путь не может быть использован для сохранения объектов на карантине.
25011	Имя папки для сохранения объектов на карантине содержит недопустимые символы.
26251	Не удалось загрузить DLL для Счетчиков производительности.
26252	Не удалось загрузить DLL для Счетчиков производительности.
27300	Драйвер не может быть установлен.
27301	Драйвер не может быть удален.
27302	Невозможно установить сетевой компонент. Достигнуто максимальное пороговое значение поддерживаемого количества устройств фильтрации.
27303	Антивирусные базы не найдены.

Установка и удаление программы через Kaspersky Security Center

Этот раздел содержит информацию об установке Kaspersky Embedded Systems Security через Kaspersky Security Center, описание процедуры установки и удаления Kaspersky Embedded Systems Security через Kaspersky Security Center, а также описание действий после установки Kaspersky Embedded Systems Security.

В этом разделе

Общие сведения об установке через Kaspersky Security Center

Вы можете установить Kaspersky Embedded Systems Security через Kaspersky Security Center с помощью задачи удаленной установки.

После выполнения задачи удаленной установки программа Kaspersky Embedded Systems Security будет установлена с одинаковыми параметрами на нескольких компьютерах.

Вы можете объединить все компьютеры в одну группу администрирования и создать групповую задачу установки Kaspersky Embedded Systems Security на компьютеры этой группы.

Вы можете создать задачу удаленной установки Kaspersky Embedded Systems Security для набора компьютеров, не объединенных в одну группу администрирования. При создании этой задачи вам нужно сформировать список отдельных компьютеров, на которые вы хотите установить Kaspersky Embedded Systems Security.

Подробная информация о задаче удаленной установки приведена в *Справке Kaspersky Security Center*.

Права для установки или удаления Kaspersky Embedded Systems Security

Учетная запись, которую вы укажете в задаче удаленной установки (удаления), должна входить в группу администраторов на каждом из защищаемых компьютеров во всех случаях, кроме следующих ситуаций:

- На компьютерах, на которых требуется установить Kaspersky Embedded Systems Security, уже установлен Агент администрирования Kaspersky Security Center (независимо от того, в каком домене находятся компьютеры и принадлежат ли они к какому-либо домену).

  Если Агент администрирования еще не установлен на компьютерах, вы можете установить его вместе с Kaspersky Embedded Systems Security с помощью задачи удаленной установки. Перед установкой Агента администрирования убедитесь, что учетная запись, которую вы укажете в задаче, входит в группу администраторов на каждом компьютере.

- Все компьютеры, на которые вы хотите установить Kaspersky Embedded Systems Security, находятся в одном домене с Сервером администрирования, а Сервер администрирования зарегистрирован под учетной записью **Администратор домена** (Domain Admin), если эта учетная запись обладает правами локального администратора на компьютерах домена.

По умолчанию задача удаленной установки методом **Форсированная установка** запускается с правами той учетной записи, под которой работает Сервер администрирования.

В групповых задачах и в задачах для набора компьютеров, в которых был выбран метод форсированной установки (удаления), учетная запись должна обладать следующими правами на клиентском компьютере:

- правом на удаленный запуск программ;
- доступом к папке общего доступа **Admin$**;
- правом **Вход в качестве службы**.

Установка Kaspersky Embedded Systems Security через Kaspersky Security Center

Подробная информация о формировании инсталляционного пакета и создании задачи удаленной установки содержится в Руководстве по внедрению Kaspersky Security Center.

Если вы планируете в дальнейшем управлять Kaspersky Embedded Systems Security через Kaspersky Security Center, убедитесь, что выполняются следующие условия:

- На компьютере с установленным Сервером администрирования Kaspersky Security Center также установлен Плагин управления (файл \product\klcfginst.exe комплекта поставки Kaspersky Embedded Systems Security).
- На защищаемых компьютерах установлен Агент администрирования Kaspersky Security Center. Если на защищаемых компьютерах не установлен Агент администрирования Kaspersky Security Center, его можно установить вместе с Kaspersky Embedded Systems Security с помощью задачи удаленной установки.

Можно также объединить компьютеры в группу администрирования, чтобы в дальнейшем управлять параметрами защиты с помощью политик и групповых задач Kaspersky Security Center.

► *Чтобы установить Kaspersky Embedded Systems Security с помощью задачи удаленной установки, выполните следующие действия:*

1. Запустите Консоль администрирования Kaspersky Security Center.
2. В Kaspersky Security Center разверните узел **Дополнительно**.
3. Разверните вложенный узел **Удаленная установка**.
4. В рабочей области узла **Инсталляционные пакеты** нажмите на кнопку **Создать инсталляционный пакет**.
5. Выберите вариант **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
6. Введите имя инсталляционного пакета.
7. Выберите файл `ess`.kud из комплекта установки Kaspersky Embedded Systems Security в качестве файла инсталляционного пакета.

   Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.
8. Если вы согласны с условиями Лицензионного соглашения и Политики конфиденциальности, для

продолжения установки установите флажки, свидетельствующие, что вы принимаете **положения и условия настоящего Лицензионного соглашения** и **Политику конфиденциальности, которая описывает обработку данных**.

Вам нужно принять условия Лицензионного соглашения и Политики конфиденциальности для продолжения установки.

9. Чтобы изменить набор устанавливаемых компонентов Kaspersky Embedded Systems Security (см. раздел "Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security" на стр. 57) и параметры установки по умолчанию (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows " на стр. 40) в инсталляционном пакете, выполните следующие действия:
   a. В Kaspersky Security Center разверните узел **Удаленная установка**.
   b. В панели результатов вложенного узла **Инсталляционные пакеты** откройте контекстное меню созданного инсталляционного пакета Kaspersky Embedded Systems Security и выберите пункт **Свойства**.
   c. В окне **Свойства: <название инсталляционного пакета>** в разделе **Настройка** выполните следующие действия:
      a. В группе параметров **Устанавливаемые компоненты** установите флажки рядом с названиями компонентов Kaspersky Embedded Systems Security, которые вы хотите установить.
      b. Чтобы указать папку назначения, отличную от папки, установленной по умолчанию, укажите имя папки и путь к ней в поле **Папка назначения**.

         Путь к папке назначения может содержать системные переменные окружения. Если указанной папки не существует на компьютере, она будет создана.
      c. В группе параметров **Дополнительные параметры установки** настройте следующие параметры:
         - **Выполнить антивирусную проверку компьютера перед началом установки**
         - **Включить постоянную защиту после установки программы**
         - **Добавить к исключениям файлы, рекомендованные Microsoft**
      d. **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**
   d. В диалоговом окне **Свойства: <название инсталляционного пакета>** нажмите на кнопку **ОК**.
10. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Kaspersky Embedded Systems Security на выбранные компьютеры (группу администрирования). Настройте параметры задачи.

    Подробная информация о создании и настройке задачи удаленной установки содержится в *Справке Kaspersky Security Center*.
11. Запустите задачу удаленной установки Kaspersky Embedded Systems Security.

Программа Kaspersky Embedded Systems Security будет установлена на указанные в задаче компьютеры.

Действия после установки Kaspersky Embedded Systems Security

После установки Kaspersky Embedded Systems Security рекомендуется обновить базы Kaspersky Embedded Systems Security на компьютерах, а также выполнить задачу Проверка важных областей, если до установки Kaspersky Embedded Systems Security на компьютерах не были установлены антивирусные программы с включенной функцией постоянной защиты.

Если компьютеры, на которых установлена программа Kaspersky Embedded Systems Security, объединены в одну группу администрирования в Kaspersky Security Center, можно выполнить эти задачи следующими способами:

1. Создать задачи обновления баз программы для группы компьютеров, на которых установлена программа Kaspersky Embedded Systems Security. Установить Сервер администрирования Kaspersky Security Center в качестве источника обновлений.
2. Создать групповую задачу проверки по требованию со статусом Проверка важных областей. Kaspersky Security Center оценивает состояние безопасности каждого компьютера группы по результатам выполнения этой задачи, а не по результатам задачи Проверка важных областей.
3. Создать новую политику для группы компьютеров. В свойствах политики в разделе **Параметры программы** выключить запуск по расписанию системных задач проверки по требованию и задачи Обновление баз программы на компьютерах группы администрирования в подразделе **Запуск системных задач**.

Вы можете также настроить уведомления администратора о событиях Kaspersky Embedded Systems Security.

Установка Консоли программы через Kaspersky Security Center

Подробная информация о создании инсталляционного пакета и задачи удаленной установки содержится в Руководстве по внедрению Kaspersky Security Center.

► *Чтобы установить Консоль программы с помощью задачи удаленной установки, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center разверните узел **Дополнительно**.
2. Разверните вложенный узел **Удаленная установка**.
3. В рабочей области узла Инсталляционные пакеты нажмите на кнопку **Создать инсталляционный пакет**. При создании нового инсталляционного пакета:
   a. В окне **Мастер создания инсталляционного пакета** выберите пункт **Создать инсталляционный пакет** для указанного исполняемого файла в качестве типа пакета.
   b. Введите имя инсталляционного пакета.
   c. В папке комплекта поставки Kaspersky Embedded Systems Security выберите файл \console\setup.exe и установите флажок **Копировать всю папку в инсталляционный пакет**.
   d. Если требуется, с помощью ключа командной строки ADDLOCAL измените состав устанавливаемых компонентов в поле **Параметры запуска исполняемого файла (необязательно)** и папку назначения.

      Например, чтобы установить только Консоль программы в папку C:\KasperskyConsole, не

устанавливая файлы справки и документации, используйте следующие ключи командной строки:

```
/s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
```

4. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Консоли программы на выбранные компьютеры (группу администрирования). Настройте параметры задачи.

   Подробная информация о создании и настройке задач удаленной установки содержится в Справке Kaspersky Security Center.

5. Запустите задачу удаленной установки.

Консоль программы будет установлена на указанные в задаче компьютеры.

Удаление Kaspersky Embedded Systems Security через Kaspersky Security Center

Если доступ к управлению Kaspersky Embedded Systems Security на компьютерах сети защищен паролем, введите пароль при создании задачи удаления нескольких программ. Если защита паролем не управляется политикой Kaspersky Security Center централизованно, программа Kaspersky Embedded Systems Security будет успешно удалена с защищаемых компьютеров, где доступ к управлению программой защищен паролем, совпавшим с введенным значением. Kaspersky Embedded Systems Security не будет удален с других компьютеров.

► *Чтобы удалить Kaspersky Embedded Systems Security в Консоли администрирования Kaspersky Security Center, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center создайте и запустите задачу удаления программы.
2. В задаче выберите метод удаления (аналогично выбору метода установки, см. предыдущий раздел) и укажите учетную запись, с правами которой Сервер администрирования будет обращаться к компьютерам. Вы можете удалить Kaspersky Embedded Systems Security только с параметрами удаления по умолчанию (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. 40).

Установка и удаление программы через групповые политики Active Directory

Этот раздел содержит описание установки и удаления Kaspersky Embedded Systems Security через групповые политики Active Directory, а также информацию о действиях, которые требуется выполнить после установки Kaspersky Embedded Systems Security через групповые политики.

В этом разделе

Установка Kaspersky Embedded Systems Security через групповые политики Active Directory

Вы можете установить Kaspersky Embedded Systems Security на несколько компьютеров через групповую политику Active Directory. Консоль программы можно установить аналогичным образом.

Компьютеры, на которые вы хотите установить Kaspersky Embedded Systems Security или Консоль программы, должны быть в одном домене и в одной организационной единице.

Операционные системы компьютеров, на которые вы хотите установить Kaspersky Embedded Systems Security с помощью политики, должны быть одной разрядности (32-разрядные или 64-разрядные).

Вы должны обладать правами администратора домена.

Чтобы установить Kaspersky Embedded Systems Security, используйте инсталляционные пакеты `ess`_x86(x64).msi. Чтобы установить Консоль программы, используйте инсталляционные пакеты `ess`tools.msi.

Подробная информация об использовании групповых политик Active Directory содержится в документации, предоставляемой корпорацией Microsoft.

► *Чтобы установить Kaspersky Embedded Systems Security (Консоль программы), выполните следующие действия:*

1. Сохраните msi-файл, соответствующий разрядности установленной версии операционной системы Microsoft Windows, в папку общего доступа на контроллере домена.
2. Сохраните файл ключа (см. раздел "О файле ключа" на стр. 80) в эту же папку общего доступа на контроллере домена.
3. В этой же папке общего доступа на контроллере домена создайте файл install_props.json, содержащий приведенные ниже строки. Это означает, что вы соглашаетесь с условиями Лицензионного соглашения и Политики конфиденциальности.

```
{
"EULA": "1",
"PRIVACYPOLICY": "1"
}
```

4. На контроллере домена создайте новую политику для группы, к которой принадлежат компьютеры.
5. С помощью **Редактора объектов групповых политик** создайте новый инсталляционный пакет в

узле **Конфигурация компьютеров**. Укажите путь к msi-файлу Kaspersky Embedded Systems Security или Консоли программы в формате UNC (Universal Naming Convention).

6. Установите флажок установщика Windows **Всегда устанавливать с повышенными правами** как в узле **Конфигурация компьютеров**, так и в узле **Конфигурация пользователей** выбранной группы.
7. Примените изменения с помощью команды `gpupdate / force`.

Программа Kaspersky Embedded Systems Security будет установлена на компьютерах группы после их перезагрузки.

Действия после установки Kaspersky Embedded Systems Security

После установки Kaspersky Embedded Systems Security на защищаемые компьютеры рекомендуется сразу обновить базы программы и выполнить Проверку важных областей. Вы можете выполнить эти действия из Консоли программы (см. Раздел "Действия после установки Kaspersky Embedded Systems Security" на стр. 54).

Вы можете также настроить уведомления администратора о событиях Kaspersky Embedded Systems Security.

Удаление Kaspersky Embedded Systems Security через групповые политики Active Directory

Если вы установили Kaspersky Embedded Systems Security или Консоль программы на компьютерах группы, используя групповую политику Active Directory, вы можете использовать эту политику, чтобы удалить Kaspersky Embedded Systems Security или Консоль программы.

Вы можете удалить программу только с параметрами удаления по умолчанию.

Подробная информация об использовании групповых политик Active Directory содержится в документации, предоставляемой корпорацией Microsoft.

Если доступ к управлению программой защищен паролем, удаление Kaspersky Embedded Systems Security через групповые политики Active Directory невозможно.

► *Чтобы удалить Kaspersky Embedded Systems Security (или Консоль программы), выполните следующие действия:*

1. На контроллере домена выберите организационную единицу, с компьютеров которой требуется удалить Kaspersky Embedded Systems Security или Консоль программы.
2. Выберите политику, созданную для установки Kaspersky Embedded Systems Security, и в **Редакторе объектов групповых политик**, в узле **Установка программ** (**Конфигурация компьютеров** > **Параметры программ** > **Установка программ**) откройте контекстное меню инсталляционного пакета Kaspersky Embedded Systems Security (Консоли программы) и выберите команду **Все задачи > Удалить**.

3. Выберите метод удаления **Немедленно удалить программы из учетных записей пользователей и компьютеров**.
4. Примените изменения с помощью команды `gpupdate / force`.

Программа Kaspersky Embedded Systems Security будет удалена с компьютеров после их перезагрузки, перед входом в Microsoft Windows.

Проверка функций Kaspersky Embedded Systems Security. Использование тестового вируса EICAR

В этом разделе описан тестовый вирус EICAR и его использование для проверки функций постоянной защиты и проверки по требованию Kaspersky Embedded Systems Security.

В этом разделе

О тестовом вирусе EICAR

Тестовый вирус предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Тестовый вирус не является вредоносным объектом и не содержит исполняемого кода, который может нанести вред вашему компьютеру, но антивирусные программы большинства производителей идентифицируют его как угрозу.

Файл, который содержит тестовый вирус, называется eicar.com. Его можно загрузить на веб-сайте EICAR http://www.eicar.org/anti_virus_test_file.htm.

Перед сохранением файла в папку на жестком диске компьютера убедитесь, что Постоянная защита файлов выключена для этого жесткого диска.

Файл eicar.com содержит текстовую строку. При проверке файла Kaspersky Embedded Systems Security обнаруживает в этой текстовой строке тестовую угрозу, присваивает файлу статус **Зараженный или обнаруживаемый** и удаляет его. Информация об обнаруженной в файле угрозе появляется в Консоли программы и в журнале выполнения задачи.

Вы также можете использовать файл eicar.com, чтобы проверять, как Kaspersky Embedded Systems Security выполняет лечение зараженных объектов и как он обнаруживает возможно зараженные объекты. Для этого откройте файл с помощью текстового редактора, добавьте к началу текстовой строки в файле один из

префиксов, перечисленных в таблице ниже, и сохраните файл с новым именем, например, eicar_cure.com.

Чтобы убедиться, что Kaspersky Embedded Systems Security обрабатывает файл eicar.com с префиксом, в блоке параметров безопасности **Защита объектов** установите значение **Все объекты** для задачи Постоянная защита файлов и для задач проверки по требованию Kaspersky Embedded Systems Security.

Таблица 7. Префиксы в файлах EICAR

Префикс	Статус файла после проверки и действие Kaspersky Embedded Systems Security
Без префикса	Kaspersky Embedded Systems Security присваивает объекту статус **Зараженный или обнаруживаемый** и удаляет его.
SUSP–	Kaspersky Embedded Systems Security присваивает статус **Возможно зараженный** объекту, обнаруженному с помощью эвристического анализатора, и удаляет его, поскольку возможно зараженные объекты не подвергаются лечению.
WARN–	Kaspersky Embedded Systems Security присваивает статус **Возможно зараженный** объекту, если код объекта частично совпадает с кодом известной угрозы, и удаляет его, поскольку возможно зараженные объекты не подвергаются лечению.
CURE–	Kaspersky Embedded Systems Security присваивает объекту статус **Зараженный или обнаруживаемый** и лечит его. Если лечение успешно, весь текст в файле заменяется словом "CURE".

Проверка функций постоянной защиты и проверки по требованию

После установки Kaspersky Embedded Systems Security вы можете убедиться, что Kaspersky Embedded Systems Security обнаруживает объекты, содержащие вредоносный код. Для проверки можно использовать тестовый вирус EICAR (см. раздел "О тестовом вирусе EICAR" на стр. 73).

► *Чтобы проверить функцию постоянной защиты, выполните следующие действия:*

1. Загрузите файл eicar.com с веб-сайта EICAR http://www.eicar.org/anti_virus_test_file.htm. Сохраните его в папку общего доступа на локальном диске любого компьютера сети.

   Перед сохранением файла в папку убедитесь, что функция постоянной защиты файлов отключена для этой папки.

2. Если вы хотите проверить работу уведомлений пользователей сети, убедитесь, что Служба сообщений Microsoft Windows включена на защищаемом компьютере и на компьютере, на котором сохранен файл eicar.com.
3. открывать Консоль программы;

4. Скопируйте сохраненный файл eicar.com на локальный диск защищаемого компьютера одним из следующих способов:
   - Чтобы проверить работу уведомлений через окно Служб терминалов, скопируйте файл eicar.com на компьютер, подключившись к компьютеру с помощью утилиты "Подключение к удаленному рабочему столу".
   - Чтобы проверить работу уведомлений через Службу сообщений Microsoft Windows, скопируйте файл eicar.com с компьютера, на котором вы его сохранили, через сетевое окружение этого компьютера.

Постоянная защита файлов работает должным образом, если выполняются следующие условия:

- Файл eicar.com удален с защищаемого компьютера.
- В Консоли программы журналу выполнения задачи присвоен статус *Критический*. В журнале появилась строка с информацией об угрозе в файле eicar.com. Чтобы просмотреть журнал выполнения задачи, в дереве Консоли программы разверните узел **Постоянная защита компьютера**, выберите задачу **Постоянная защита файлов** и в панели результатов узла перейдите по ссылке **Открыть журнал выполнения**.
  - На компьютере, с которого вы скопировали файл, появилось следующее сообщение Службы сообщений Microsoft Windows: `Kaspersky Embedded Systems Security заблокировал доступ к <путь к файлу eicar.com на компьютере>\eicar.com на компьютере <сетевое имя компьютера> в <время возникновения события>. Причина: обнаружена угроза. Вирус: EICAR-Test-File. Имя пользователя: <имя пользователя>. Имя компьютера: <сетевое имя компьютера, с которого вы скопировали файл>.`

  > Убедитесь, что Служба сообщений Microsoft Windows работает на компьютере, с которого вы скопировали файл eicar.com.

► *Чтобы проверить функцию проверки по требованию, выполните следующие действия:*

1. Загрузите файл eicar.com с веб-сайта EICAR http://www.eicar.org/anti_virus_test_file.htm. Сохраните его в папку общего доступа на локальном диске любого компьютера сети.

   > Перед сохранением файла в папку убедитесь, что функция постоянной защиты файлов отключена для этой папки.

2. открывать Консоль программы;
3. Выполните следующие действия:
   a. В дереве Консоли программы разверните узел **Проверка по требованию**.
   b. Выберите вложенный узел **Проверка важных областей**.
   c. На закладке **Настройка области проверки** откройте контекстное меню на узле **Сетевое окружение** и выберите **Добавить сетевой файл**.
   d. Введите сетевой путь к файлу eicar.com на удаленном компьютере в формате UNC (Universal Naming Convention).
   e. Установите флажок, чтобы включить добавленный сетевой путь в область проверки.

f. Запустите задачу Проверка важных областей.

Проверка по требованию работает должным образом, если выполняются следующие условия:

- Файл eicar.com удален с жесткого диска компьютера.
- В Консоли программы журналу выполнения задачи присвоен статус *Критический*. В журнале выполнения задачи проверки важных областей появилась строка с информацией об угрозе в файле eicar.com. Чтобы просмотреть журнал выполнения задачи, в дереве Консоли программы разверните узел **Проверка по требованию**, выберите задачу Проверка важных областей и в панели результатов перейдите по ссылке **Открыть журнал выполнения**.

Интерфейс программы

Вы можете управлять Kaspersky Embedded Systems Security с помощью Плагина управления и через локальную Консоль программы.

Действия в интерфейсе локальной Консоли программы описаны в разделе Работа с Консолью программы (см. раздел "Работа с Консолью Kaspersky Embedded Systems Security" на стр. 136).

Действия с Плагином управления осуществляются в интерфейсе Консоли администрирования Kaspersky Security Center. Подробная информация об интерфейсе Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

Лицензирование программы

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

В этом разделе

О Лицензионном соглашении

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

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Embedded Systems Security.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

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

О лицензии

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

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем услуг и срок использования программы зависит от типа лицензии, используемой для активации программы.

Программа активируется с помощью файла ключа или кода активации для приобретенной коммерческой лицензии.

Коммерческая лицензия – это платная лицензия, предоставляемая при приобретении программы.

В Kaspersky Embedded Systems Security предусмотрены следующие типы коммерческих лицензий:

- стандартная лицензия Kaspersky Embedded Systems Security;
- расширенная лицензия Kaspersky Embedded Systems Security Compliance Edition, распространяющаяся на два дополнительных компонента системы: Мониторинг файловых операций и Анализ журналов.

По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Embedded Systems Security). Чтобы продолжить использование Kaspersky Embedded Systems Security в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

Убедитесь, что дата окончания срока действия дополнительного ключа наступает позже даты окончания срока действия активного ключа.

О Лицензионном сертификате

Лицензионный сертификат – это документ, предоставляемый вместе с файлом ключа или кодом активации (если применимо).

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- номер заказа;
- информация о пользователе, которому предоставлена лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение количества лицензионных единиц (например, устройства, на которых можно использовать программу с предоставленной лицензией);

- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- Тип лицензии

О ключе

Ключ – это последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить ключ в программу с помощью файла ключа. Ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

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

Ключ может быть активным и дополнительным.

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

Дополнительный ключ – ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом. Дополнительный ключ может быть добавлен только при наличии активного ключа.

О файле ключа

Файл ключа – это файл с расширением key, предоставляемый "Лабораторией Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу.

Вы получаете файл ключа на указанный вами адрес электронной почты после приобретения Kaspersky Embedded Systems Security или заказа пробной версии Kaspersky Embedded Systems Security.

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

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

Для восстановления файла ключа выполните одно из следующих действий:

- Обратитесь к поставщику лицензии.
- Получите файл ключа на сайте "Лаборатории Касперского (https://keyfile.kaspersky.com/ru/) с помощью имеющегося у вас кода активации.

О коде активации

Код активации – это уникальная последовательность из 20 символов (букв и цифр). Вам нужно ввести код активации, чтобы добавить ключ для активации Kaspersky Embedded Systems Security. Вы получаете код активации на адрес электронной почты, указанный при приобретении Kaspersky Embedded Systems Security.

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

Можно восстановить утерянный после установки программы код активации. Код активации может понадобиться, например, чтобы зарегистрировать Kaspersky CompanyAccount. Для восстановления кода активации обратитесь в Службу технической поддержки "Лаборатории Касперского".

О предоставлении данных

Лицензионное соглашение для Kaspersky Embedded Systems Security, в частности в разделе «Условия обработки данных», определяет условия, ответственность и порядок передачи и обработки данных, указанных в настоящем Руководстве. Внимательно ознакомьтесь с условиями Лицензионного соглашения, а также со всеми документами, ссылки на которые содержит Лицензионное соглашение, перед тем, как принять его.

Данные, которые «Лаборатория Касперского» получает от вас при использовании программы, защищаются и обрабатываются в соответствии с Политикой конфиденциальности, опубликованной по адресу: www.kaspersky.ru/Products-and-Services-Privacy-Policy.

Принимая условия Лицензионного соглашения, вы соглашаетесь отправлять в автоматическом режиме следующие данные в «Лабораторию Касперского»:

- Для обеспечения механизма получения обновлений - информацию об установленной программе и активации программы: идентификатор устанавливаемой программы и ее полную версию, включая номер сборки, тип и идентификатор лицензии, идентификатор установки, идентификатор задачи обновления.
- Для использования функциональности перенаправления на статьи Базы знаний при возникновении ошибок в работе программы (служба Redirector): название, локализацию и полный номер версии программы, включая номер сборки, тип перенаправляющей ссылки, а также идентификатор возникшей ошибки.
- Для контроля получения согласий на обработку данных – информацию о статусе согласия с условиями Лицензионного соглашения и других документов, регламентирующих отправку данных: идентификатор и версия Лицензионного соглашения или другого документа, в рамках которого выполняется согласие с условиями обработки данных или отзыв согласия; признак, указывающий на действие пользователя (подтверждение согласия с условиями или отзыв согласия); дата и время изменения статуса согласия с условиями обработки данных.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки программы. Мастер установки Kaspersky Embedded Systems Security демонстрирует полный текст Лицензионного соглашения на шаге с запросом согласия с условиями Лицензионного соглашения.
- В любой момент с помощью файла в формате TXT (license.txt), содержащего полный текст Лицензионного соглашения. Файл предоставляется в комплекте поставки Kaspersky Embedded Systems Security, совместно с установочными файлами программы.

Локальная обработка данных

В процессе выполнения основных функций программы, описанных в настоящем Руководстве, Kaspersky Embedded Systems Security локально обрабатывает и хранит набор данных на защищаемом компьютере.

Kaspersky Embedded Systems Security локально обрабатывает и хранит следующие данные:

- информацию о проверяемых файлах и обнаруженных объектах, например, имена и атрибуты обработанных файлов и полные пути к ним на проверяемом носителе, типы файлов, действия над проверяемыми файлами, учетные данные пользователей, выполняющих какие-либо действия в защищаемой сети или на защищаемом компьютере, имена и атрибуты проверяемых устройств, информацию о запущенных в системе процессах, контрольные суммы (MD5, SHA256) и временные метки исполняемых файлов процессов, параметры цифрового сертификата, данные о запускаемых скриптах;
- информацию об активности и параметрах в операционной системе, например, параметры Брандмауэра Windows, записи Журнала событий Windows, имена учетных записей пользователей, запуски исполняемых файлов, их контрольные суммы и атрибуты;

Kaspersky Embedded Systems Security обрабатывает и хранит данные в рамках основной функциональности программы, в том числе для регистрации событий программы и получения диагностических данных. Защита локально обрабатываемых данных выполняется в соответствии с настроенными и применяющимися параметрами программы.

Kaspersky Embedded Systems Security позволяет настроить уровень защиты данных, обрабатываемых локально: вы можете изменять права пользователей на доступ к обрабатываемым данным, изменять сроки хранения таких данных, частично или полностью отключать функциональность, в рамках которой выполняется регистрация данных, а также изменять путь к папке, в которую выполняется запись данных, и ее атрибуты.

Детальная информация по настройке функциональности программы, в рамках которой выполняется обработка данных, а также параметры хранения обрабатываемых данных по умолчанию, содержится в соответствующих разделах настоящего Руководства.

Данные, обрабатываемые программой локально, не передаются автоматически в "Лабораторию Касперского" или другие сторонние системы.

По умолчанию все данные, локально обрабатываемые программой в ходе работы, удаляются после удаления Kaspersky Embedded Systems Security с компьютера.

Исключение составляют файлы с диагностической информацией (файлы трассировки и файлы дампов) и файлы Журнала событий Windows с событиями программы - рекомендуется самостоятельно удалить эти файлы.

Вы можете найти детальную информацию по работе с файлами, содержащими диагностические данные программы, в соответствующих разделах настоящего Руководства.

Вы можете удалить файлы Журнала событий Windows с программными событиями Kaspersky Embedded Systems Security стандартными средствами операционной системы.

Локальная обработка данных вспомогательными компонентами программы

В пакет установки Kaspersky Embedded Systems Security включены вспомогательные компоненты программы, которые могут быть установлены на вашем компьютере, даже если на нём не установлена программа Kaspersky Embedded Systems Security. К таким вспомогательным компонентам относятся:

- Консоль локального управления программой. Компонент входит в состав Средств администрирования и представляет собой оснастку Microsoft Management Console.

- Плагин управления. Компонент обеспечивает полноценную интеграцию с программой Kaspersky Security Center.

В процессе выполнения основных функций программы, описанных в настоящем Руководстве, вспомогательные компоненты программы локально обрабатывают и хранят набор данных на компьютере, на котором установлены, в том числе если установлены отдельно от Kaspersky Embedded Systems Security.

Компоненты программы локально обрабатывают и хранят следующие данные:

- Консоль локального управления программой: имя компьютера с установленной программой Kaspersky Embedded Systems Security (IP-адрес или доменное имя), к которому в последний раз выполнялось удаленное подключение через Консоль программы; настроенные параметры отображения в оснастке Microsoft Management Console; данные о последней папке, в которой пользователь выполнял выбор объектов посредством Консоли программы (через системный диалог, открывающийся по кнопке **Обзор**). Файлы трассировки Консоли программы могут содержать следующие данные: имя компьютера с установленной программой Kaspersky Embedded Systems Security, к которой выполнялось удаленное подключение, имя учетной записи, под которой выполнялось удаленное подключение.
- Плагин управления может обрабатывать и временно хранить данные, обрабатываемые Kaspersky Embedded Systems Security, например, настроенные параметры задач и компонентов программы, параметры политик Kaspersky Security Center, данные, передаваемые в сетевых списках.

Данные, обрабатываемые вспомогательными компонентами программы, автоматически не передаются в "Лабораторию Касперского" или другие сторонние системы.

По умолчанию все данные, локально обрабатываемые вспомогательными компонентами программы в ходе работы, удаляются после удаления этих компонентов.

Исключение составляют файлы трассировки вспомогательных компонентов программы - рекомендуется самостоятельно удалить эти файлы.

Вы можете найти детальную информацию по работе с файлами, содержащими диагностические данные вспомогательных компонентов программы, в соответствующих разделах настоящего Руководства.

Активация программы с помощью лицензионного ключа

Вы можете активировать Kaspersky Embedded Systems Security с помощью файла ключа.

Если в Kaspersky Embedded Systems Security уже добавлен активный ключ и вы добавите другой ключ в качестве активного, то новый ключ заменит ранее добавленный ключ. Добавленный ранее ключ будет удален.

Если в Kaspersky Embedded Systems Security уже добавлен дополнительный ключ и вы добавите другой ключ в качестве дополнительного, то новый ключ заменит ранее добавленный ключ. Добавленный ранее дополнительный ключ будет удален.

Если в Kaspersky Embedded Systems Security уже добавлены активный ключ и дополнительный ключ, а вы добавите новый ключ в качестве активного, то новый ключ заменит ранее добавленный активный ключ, а дополнительный ключ не будет удален.

► *Чтобы активировать Kaspersky Embedded Systems Security с помощью файла ключа, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** перейдите по ссылке **Добавить ключ**.
3. В открывшемся окне нажмите на кнопку **Обзор** и выберите файл ключа с расширением key.

   Вы также можете добавить ключ в качестве дополнительного. Для этого установите флажок **Использовать в качестве дополнительного ключа**.

4. Нажмите на кнопку **OK**.

Будет применен выбранный файл ключа. Информация о добавленном ключе отобразится в панели результатов узла **Лицензирование**.

Активация программы с помощью кода активации

Для активации программы с помощью кода активации компьютер должен быть подключен к интернету.

Вы можете активировать Kaspersky Embedded Systems Security с помощью кода активации.

При активации этим способом Kaspersky Embedded Systems Security отправляет данные на сервер активации для проверки введенного кода:

- В случае успешной проверки кода активации программа будет активирована.
- При сбое проверки кода активации отобразится соответствующее уведомление. В этом случае вам нужно обратиться к поставщику программ, у которого была приобретена лицензия на программу Kaspersky Embedded Systems Security.
- В случае превышения количества активаций с помощью указанного кода активации, отображается соответствующее уведомление. Процесс активации программы будет прерван, и вам будет предложено обратиться в Службу технической поддержки "Лаборатории Касперского".

► *Чтобы добавить ключ для активации Kaspersky Embedded Systems Security с помощью кода активации, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** перейдите по ссылке **Добавить код активации**.
3. В открывшемся окне введите код активации в поле **Код активации**.
   - Чтобы применить код активации для добавления дополнительного ключа, установите флажок **Использовать в качестве дополнительного ключа**.
   - Чтобы просмотреть информацию о лицензии, нажмите на кнопку **Посмотреть данные лицензии**. Информация отобразится в поле **Данные лицензии**.
4. Нажмите на кнопку **OK**.

   Kaspersky Embedded Systems Security отправит информацию о примененном коде активации на сервер активации.

Просмотр информации о действующей лицензии

Просмотр информации о лицензии

Информация о действующей лицензии отображается в панели результатов узла **Kaspersky Embedded Systems Security** Консоли программы. Ключ может иметь один из следующих статусов:

- **Выполняется проверка статуса ключа** – Kaspersky Embedded Systems Security проверяет примененный файл ключа или код активации и ожидает ответа о текущем статусе ключа.
- **Дата окончания срока действия лицензии** – программа Kaspersky Embedded Systems Security активирована до указанной даты и времени. Статус ключа выделен желтым цветом в следующих случаях:
  - До истечения срока действия лицензии остается не более 14 дней, и не добавлен дополнительный ключ.
  - Добавленный ключ помещен в черный список и будет заблокирован.
- **Срок действия лицензии истек** – программа Kaspersky Embedded Systems Security не активирована, поскольку истек срок действия лицензии. Статус выделен красным цветом.
- **Нарушено Лицензионное соглашение** – программа Kaspersky Embedded Systems Security не активирована, поскольку нарушены условия Лицензионного соглашения (см. раздел "О Лицензионном соглашении" на стр. 78). Статус выделен красным цветом.
- **Ключ помещен в черный список** – добавленный ключ заблокирован и помещен в черный список специалистами "Лаборатории Касперского", например, если ключ был использован сторонними лицами для незаконной активации программы. Статус выделен красным цветом.

Просмотр информации о действующей лицензии

► *Чтобы просмотреть информацию о действующей лицензии,*

В дереве Консоли программы разверните узел **Лицензирование**.

В панели результатов узла **Лицензирование** отобразится общая информация о действующей лицензии (см. таблицу ниже).

Таблица 8. Общая информация о лицензии в узле Лицензирование

Поле	Описание
Код активации	Код активации. Поле заполняется, если вы активируете программу с помощью кода активации.
Статус активации	Информация о статусе активации программы. В графе **Активация** в панели результатов узла **Лицензирование** могут отображаться следующие значения: • **Применено** – если вы активировали программу с помощью кода активации или файла ключа. **Активация** – если вы применили код активации для активации программы и процесс активации еще не закончен. Статус изменяется на *Применено* после завершения активации программы и обновления содержимого панели результатов узла. • **Ошибка активации** – если не удалось активировать программу. Вы можете посмотреть причину неудачного завершения активации в журнале выполнения задач.

Поле	Описание
Ключ	Ключ, добавленный для активации программы.
Тип лицензии	Тип лицензии: коммерческая или пробная.
Дата окончания срока действия	Дата и время окончания срока действия лицензии, связанной с активным ключом.
Статус кода активации или ключа	Статус кода активации или ключа: активный или дополнительный.

► *Чтобы просмотреть подробную информацию о лицензии,*

в панели результатов узла **Лицензирование** в контекстном меню строки с информацией о лицензии, которую вы хотите просмотреть, выберите пункт **Свойства**.

В окне **Свойства: <Статус кода активации или ключа>** на закладке **Общие** отображается подробная информация о действующей лицензии, на закладке **Дополнительно** отображается информация о заказчике и контактная информация "Лаборатории Касперского" или партнера, у которого вы приобрели Kaspersky Embedded Systems Security (см. таблицу ниже).

Таблица 9. Подробная информация о лицензии в окне Свойства: <Статус кода активации или ключа>

Поле	Описание
Закладка Общие	
Ключ	Ключ, добавленный для активации программы.
Дата добавления ключа	Дата добавления ключа в программу.
Тип лицензии	Тип лицензии: коммерческая или пробная.
Истекает через (дней)	Количество дней, оставшихся до окончания срока действия лицензии, связанной с активным ключом.
Дата окончания срока действия	Дата и время окончания срока действия лицензии, связанной с активным ключом. Если вы активируете программу по неограниченной подписке, в поле указывается значение *Не ограничена*. Если Kaspersky Embedded Systems Security не удается определить дату окончания действия лицензии, указывается значение *Неизвестна*.
журнал приложений;	Название программы, активированной с помощью файла ключа или кода активации.
Ограничение на использование ключа	Ограничение на использование ключа (если есть).
Осуществление технической поддержки	Информация о том, оказывает ли "Лаборатория Касперского" или ее партнеры техническую поддержку по условиям Лицензионного соглашения.

Поле	Описание
Закладка Дополнительно	
Информация о лицензии	Номер текущей лицензии.
Информация о поддержке	Контактная информация "Лаборатории Касперского" или партнера, который осуществляет техническую поддержку. Поле может быть пустым, если техническая поддержка не осуществляется.
Информация о владельце	Информация о владельце лицензии: имя клиента и название организации, для которой приобретена лицензия.

Функциональные ограничения после окончания срока действия лицензии

Когда заканчивается срок действия текущей лицензии, возникают следующие ограничения в работе функциональных компонентов:

- Останавливаются все задачи, за исключением задач Постоянная защита файлов, Проверка по требованию и Проверка целостности программы.
- Невозможно запустить ни одну задачу, кроме задач Постоянная защита файлов, Проверка по требованию и Проверка целостности программы. Эти задачи продолжат работать с использованием старых антивирусных баз.
- Функция Защита от эксплойтов ограничена:
  - Процессы защищаются до их перезапуска.
  - Новые процессы нельзя включить в область защиты.

Другие функции (хранилища, журналы, диагностические данные) по-прежнему доступны.

Продление срока действия лицензии

По умолчанию Kaspersky Embedded Systems Security уведомляет вас о скором окончании срока действия лицензии за 14 дней до окончания срока действия лицензии. При этом поле **Дата окончания срока действия лицензии** в панели результатов узла **Kaspersky Embedded Systems Security** выделено желтым цветом.

Можно продлить срок действия лицензии, не дожидаясь его окончания, с помощью дополнительного ключа или кода активации. Это позволяет не прерывать защиту компьютера на период после окончания срока действия текущей лицензии и до активации программы по новой лицензии.

► *Чтобы продлить срок действия лицензии, выполните следующие действия:*

1. Получите новый файл ключа или код активации.
2. В дереве Консоли программы выберите узел **Лицензирование**.

3. В панели результатов узла **Лицензирование** выполните одно из следующих действий:
   - Чтобы продлить срок действия лицензии с помощью дополнительного ключа:
     a. Перейдите по ссылке **Добавить ключ**.
     b. В открывшемся окне нажмите на кнопку **Обзор** и выберите новый файл ключа с расширением key.
     c. Установите флажок **Использовать в качестве дополнительного ключа**.
   - Чтобы продлить срок действия лицензии с помощью кода активации:
     a. Перейдите по ссылке **Добавить код активации**.
     b. В открывшемся окне введите приобретенный код активации.
     c. Установите флажок **Использовать в качестве дополнительного ключа**.

   Для применения кода активации требуется подключение к интернету.

4. Нажмите на кнопку **ОК**.

Дополнительный ключ будет добавлен и автоматически станет активным по истечении срока действия текущей лицензии на Kaspersky Embedded Systems Security.

Удаление ключа

Вы можете удалить добавленный ключ из программы.

Если в Kaspersky Embedded Systems Security добавлен дополнительный ключ, и вы удалите активный ключ, дополнительный ключ автоматически станет активным.

Если вы удалите добавленный ключ, вы можете его восстановить, повторно применив файл ключа.

► *Чтобы удалить добавленный ключ, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** в таблице с информацией о добавленных ключах выберите ключ, который вы хотите удалить.
3. В контекстном меню строки с информацией о выбранном ключе выберите пункт **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить удаление ключа.

Выбранный ключ будет удален.

Работа с Плагином управления

Этот раздел содержит информацию о Плагине управления Kaspersky Embedded Systems Security и об управлении программой, установленной на защищаемом компьютере или на группе компьютеров.

В этом разделе

Управление Kaspersky Embedded Systems Security из Kaspersky Security Center

Вы можете централизованно управлять несколькими компьютерами с установленной программой Kaspersky Embedded Systems Security, включенными в группу администрирования, с помощью Плагина управления Kaspersky Embedded Systems Security. Также в Kaspersky Security Center можно отдельно настраивать параметры работы каждого компьютера, входящего в группу администрирования.

Группа администрирования формируется на стороне Kaspersky Security Center вручную и включает несколько компьютеров с установленной программой Kaspersky Embedded Systems Security, для которых требуется настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования содержится в *Справке Kaspersky Security Center*.

Параметры программы для отдельного компьютера недоступны для настройки, если работа Kaspersky Embedded Systems Security на этом компьютере контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Embedded Systems Security из Kaspersky Security Center следующими способами:

- **С помощью политик Kaspersky Security Center**. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы компьютеров. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли администрирования или удаленно в окне **Свойства: <Имя компьютера>** в Kaspersky Security Center.

  С помощью политик вы можете настроить общие параметры программы, параметры задач постоянной защиты и задач контроля активности на компьютерах, параметры запуска системных задач по расписанию и параметры использования профилей.

- **С помощью групповых задач Kaspersky Security Center**. Групповые задачи Kaspersky Security Center позволяют удаленно настроить единые параметры задач, имеющих ограниченный срок выполнения, для группы компьютеров.
- С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи формирования правил контроля запуска программ.
- **С помощью задач для набора устройств**. Задачи для набора устройств позволяют удаленно настроить единые параметры задач, имеющих ограниченный срок выполнения, для компьютеров, не входящих ни в одну из групп администрирования.
- **С помощью окна настройки параметров отдельного сервера**. В окне **Свойства: <Имя компьютера>** можно удаленно настроить параметры задачи для отдельного компьютера, включенного в группу администрирования. Вы можете настроить как общие параметры работы программы, так и параметры работы всех задач Kaspersky Embedded Systems Security, если выбранный компьютер не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center позволяет настроить параметры программы, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры как для группы компьютеров, так и для отдельного компьютера.

Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Embedded Systems Security в Kaspersky Security Center.

В этом разделе

Управление Kaspersky Embedded Systems Security из Kaspersky Security Center

Вы можете централизованно управлять несколькими компьютерами с установленной программой Kaspersky Embedded Systems Security, включенными в группу администрирования, с помощью Плагина управления Kaspersky Embedded Systems Security. Также в Kaspersky Security Center можно отдельно настраивать параметры работы каждого компьютера, входящего в группу администрирования.

Группа администрирования формируется на стороне Kaspersky Security Center вручную и включает несколько компьютеров с установленной программой Kaspersky Embedded Systems Security, для которых требуется настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования содержится в *Справке Kaspersky Security Center*.

Параметры программы для отдельного компьютера недоступны для настройки, если работа Kaspersky Embedded Systems Security на этом компьютере контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Embedded Systems Security из Kaspersky Security Center следующими способами:

- **С помощью политик Kaspersky Security Center**. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы компьютеров. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли администрирования или удаленно в окне **Свойства: <Имя компьютера>** в Kaspersky Security Center.

  С помощью политик вы можете настроить общие параметры программы, параметры задач постоянной защиты и задач контроля активности на компьютерах, параметры запуска системных задач по расписанию и параметры использования профилей.

- **С помощью групповых задач Kaspersky Security Center**. Групповые задачи Kaspersky Security Center позволяют удаленно настроить единые параметры задач, имеющих ограниченный срок выполнения, для группы компьютеров.
- С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи формирования правил контроля запуска программ.
- **С помощью задач для набора устройств**. Задачи для набора устройств позволяют удаленно настроить единые параметры задач, имеющих ограниченный срок выполнения, для компьютеров, не входящих ни в одну из групп администрирования.
- **С помощью окна настройки параметров отдельного сервера**. В окне **Свойства: <Имя компьютера>** можно удаленно настроить параметры задачи для отдельного компьютера, включенного в группу администрирования. Вы можете настроить как общие параметры работы программы, так и параметры работы всех задач Kaspersky Embedded Systems Security, если выбранный компьютер не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center позволяет настроить параметры программы, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры как для группы компьютеров, так и для отдельного компьютера.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

В этом разделе

Переход к общим параметрам из политики

► *Чтобы открыть параметры программы Kaspersky Embedded Systems Security из политики, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую требуется настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Параметры программы**.
6. Нажмите на кнопку **Настройка** для группы параметров, которую требуется настроить.

Переход к общим параметрам из окна свойств программы

► *Чтобы открыть окно свойств Kaspersky Embedded Systems Security для отдельного компьютера, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя компьютера>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого компьютера;
   - Выберите пункт **Свойства** в контекстном меню защищаемого компьютера.

   Откроется окно **Свойства: <Имя компьютера>**.
5. В разделе **Программы** выберите **Kaspersky Embedded Systems Security**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры программы "Kaspersky Embedded Systems Security"**.
7. Перейдите в раздел **Параметры программы**.

О настройке общих параметров программы в Kaspersky Security Center

Вы можете настроить общие параметры Kaspersky Embedded Systems Security из Kaspersky Security Center для группы компьютеров или для отдельного компьютера.

В этом разделе

Настройка масштабируемости и интерфейса в Kaspersky Security Center

► *Чтобы настроить параметры масштабируемости и интерфейс программы, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

   > Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Параметры программы** в блоке **Масштабируемость и интерфейс** нажмите на кнопку **Настройка**.
5. В окне **Дополнительные параметры программы** на закладке **Общие** настройте следующие параметры:

   - В блоке **Параметры масштабируемости** настройте следующие параметры, определяющие количество используемых Kaspersky Embedded Systems Security рабочих процессов:

     - **Определять параметры масштабируемости автоматически**

       Kaspersky Embedded Systems Security регулирует количество используемых процессов автоматически.

       Это значение установлено по умолчанию.

     - **Указать количество рабочих процессов вручную**

       Kaspersky Embedded Systems Security регулирует количество активных рабочих процессов в соответствии с указанными значениями.

       - **Максимальное количество активных процессов**

         Максимальное количество процессов, которые использует Kaspersky Embedded Systems Security. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

       - **Количество процессов для постоянной защиты**

         Максимальное количество процессов, которые используют компоненты задач постоянной защиты. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

       - **Количество процессов для фоновых задач проверки по требованию**

         Максимальное количество процессов, которые использует компонент проверки по требованию при выполнении задач проверки по требованию в фоновом режиме. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.

   - В блоке **Взаимодействие с пользователем** настройте отображение Значка области уведомлений программы в панели задач: снимите или установите флажок **Показывать Значок области уведомлений**.

6. На закладке **Иерархическое хранилище** выберите вариант доступа к иерархическому хранилищу.
7. Нажмите на кнопку **ОК**.

Настроенные параметры программы будут сохранены.

Настройка параметров безопасности в Kaspersky Security Center

► *Чтобы вручную настроить параметры безопасности, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Параметры программы** в блоке **Безопасность** нажмите на кнопку **Настройка**.
5. В окне **Параметры безопасности** настройте следующие параметры:
   - В блоке **Параметры надежности** настройте параметры восстановления задач Kaspersky Embedded Systems Security в случае возникновения сбоев в работе программы или аварийного завершения работы программы.
     - **Выполнять восстановление задач**

       Флажок включает или выключает восстановление задач Kaspersky Embedded Systems Security после сбоя в работе программы или аварийного завершения работы программы.

       Если флажок установлен, Kaspersky Embedded Systems Security автоматически восстанавливает задачи Kaspersky Embedded Systems Security после сбоя в работе программы или аварийного завершения работы программы.

       Если флажок снят, Kaspersky Embedded Systems Security не восстанавливает задачи Kaspersky Embedded Systems Security после сбоя в работе программы или аварийного завершения работы программы.

       По умолчанию флажок установлен.
     - **Выполнять восстановление задач проверки по требованию не более (раз)**

       Количество попыток восстановления задач проверки по требованию после сбоя в работе Kaspersky Embedded Systems Security. Поле ввода доступно, если установлен флажок **Выполнять восстановление задач**.
   - В блоке **Действия при переходе на источник бесперебойного питания** задайте ограничение нагрузки на компьютер, создаваемой Kaspersky Embedded Systems Security при переходе на источник бесперебойного питания:

- **Не запускать задачи проверки по расписанию**

  Флажок включает или выключает запуск задач проверки по расписанию при переходе компьютера на источник бесперебойного питания до восстановления стандартного режима питания.

  Если флажок установлен, Kaspersky Embedded Systems Security не запускает задачи проверки по расписанию при переходе на источник бесперебойного питания до восстановления стандартного режима питания.

  Если флажок снят, Kaspersky Embedded Systems Security запускает задачи проверки по расписанию вне зависимости от режима питания.

  По умолчанию флажок установлен.

- **Остановить выполнение задачи проверки**

  Флажок включает или выключает выполнение запущенных задач проверки при переходе компьютера на источник бесперебойного питания.

  Если флажок установлен, Kaspersky Embedded Systems Security останавливает выполнение запущенных задач проверки при переходе компьютера на источник бесперебойного питания.

  Если флажок снят, Kaspersky Embedded Systems Security продолжает выполнение запущенных задач проверки при переходе компьютера на источник бесперебойного питания.

  По умолчанию флажок установлен.

- В блоке **Параметры применения пароля** задайте пароль для защиты доступа к функциям Kaspersky Embedded Systems Security.

6. Нажмите на кнопку **OK**.

Настроенные параметры безопасности и надежности будут сохранены.

Настройка параметров соединения в Kaspersky Security Center

Настроенные параметры соединения используются для подключения Kaspersky Embedded Systems Security к серверам обновлений и активации, а также при интеграции программ со службами KSN.

► *Чтобы настроить параметры соединения, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Параметры программы** в блоке **Соединение** нажмите на кнопку **Настройка**.

   Откроется окно **Настройка параметров соединения**.

5. В окне **Параметры соединения** настройте следующие параметры:

   - В блоке **Параметры прокси-сервера** задайте параметры использования прокси-сервера:
     - **Не использовать прокси-сервер**

       Если выбран этот вариант, Kaspersky Embedded Systems Security не использует прокси-сервер для соединения с службами KSN, а выполняет соединение напрямую.

     - **Использовать параметры указанного прокси-сервера**

       Если выбран этот вариант, для соединения с KSN Kaspersky Embedded Systems Security использует параметры прокси-сервера, указанные вручную.

     - IP-адрес или символьное имя прокси-сервера и номер порта.
     - **Не использовать прокси-сервер для локальных адресов**

       Флажок включает или выключает использование прокси-сервера при обращении к компьютерам из сети, к которой принадлежит компьютер с установленным Kaspersky Embedded Systems Security.

       Если флажок установлен, обращение к компьютерам из сети, к которой принадлежит компьютер с установленным Kaspersky Embedded Systems Security, выполняется напрямую. Прокси-сервер не используется.

       Если флажок снят, для обращения к локальным компьютерам используется прокси-сервер.

       По умолчанию флажок установлен.

   - В блоке **Параметры аутентификации на прокси-сервере** задайте параметры аутентификации:
     - Выберите параметры аутентификации в раскрывающемся списке.
       - **Не использовать аутентификацию** – проверка подлинности не производится. Этот режим выбран по умолчанию.
       - **Использовать NTLM-аутентификацию** – проверка подлинности с помощью протокола сетевой аутентификации NTLM, разработанного компанией Microsoft.
       - **Использовать NTLM-аутентификацию с именем пользователя и паролем** – проверка подлинности с помощью протокола сетевой аутентификации NTLM, разработанного компанией Microsoft, а также имени пользователя и пароля.
       - **Использовать имя пользователя и пароль** – проверка подлинности с помощью имени пользователя и пароля.
     - Если требуется, укажите имя пользователя и пароль.
   - В блоке **Лицензирование** установите или снимите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы**.

6. Нажмите на кнопку **OK**.

Настроенные параметры соединения будут сохранены.

Настройка запуска по расписанию локальных системных задач

С помощью политик можно разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления по расписанию, установленному локально на каждом компьютере группы администрирования:

- Если запуск по расписанию для локальных системных задач указанного типа запрещен в политике, такие задачи не будут выполняться на локальном компьютере по расписанию. Вы можете запустить локальные системные задачи вручную.
- Если запуск по расписанию для локальных системных задач указанного типа разрешен в политике, такие задачи будут выполняться в соответствии с параметрами расписания, настроенными локально для этой задачи.

По умолчанию запуск локальных системных задач запрещается политикой.

Рекомендуется не разрешать запуск локальных системных задач, если обновления или проверки по требованию регулируются с помощью групповых задач Kaspersky Security Center.

Если вы не используете групповые задачи обновления или проверки по требованию, разрешите запуск локальных системных задач в политике: Kaspersky Embedded Systems Security будет выполнять обновления баз и модулей программы, а также запускать все локальные системные задачи проверки по требованию в соответствии с определенным по умолчанию расписанием.

С помощью политик вы можете разрешать или запрещать запуск по расписанию для следующих локальных системных задач:

- Задачи проверки по требованию: Проверка важных областей, Проверка объектов на карантине, Проверка при старте операционной системы, Проверка целостности программы.
- Задачи обновления: Обновление баз программы, Обновление модулей программы и Копирование обновлений.

Если вы исключите защищаемый компьютер из группы администрирования, расписание системных задач будет автоматически включено.

► *Чтобы разрешить или запретить в политике запуск по расписанию системных задач Kaspersky Embedded Systems Security, выполните следующие действия:*

1. В дереве Консоли администрирования разверните узел **Управляемые устройства**, разверните нужную группу и в панели результатов выберите закладку **Политики**.
2. На закладке **Политики** в контекстном меню политики, с помощью которой вы хотите настроить запуск по расписанию системных задач Kaspersky Embedded Systems Security на компьютерах группы, выберите пункт **Свойства**.

3. В окне **Свойства: <Имя политики>** откройте раздел **Параметры программы**. В блоке **Запуск системных задач** нажмите кнопку **Настройка** и выполните одно из следующих действий:

   - Установите флажки **Разрешить запуск задач проверки по требованию** и **Разрешить запуск задач обновления и копирования обновлений**, чтобы разрешить запуск по расписанию перечисленных задач.
   - Снимите флажки **Разрешить запуск задач проверки по требованию** и **Разрешить запуск задач обновления и копирования обновлений**, чтобы запретить запуск по расписанию перечисленных задач.

   Установка или снятие флажков не влияет на параметры запуска локальных пользовательских задач указанного типа.

4. Убедитесь, что настраиваемая политика активна и применена к выбранной группе компьютеров.
5. Нажмите на кнопку **OK**.

Настроенные параметры запуска по расписанию для выбранных задач будут применены.

Настройка параметров карантина и резервного хранилища в Kaspersky Security Center

► *Чтобы настроить параметры резервного хранилища в Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

   Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.
5. В окне параметров **Хранилища** на закладке **Резервное хранилище** настройте следующие параметры резервного хранилища:

   - Чтобы задать папку резервного хранилища, в поле **Папка резервного хранилища** выберите нужную папку на локальном диске защищаемого компьютера или введите полный путь к ней.
   - Чтобы задать максимальный размер резервного хранилища, установите флажок

Максимальный размер резервного хранилища (МБ) и в поле ввода укажите нужное значение параметра в мегабайтах.

- Чтобы задать порог свободного места в резервном хранилище, определите значение параметра **Максимальный размер резервного хранилища (МБ)**, установите флажок **Порог доступного пространства (МБ)** и укажите минимальный размер свободного места в папке резервного хранилища в мегабайтах.
- Чтобы задать папку для восстановления, в блоке **Параметры восстановления** выберите нужную папку на локальном диске защищаемого компьютера или введите имя папки и полный путь к ней в поле **Папка, в которую восстанавливаются объекты**.

6. В окне параметров **Хранилища** на закладке **Карантин** настройте следующие параметры карантина:
   - Чтобы изменить папку карантина, в поле **Папка карантина** укажите полный путь к папке на локальном диске защищаемого компьютера.
   - Чтобы указать максимальный размер карантина, установите флажок **Максимальный размер карантина (МБ)** и в поле ввода укажите значение параметра в мегабайтах.
   - Чтобы указать минимальный размер свободного пространства в карантине, установите флажок **Максимальный размер карантина (МБ)** и флажок **Порог доступного пространства (МБ)**, затем в поле ввода укажите пороговое значение параметра в мегабайтах.
   - Если вы хотите изменить папку, в которую восстанавливаются объекты с карантина, в поле **Папка, в которую восстанавливаются объекты** укажите полный путь к папке на локальном диске защищаемого компьютера.
7. Нажмите на кнопку **OK**.

Настроенные параметры карантина и резервного хранилища будут сохранены.

О настройке журналов и уведомлений

В Консоли администрирования Kaspersky Security Center можно настроить уведомление администратора и пользователей о следующих событиях, связанных с работой Kaspersky Embedded Systems Security и состоянием антивирусной защиты компьютера:

- Администратор может получать информацию о событиях выбранных типов.
- Пользователи локальной сети, которые обращаются к защищаемому компьютеру, и пользователи терминального компьютера могут получать информацию о событиях типа *Обнаружен объект*.

Вы можете настроить уведомления о событиях Kaspersky Embedded Systems Security как для отдельного компьютера в окне **Свойства: <Имя компьютера>** выбранного компьютера, так и для группы компьютеров в окне **Свойства: <Имя политики>** выбранной группы администрирования.

На закладке **Уведомления о событиях** или в окне **Параметры уведомлений** можно настроить следующие типы уведомлений:

- На закладке **Уведомления о событиях** (стандартная закладка программы Kaspersky Security Center) можно настроить уведомления администратора о событиях выбранных типов. Подробная информация о способах уведомлений содержится в *Справке Kaspersky Security Center*.
- В окне **Параметры уведомлений** вы можете настраивать уведомления как администратора, так и пользователей.

Уведомления о событиях некоторых типов вы можете настраивать только на закладке или в окне, о событиях других типов – как на закладке, так и в окне.

Если вы настроите одинаковые уведомления о событиях одного типа на закладке **Уведомления о событиях** и в окне **Параметры уведомлений**, системный администратор будет получать уведомления об этих событиях дважды.

В этом разделе

Настройка параметров журналов

► *Чтобы настроить параметры журналов Kaspersky Embedded Systems Security, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Журналы и уведомления** нажмите на кнопку **Настройка** в блоке **Журналы выполнения задач**.
5. В окне **Параметры журналов** настройте следующие параметры Kaspersky Embedded Systems Security согласно вашим требованиям:
   - Настройте уровень детализации событий в журналах. Для этого выполните следующие действия:
     a. В списке **Компонент** выберите функциональный компонент Kaspersky Embedded Systems Security, уровень детализации событий которого вы хотите указать.
     b. Чтобы задать уровень детализации в журналах выполнения задач и журнале системного

аудита выбранного функционального компонента, выберите нужный уровень в списке **Уровень важности**.

- Чтобы изменить местоположение журналов по умолчанию, укажите полный путь к папке или выберите папку с помощью кнопки **Обзор**.
- Укажите, сколько дней будут храниться журналы выполнения задач.
- Укажите, сколько дней будет храниться информация, которая отображается в узле **Журнал системного аудита**.

6. Нажмите на кнопку **ОК**.

Настроенные параметры журналов будут сохранены.

Журнал безопасности

Kaspersky Embedded Systems Security ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом компьютере. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.
- Критические события компонента Анализ журналов.
- Критические события, свидетельствующие о попытке нарушения безопасности (для задач постоянной защиты компьютера, проверки по требованию, мониторинга файловых операций, контроля запуска программ и контроля устройств).

Вы можете очистить журнал безопасности и журнал системного аудита (см. раздел "Удаление событий из журнала системного аудита" на стр. 205). При этом Kaspersky Embedded Systems Security регистрирует событие системного аудита об очистке журнала безопасности.

Настройка параметров интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и снизить риск деградации системы в результате увеличения объемов журналов программы, вы можете настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он собирает и анализирует полученные события, а также выполняет другие действия в рамках управления журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: этот режим предполагает, что все события выполнения задач, публикация которых настроенная в параметрах журналов, а также все события системного аудита продолжают храниться на локальном компьютере даже после отправки в SIEM.

  Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемый компьютер.

- Удалять локальные копии событий: этот режим предполагает, что все события, зарегистрированные в ходе работы программы и опубликованные в SIEM, будут удалены с локального компьютера.

  > Программа никогда не удаляет локальные версии журнала безопасности.

Kaspersky Embedded Systems Security может конвертировать события в журналах программы в форматы,

поддерживаемые syslog-сервером, для передачи событий и их успешного распознавания на стороне SIEM. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Чтобы снизить риск неудачной отправки событий в SIEM, вы можете задать параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если не удается подключиться к основному syslog-серверу или использовать его.

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и отключать интеграцию с SIEM, а также настраивать параметры функциональности (см. таблицу ниже).

Таблица 10. Параметры интеграции с SIEM

Параметр	Значение по умолчанию	Описание
Отправлять события по протоколу syslog на внешний syslog-сервер	Не применяется	Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка.
Удалять локальные копии событий при записи на внешний syslog-сервер	Не применяется	Вы можете настраивать параметры хранения локальных копий журналов, после их отправки в SIEM с помощью установки или снятия флажка.
Формат событий	Структурированные данные	Вы можете выбирать один из двух форматов, в которые программа конвертирует свои события перед их отправкой на syslog-сервер для лучшего распознавания этих событий на стороне SIEM.
Протокол подключения	TCP	С помощью выпадающего списка вы можете настроить подключение к основному syslog-серверу по протоколам UPD или TCP, к дополнительному syslog-серверу по протоколу TCP.
Параметры подключения к основному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.
Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен	Не применяется	Вы можете включать и отключать применение зеркального syslog-сервера с помощью флажка.

Параметр	Значение по умолчанию	Описание
Параметры подключения к дополнительному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к дополнительному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.

► *Чтобы настроить параметры интеграции с SIEM, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

   Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Журналы и уведомления** нажмите на кнопку **Настройка** в блоке **Журналы выполнения задач**.

   Откроется окно **Параметры журналов и уведомлений**.
5. Выберите закладку **Интеграция с SIEM**.
6. В блоке **Параметры интеграции** установите флажок **Отправлять события по протоколу syslog на внешний syslog-сервер**.

   Флажок включает или отключает использование функциональности отправки публикуемых событий на внешний syslog-сервер.

   Если флажок установлен, программа выполняет отправку публикуемых событий в SIEM в соответствии с настроенными параметрами интеграции с SIEM.

   Если флажок снят, программа не выполняет интеграцию с SIEM. Вы не можете настраивать параметры интеграции SIEM, если флажок снят.

   По умолчанию флажок снят.
7. Если требуется, установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер** в блоке **Параметры интеграции**.

   Флажок включает или отключает удаление локальных копий журналов по их отправке в SIEM.

Если флажок установлен, программа удаляет локальные копии событий после того, как они были успешно опубликованы в SIEM. Рекомендуется использовать этот режим на маломощных компьютерах.

Если флажок снят, программа только отправляет события в SIEM. Копии журналов продолжают храниться локально.

По умолчанию флажок снят.

Статус флажка **Удалять локальные копии событий при записи на внешний syslog-сервер** не влияет на параметры хранения событий журнала безопасности: программа никогда не удаляет события журнала безопасности автоматически.

8. В блоке **Формат событий** укажите формат, в который вы хотите конвертировать события по работе программы для их отправки в SIEM.

   По умолчанию программа выполняет конвертацию в формат структурированных данных.

9. В блоке **Параметры соединения**:

   - Укажите протокол подключения к SIEM.
   - Укажите параметры соединения с основным syslog-сервером.

     Вы можете указать IP-адрес только в формате IPv4.

   - Установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если вы хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер недоступна.
     - Укажите следующие параметры подключения к зеркальному syslog-серверу: **IP-адрес** и **Порт**.

       Поля **IP-адрес** и **Порт** для зеркального syslog-сервера недоступны для редактирования, если снят флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**.

       Вы можете указать IP-адрес только в формате IPv4.

10. Нажмите на кнопку **OK**.

Настроенные параметры интеграции с SIEM будут применены.

Настройка параметров уведомлений

► *Чтобы настроить уведомления Kaspersky Embedded Systems Security, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Журналы и уведомления** в подразделе **Уведомления о событиях** нажмите на кнопку **Настройка**.
5. В окне **Параметры уведомлений** настройте следующие параметры Kaspersky Embedded Systems Security согласно вашим требованиям:

   - В списке **Настройка уведомлений** выберите тип уведомления, параметры которого вы хотите настроить.
   - В разделе **Уведомление пользователей** настройте способ уведомления пользователей. Если требуется, задайте текст уведомления.
   - В разделе **Уведомление администраторов** настройте способ уведомления администратора. Если требуется, задайте текст уведомления. Если требуется, настройте дополнительные параметры уведомлений по кнопке **Настройка**.
   - В разделе **Пороги формирования событий** укажите интервалы времени, по истечении которых Kaspersky Embedded Systems Security регистрирует события *Базы программы устарели, Базы программы сильно устарели* и *Проверка важных областей давно не выполнялась*.

     - **Базы программы устарели (сут)**

       Количество дней с момента последнего обновления баз программы.

       По умолчанию установлено 7 дней.

     - **Базы программы сильно устарели (сут)**

       Количество дней с момента последнего обновления баз программы.

       По умолчанию установлено 14 дней.

     - **Проверка важных областей давно не выполнялась (сут)**

       Количество дней с момента последнего успешного завершения задачи Проверка важных областей.

       По умолчанию установлено 30 дней.

6. Нажмите на кнопку **OK**.

Настроенные параметры уведомлений будут сохранены.

Настройка обмена информацией с Сервером администрирования

► *Чтобы выбрать типы объектов, информацию о которых Kaspersky Embedded Systems Security будет передавать на Сервер администрирования Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

   Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Журналы и уведомления** в блоке **Взаимодействие с Сервером администрирования** нажмите на кнопку **Настройка**.

   Откроется окно **Сетевые списки Сервера администрирования**.
5. В окне **Сетевые списки Сервера администрирования** выберите типы объектов, информацию о которых Kaspersky Embedded Systems Security будет передавать на Сервер администрирования Kaspersky Security Center:
   - объекты на карантине;
   - резервные копии объектов;
6. Нажмите на кнопку **OK**.

   Kaspersky Embedded Systems Security будет передавать информацию о выбранных типах объектов на Сервер администрирования.

Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления задачами Kaspersky Embedded Systems Security на нескольких компьютерах.

Вы можете создавать единые политики Kaspersky Security Center для управления защитой нескольких компьютеров, на которых установлена программа Kaspersky Embedded Systems Security.

Политика применяет указанные в ней значения параметров, функции и задачи Kaspersky Embedded Systems Security на всех защищаемых компьютерах одной группы администрирования.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. Политика, действующая в группе в текущий момент, в Консоли администрирования имеет статус *активна*.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Embedded Systems Security. Вы можете просмотреть ее в Консоли программы в узле **Журнал системного аудита**.

В Kaspersky Security Center существует единственный способ применения политик на локальных компьютерах: *Запретить изменение параметров*. После применения политики Kaspersky Embedded Systems Security применяет на локальных компьютерах значения параметров, рядом с которыми в свойствах политики вы установили значок 🔒, вместо значений этих параметров, установленных локально до применения политики. Kaspersky Embedded Systems Security не применяет значения параметров активной политики, рядом с которыми в свойствах политики установлен значок 🔓.

Если политика активна, то значения параметров, отмеченные в политике значком 🔒, отображаются в Консоли программы, но недоступны для редактирования. Значения остальных параметров (отмеченных в политике значком 🔓) доступны для редактирования в Консоли программы.

Параметры, настроенные в активной политике и отмеченные значком 🔒, также блокируют изменение параметров в окне **Свойства: <имя компьютера>** Kaspersky Security Center для отдельного компьютера.

Параметры, настроенные и переданные на локальный компьютер с помощью активной политики, сохраняются в параметрах локальных задач после снятия активной политики.

Если политика определяет параметры для задачи постоянной защиты компьютера, которая выполняется в текущий момент, то параметры, задаваемые политикой, изменятся сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

В этом разделе

Создание политики

Создание новой политики состоит из следующих этапов:

1. Создание политики с помощью мастера создания политик. В окнах мастера можно настроить параметры задач постоянной защиты компьютера.
2. Настройка параметров политики. В окне **Свойства: <Имя политики>** созданной политики вы можете настроить параметры задач постоянной защиты компьютера, общие параметры Kaspersky Embedded Systems Security, параметры карантина и резервного хранилища, уровень детализации для журналов выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Embedded Systems Security.

► *Чтобы создать политику для группы компьютеров, на которых установлена и запущена программа Kaspersky Embedded Systems Security, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите создать политику.
2. В панели результатов выбранной группы администрирования выберите закладку **Политики** и откройте окно мастера создания политик по ссылке **Создать политику**.

   Откроется окно **Мастер создания политики**.
3. В окне **Выбор программы для создания групповой политики** выберите Kaspersky Embedded Systems Security и нажмите на кнопку **Далее**.
4. В поле **Имя** укажите название групповой политики.

   Имя политики не должно содержать следующие символы: `" * < : > ? \ | .`
5. Чтобы применить параметры политики, используемые для предыдущей версии программы, выполните следующие действия:
   a. Установите флажок **Использовать параметры политики, созданной для предыдущей версии программы**.
   b. Нажмите на кнопку **Выбрать**.
   c. Выберите политику, которую требуется применить.
   d. Нажмите на кнопку **Далее**.
6. В окне **Выбор типа операции** выберите один из следующих вариантов:
   - **Создать**, чтобы создать политику с заданными по умолчанию параметрами.
   - **Импортировать политику, созданную с помощью предыдущих версий Kaspersky Embedded Systems Security**, чтобы использовать эту версию политики в качестве шаблона.
   - Нажмите на кнопку **Обзор** и выберите конфигурационный файл, в который вы сохранили параметры ранее созданной политики.

7. В окне **Постоянная защита компьютера** настройте задачи Постоянная защита файлов и Использование KSN, а также компонент Защита от эксплойтов. Разрешите или запретите применение настроенных задач политики на локальных компьютерах сети:

   - Нажмите на кнопку , чтобы разрешить настройку параметров задачи на компьютерах сети и запретить применение настроенных в политике параметров задачи.
   - Нажмите на кнопку , чтобы запретить настройку параметров задачи на компьютерах сети и разрешить применение настроенных в политике параметров задачи.

   Во вновь созданной политике используются заданные по умолчанию параметры задач постоянной защиты компьютера.

   - Чтобы изменить заданные по умолчанию параметры задачи Постоянная защита файлов, нажмите на кнопку **Настройка** в блоке **Постоянная защита файлов**. В открывшемся окне настройте параметры задачи в соответствии с вашими требованиями. Нажмите на кнопку **OK**.
   - Чтобы изменить заданные по умолчанию параметры задачи Использование KSN, нажмите на кнопку **Настройка** в подразделе **Использование KSN**. В открывшемся окне настройте параметры задачи в соответствии с вашими требованиями. Нажмите на кнопку **OK**.

     Чтобы запустить задачу Использование KSN, необходимо принять Положение о KSN в окне Обработка данных (см. раздел "Настройка обработки данных с помощью Плагина управления" на стр. 286).

   - Чтобы изменить заданные по умолчанию параметры компонента Защита от эксплойтов, нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**. В открывшемся окне настройте компонент в соответствии с вашими требованиями. Нажмите на кнопку **OK**.

8. В окне **Создание групповой политики для программы** выберите одно из следующих состояний политики:

   - **Активная политика**, если требуется, чтобы политика вступила в действие сразу после ее создания. Если в группе уже существует активная политика, то она станет неактивной и будет применена новая созданная политика.
   - **Неактивная политика**, если вы не хотите сразу применять создаваемую политику. Вы сможете активировать эту политику позже.
   - Установите флажок **Открыть окно свойств политики сразу после создания**, чтобы автоматически закрыть **мастер создания политики** и по нажатию на кнопку **Далее** перейти к настройке созданной политики.

9. Нажмите на кнопку **Готово**.

Созданная политика отобразится в списке политик на закладке **Политики** выбранной группы администрирования. В окне **Свойства: <Имя политики>** вы можете настроить другие параметры, задачи и функции Kaspersky Embedded Systems Security.

Разделы параметров политики Kaspersky Embedded Systems Security

Общие

В разделе **Общие** вы можете настроить следующие параметры политики:

- указать состояние политики;
- настроить наследование параметров от родительских политик и для дочерних политик.

Настройка событий

В разделе **Настройка событий** вы можете настроить параметры для следующих категорий событий:

- *Критическое событие*
- *Отказ функционирования*
- *Предупреждение*
- *Информационное сообщение*

По кнопке **Свойства** вы можете настроить следующие параметры для выбранных событий:

- указать место хранения и срок хранения информации о зарегистрированном событии;
- выбрать способ уведомления о регистрируемых событиях.

Параметры программы

Таблица 11. Параметры в разделе Параметры программы

Подраздел	Параметры
Масштабируемость и интерфейс	В подразделе **Масштабируемость и интерфейс** по кнопке **Настройка** вы можете настроить следующие параметры: • выбрать автоматическую или ручную настройку параметров масштабирования; • настроить параметры отображения значка программы.
журнал безопасности;	В подразделе **Безопасность** по кнопке **Настройка** вы можете настроить следующие параметры: • настроить параметры запуска задачи; • указать действия программы при переходе на источник бесперебойного питания; • включить или выключить защиту функций программы паролем.
Соединение	В подразделе **Параметры соединения** по кнопке **Настройка** вы можете настроить следующие параметры прокси-сервера для соединения с серверами обновлений, серверами активации и KSN: • указать параметры использования прокси-сервера; • указать параметры аутентификации на прокси-сервере.
Запуск системных задач	В подразделе **Запуск системных задач** по кнопке **Настройка** можно разрешить или запретить запуск следующих системных задач по расписанию, настроенному на локальных компьютерах: • задачи проверки по требованию; • задачи обновления и копирования обновлений.

Дополнительные возможности

Таблица 12. Параметры в разделе Дополнительные возможности

Подраздел	Параметры
Доверенная зона	В подразделе **Доверенная зона** по кнопке **Настройка** вы можете настроить следующие параметры применения доверенной зоны: • сформировать список исключений доверенной зоны; • включить или выключить проверку операций резервного копирования файлов; • сформировать список доверенных процессов.
Проверка съемных дисков	В подразделе **Проверка съемных дисков** по кнопке **Настройка** вы можете настроить параметры проверки съемных дисков, подключаемых по USB.
Права пользователей на управление программой	В подразделе **Права пользователей на управление программой** вы можете настроить параметры доступа пользователей и групп пользователей на управление Kaspersky Embedded Systems Security.
Права пользователей на управление службой Kaspersky Security	В подразделе **Права пользователей на управление службой Kaspersky Security** вы можете настроить параметры доступа пользователей и групп пользователей на управление службой Kaspersky Security.
Хранилища	В подразделе **Хранилища** по кнопке **Настройка** вы можете настроить следующие параметры карантина, резервного хранилища и хранилища заблокированных узлов: • указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище; • настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства; • указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина; • настроить период блокирования серверов.

Постоянная защита компьютера

Таблица 13. Параметры в разделе Постоянная защита компьютера

Подраздел	Параметры
Постоянная защита файлов	В подразделе **Постоянная защита файлов** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • указать режим защиты объектов; • настроить применение эвристического анализатора; • настроить применение доверенной зоны; • указать область защиты; • задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную; • параметры запуска задачи.

Подраздел	Параметры
Использование KSN	В подразделе **Использование KSN** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • указать действия над объектами, недоверенными в KSN; • настроить передачу данных и использование Kaspersky Security Center в качестве прокси-сервера KSN. Нажмите на кнопку **Обработка данных**, чтобы принять или отклонить Положение о KSN и Положение о KMP, а также настроить параметры для надежной передачи данных.
Защита от эксплойтов	В подразделе **Защита от эксплойтов** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • выбрать режим защиты памяти процессов; • указать действия для снижения рисков эксплуатации уязвимостей; • дополнить и изменить список защищаемых процессов.

Контроль активности на компьютерах

Таблица 14. Параметры в разделе Контроль активности на компьютерах

Подраздел	Параметры
Контроль запуска программ	В подразделе **Контроль запуска программ** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • выбрать режим работы задачи; • настроить параметры контроля повторных запусков программ; • указать область применения правил контроля запуска программ; • настроить использование KSN; • параметры запуска задачи.
Контроль устройств	В подразделе **Контроль устройств** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • выбрать режим работы задачи; • параметры запуска задачи.

Контроль активности в сети

Таблица 15. Параметры в разделе Контроль активности в сети

Подраздел	Параметры
Управление сетевым экраном	В подразделе **Управление сетевым экраном** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • настроить правила сетевого экрана; • параметры запуска задачи.

Диагностика системы

Таблица 16. Параметры в разделе Диагностика системы

Подраздел	Параметры
Мониторинг файловых операций	В подразделе **Мониторинг файловых операций** можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом компьютере.
Анализ журналов	В подразделе **Анализ журналов** можно настроить контроль целостности защищаемого компьютера на основе результатов анализа журнала событий Windows.

Журналы и уведомления

Таблица 17. Параметры в разделе Журналы и уведомления

Подраздел	Параметры
Журналы выполнения задач	В подразделе **Журналы выполнения задач** по кнопке **Настройка** вы можете настроить следующие параметры: • указать уровень важности регистрируемых событий для выбранных компонентов программы; • указать параметры хранения журналов выполнения задач. • указать параметры интеграции SIEM-системы с Kaspersky Security Center.
Уведомления о событиях	В подразделе **Уведомления о событиях** по кнопке **Настройка** вы можете настроить следующие параметры: • указать параметры уведомления пользователя для событий *Обнаружен объект*, *Обнаружено и заблокировано недоверенное запоминающее устройство* и *Недоверенный узел в списке*. • указать параметры уведомления администратора для любого выбранного события из списка событий в блоке **Настройка уведомлений**.
Взаимодействие с Сервером администрирования	В подразделе **Взаимодействие с Сервером администрирования** по кнопке **Настройка** вы можете выбрать типы объектов, информацию о которых Kaspersky Embedded Systems Security будет передавать на Сервер администрирования. Можно также настроить передачу информации об объектах резервного хранилища и карантина на Сервер администрирования.

Подробную информацию о задачах Защиты сетевых хранилищ см. в документе *Руководство по внедрению Kaspersky Embedded Systems Security для защиты сетевых хранилищ*.

История ревизий

В подразделе **История ревизий** вы можете управлять ревизиями: сравнивать с текущей ревизией или другой политикой, добавлять описания ревизий, сохранять ревизии в файл или выполнить откат.

Настройка политики

В окне **Свойства: <Имя политики>** существующей политики можно настроить общие параметры Kaspersky Embedded Systems Security, параметры карантина и резервного хранилища, параметры доверенной зоны, параметры постоянной защиты компьютера, параметры контроля активности на компьютерах, уровень детализации в журналах выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Embedded Systems Security, права доступа к управлению программой и службой Kaspersky Security, параметры применения профилей политики.

► *Чтобы настроить параметры политики, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Разверните группу администрирования, параметры политики которой вы хотите настроить, и выберите в панели результатов закладку **Политики**.
3. Выберите политику, параметры которой вы хотите настроить, и откройте окно **Свойства: <Имя политики>** одним из следующих способов:
   - Выберите параметр **Свойства** в контекстном меню политики.
   - В панели результатов выбранного узла перейдите по ссылке **Настроить параметры политики**.
   - Дважды щелкните выбранную политику.
4. На закладке **Общие** в блоке **Состояние политики** включите или выключите применение политики. Для этого выберите один из следующих вариантов:
   - **Активная политика**, если вы хотите, чтобы политика применялась на всех компьютерах, входящих в выбранную группу администрирования;
   - **Неактивная политика**, если вы хотите активировать политику позже на всех компьютерах, входящих в выбранную группу администрирования.

   Вариант **Политика для автономных пользователей** недоступен при работе с Kaspersky Embedded Systems Security.
5. В блоках **Настройка событий**, **Параметры программы**, **Дополнительные возможности**, **Журналы и уведомления**, **История ревизий** можно настроить параметры программы (см. таблицу ниже).
6. В разделах **Постоянная защита компьютера**, **Контроль активности на компьютерах**, **Контроль активности в сети**, **Диагностика системы** можно настроить параметры программы, а также параметры запуска программы (см. таблицу ниже).

   Вы можете включать и выключать выполнение любой задачи на всех компьютерах, входящих в группу администрирования, с помощью политики Kaspersky Security Center.
   Вы можете настроить применение параметров, заданных в политике, на всех компьютерах сети для каждого отдельного компонента программы.
7. Нажмите на кнопку **OK**.

Настроенные параметры будут применены в политике.

Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security, их создании, настройке параметров выполнения, запуске и остановке.

В этом разделе

О создании задач в Kaspersky Security Center

Вы можете создавать групповые задачи для групп администрирования и для наборов компьютеров. Вы можете создавать задачи следующих типов:

- Активация программы
- Копирование обновлений
- Обновление баз программы
- Обновление модулей программы
- Откат обновления баз программы
- Проверка по требованию
- Проверка целостности программы
- Формирование правил контроля запуска программ
- Формирование правил контроля устройств

Вы можете создать локальные и групповые задачи следующими способами:

- для отдельного компьютера: в окне **Свойства <Имя компьютера>** в разделе **Задачи**;
- для группы администрирования: в панели результатов узла выбранной группы компьютеров на закладке **Задачи**;
- для набора компьютеров: в панели результатов узла **Выборки устройств**.

С помощью политик можно отключить расписания локальных системных задач Обновление и Проверка по требованию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 98) на всех защищаемых компьютерах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center содержится в *Справке Kaspersky Security Center*.

Создание задачи в Kaspersky Security Center

► *Чтобы создать новую задачу в Консоли администрирования Kaspersky Security Center, выполните следующие действия:*

1. Запустите мастер создания задачи одним из следующих способов:
   - Для создания локальной задачи:
     a. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый компьютер.
     b. В панели результатов на закладке **Устройства** откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.
     c. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.
   - Для создания групповой задачи:
     a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
     b. Выберите группу администрирования, для которой требуется создать задачу.
     c. В панели результатов выберите закладку **Задачи** и выберите пункт **Создать задачу**.
   - Чтобы создать задачу для произвольного набора компьютеров, выполните следующие действия:
     a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
     b. Выберите группу администрирования, к которой относятся компьютеры.
     c. Выберите компьютер или произвольный набор компьютеров.
     d. В раскрывающемся списке **Выполнить действие** выберите элемент **Создать задачу**.

   Откроется окно мастера создания задачи.
2. В окне **Выбор типа задачи** под заголовком **Kaspersky Embedded Systems Security** выберите тип создаваемой задачи.
3. Если вы выбрали любой тип задачи, кроме типов Откат обновления баз программы, Проверка целостности программы и Активация программы, откроется окно **Параметры**. В зависимости от типа задачи параметры могут различаться.
   - Создайте задачу проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. 424).
   - Для создания задачи обновления настройте параметры задачи в соответствии с вашими требованиями:
     a. Выберите источник обновлений в окне **Источник обновлений**.
     b. Нажмите на кнопку **Параметры соединения**. Откроется окно **Настройка параметров соединения**.
     c. В окне **Параметры соединения** выполните следующие действия:

        Укажите режим FTP-сервера для соединения с защищаемым компьютером.

Если требуется, измените время ожидания при соединении с источником обновления.

Настройте параметры доступа к прокси-серверу при соединении с источником обновлений.

Укажите местоположение защищаемого компьютера, чтобы оптимизировать получение обновлений.

- Для создания задачи Обновление модулей программы настройте требуемые параметры обновления программных модулей в окне **Параметры обновления модулей программы**.
  a. Выберите либо копирование и установку критических обновлений модулей программы, либо только проверку на их наличие, без установки.
  b. Если вы выбрали **Копировать и устанавливать критические обновления модулей программы**, для применения установленных программных модулей может потребоваться перезагрузка компьютера. Чтобы программа Kaspersky Embedded Systems Security автоматически выполняла перезагрузку компьютера после завершения задачи, установите флажок **Разрешать перезагрузку операционной системы**.
  c. Если вы хотите получать информацию о выходе плановых обновлений модулей Kaspersky Embedded Systems Security, установите флажок **Получать информацию о доступных плановых обновлениях модулей программы**.

  "Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете сами загружать их с веб-сайта "Лаборатории Касперского". Уведомление администратора о событии **Доступны новые плановые обновления модулей программы** можно настроить. Оно будет включать адрес нашего веб-сайта, на котором можно загрузить запланированные обновления.
- Для создания задачи Копирование обновлений укажите состав обновлений и папку, в которую будут сохранены обновления, в окне **Настройка параметров копирования обновлений**.
- Для создания задачи Активация программы:
  a. В окне **Параметры активации программы** укажите файл ключа, с помощью которого вы хотите активировать программу.
  b. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите создать задачу для продления срока действия лицензии.
- Создайте задачу Формирование правил контроля запуска программ (см. раздел "Создание задачи Формирование правил контроля запуска программ" на стр. 325).
- Создайте задачу Формирование правил контроля устройств (см. раздел "Создание правил с помощью задачи Формирование правил контроля устройств" на стр. 366).

4. Настройте расписание задачи (см. раздел "Настройка расписания запуска задач" на стр. 130). Можно настроить расписание для всех типов задач, кроме Откат обновления баз программы.
5. Нажмите на кнопку **ОК**.
6. Если задача создана для набора компьютеров, выберите сеть (группу) компьютеров, на которых она будет выполняться.
7. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, с правами которой вы хотите выполнять задачу.
8. В окне **Определение названия задачи** введите название задачи (не более 100 символов, не должно содержать символы **" * < > ? \ | :**).

   Рекомендуется включить в название задачи ее тип (например, "Проверка по требованию папок общего доступа").

9. В окне **Завершение создания задачи** установите флажок **Запустить задачу после завершения работы мастера**, если вы хотите, чтобы задача была запущена сразу после создания. Нажмите на кнопку **Готово**.

Созданная задача отобразится в списке **Задачи**.

Настройка локальных задач в окне Параметры программы в Kaspersky Security Center

► *Чтобы настроить локальные задачи или общие параметры программы для отдельного компьютера, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый компьютер.
2. В панели результатов выберите закладку **Устройства**.
3. Откройте окно **Свойства: <Имя компьютера>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого компьютера;
   - выбором пункта **Свойства** в контекстном меню защищаемого компьютера.

   Откроется окно **Свойства: <Имя компьютера>**.
4. Чтобы настроить параметры локальной задачи, выполните следующие действия:
   a. Перейдите в раздел **Задачи**.
      - В списке задач выберите локальную задачу, параметры которой вы хотите настроить.
      - Откройте окно свойств задачи двойным щелчком мыши на названии задачи в списке задач.
      - Выберите название задачи и нажмите на кнопку **Свойства**.
      - Выберите пункт **Свойства** в контекстном меню выбранной задачи.

        Откроется окно **Свойства: <Название задачи>**.
5. Чтобы настроить параметры программы, выполните следующие действия:
   a. Перейдите в раздел **Программы**.
      - В списке установленных программ выберите программу, которую требуется настроить.
      - Откройте окно параметров программы двойным щелчком мыши на названии программы в списке установленных программ.
      - Выделите название программы в списке установленных программ и нажмите на кнопку **Свойства**.
      - Откройте контекстное меню на названии программы в списке установленных программ и выберите пункт **Свойства**.

        Откроется окно **Параметры <Название программы>**.

Если программа работает под управлением политики Kaspersky Security Center и в этой политике запрещено изменять параметры программы, эти параметры недоступны для изменения в окне **Параметры <Название программы>**.

Настройка групповых задач в Kaspersky Security Center

► *Чтобы настроить групповую задачу для нескольких компьютеров, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой требуется настроить задачи.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню на названии задачи в списке созданных задач и выберите пункт **Свойства**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*

5. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:
   - Если вы настраиваете задачу проверки по требованию:
     a. В разделе **Область проверки** настройте область проверки.
     b. В разделе **Параметры** настройте интеграцию с другими компонентами программы и уровень приоритета задачи.
   - Если вы настраиваете одну из задач обновления, установите параметры задачи в соответствии с вашими требованиями:
     a. В разделе **Параметры** настройте параметры источника обновлений и оптимизацию использования дисковой подсистемы.
     b. По кнопке **Параметры соединения** настройте параметры соединения с источником обновлений.
   - Чтобы настроить задачу Обновление модулей программы, в разделе **Настройка параметров обновления модулей программы** выберите действие, которое требуется выполнить: копировать и устанавливать критические обновления программных модулей или только проверять их наличие.
   - Чтобы настроить задачу Копирование обновлений, в разделе **Настройка параметров копирования обновлений** укажите состав обновлений и папку локального источника обновлений, в которую будут сохранены обновления.

- Чтобы настроить задачу Активация программы, в блоке **Параметры активации** примените файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить код активации или файл ключа для продления срока действия лицензии.
- Чтобы настроить автоматическое формирование разрешающих правил контроля компьютера, в блоке **Настройка** укажите параметры, на основе которых будет сформирован список разрешающих правил.

6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз программы).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу. Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*
8. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи. Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*
9. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

Настроенные параметры групповых задач будут сохранены.

Параметры групповых задач, доступные для настройки, описаны в таблице ниже.

Таблица 18. Параметры групповых задач Kaspersky Embedded Systems Security

Типы задач Kaspersky Embedded Systems Security	Раздел в окне Свойства: <Название задачи>	Параметры задачи
Формирование правил контроля запуска программ	**Настройка**	При настройке параметров задачи Формирование правил контроля запуска программ вы можете: • Создавать разрешающие правила на основе запущенных программ. • Создавать разрешающие правила для программ из определенных папок.
	Параметры	Вы можете указать следующие действия при формировании разрешающих правил контроля запуска программ: • **Использовать цифровой сертификат** • **Использовать заголовок и отпечаток цифрового сертификата** • **Если сертификат отсутствует, использовать** • **Использовать хеш SHA256** • **Формировать правила для пользователя или группы пользователей** Вы можете настроить параметры для конфигурационных файлов со списком сформированных разрешающих правил контроля устройств и контроля запуска программ, которые Kaspersky Embedded Systems Security создает по завершении задач.

Типы задач Kaspersky Embedded Systems Security	Раздел в окне Свойства: <Название задачи>	Параметры задачи
	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.
Формирование правил контроля устройств	**Настройка**	• Выбор режима работы: учитывать данные системы обо всех когда-либо подключавшихся запоминающих устройствах или только о подключенных в настоящий момент запоминающих устройствах. • Настройте параметры для конфигурационных файлов со списком разрешающих правил, которые Kaspersky Embedded Systems Security создает по завершении задачи.
	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.
Активация программы (см. раздел "Задача Активация программы" на стр. 125).	**Параметры активации**	Для активации программы или для продления срока действия лицензии можно указать файл ключа.
	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.
Копирование обновлений (см. раздел "Задачи обновления" на стр. 126).	**Источник обновлений**	Вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений. Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.
	Окно **Настройка параметров соединения**	В окне **Настройка параметров соединения**, доступном из раздела **Источник обновлений**, можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.
	Настройка параметров копирования обновлений	Вы можете указать состав обновлений для копирования. В поле **Папка для локального хранения скопированных обновлений** укажите путь к папке, в которой Kaspersky Embedded Systems Security будет сохранять скопированные обновления.
	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.

Типы задач Kaspersky Embedded Systems Security	Раздел в окне Свойства: <Название задачи>	Параметры задачи
Обновление баз программы (см. раздел "Задачи обновления" на стр. 126)	**Настройка**	В блоке **Источник обновлений** вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений. Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны. В блоке Оптимизация использования дисковой подсистемы вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему: • **Снизить нагрузку на дисковую систему** • **Объем оперативной памяти, используемый для оптимизации (МБ)**
	Окно **Настройка параметров соединения**	В окне **Настройка параметров соединения**, доступном из раздела **Источник обновлений**, можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.
	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.
Обновление модулей программы (см. раздел "Задачи обновления" на стр. 126)	**Источник обновлений**	Вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений. Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.
	Окно **Настройка параметров соединения**	В блоке **Параметры соединения с источниками обновлений** вы можете настроить параметры использования прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.

Типы задач Kaspersky Embedded Systems Security	Раздел в окне Свойства: <Название задачи>	Параметры задачи
	Настройка параметров обновления модулей программы	Вы можете указать действия, которые Kaspersky Embedded Systems Security будет совершать при наличии критических обновлений модулей программы, при наличии информации о доступных плановых обновлениях, а также настроить действия программы по завершении установки критических обновлений.
	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.
Параметры проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. 424).	**Область проверки**	Вы можете сформировать область проверки для задачи проверки по требованию, а также перейти к настройке уровня безопасности.
	Окно **Параметры проверки по требованию**	В окне **Параметры проверки по требованию**, доступном из раздела **Область проверки**, вы можете выбрать один из стандартных уровней безопасности или настроить уровень безопасности вручную.
	Параметры	В блоке **Эвристический анализатор** вы можете включить или выключить применение эвристического анализатора в задаче проверки по требованию и настроить уровень анализа с помощью ползунка. В блоке **Интеграция с другими компонентами** вы можете настроить следующие параметры: • применение Доверенной зоны в задачах проверки по требованию; • применение служб KSN в задачах проверки по требованию; • указать приоритет задачи проверки по требованию: выполнять задачу в фоновом режиме (низкий приоритет) или считать выполнение задачи проверкой важных областей.
	Расписание	Вы можете настраивать параметры запуска задачи по расписанию.
Проверка целостности программы (на стр. 127)	**Расписание**	Вы можете настраивать параметры запуска задачи по расписанию.

Для задачи Откат обновления баз программы можно настроить только стандартные параметры задачи, регулируемые Kaspersky Security Center, в разделах **Уведомления** и **Исключения из области действия задачи**.

Подробная информация о настройке параметров в этих разделах содержится в *Справке Kaspersky Security Center.*

В этом разделе

Задача Активация программы

► *Чтобы настроить задачу Активация программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой требуется настроить задачи.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню на названии задачи в списке созданных задач и выберите пункт **Свойства**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*
5. В разделе **Параметры активации программы** укажите файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить ключ для продления срока действия лицензии.
6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз программы).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.
8. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*
9. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

Задачи обновления

► *Чтобы настроить задачу Копирование обновлений, Обновление баз программы или Обновление модулей программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой требуется настроить задачи.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню на названии задачи в списке созданных задач и выберите пункт **Свойства**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*

5. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:
   - В разделе **Источник обновлений** настройте параметры источника обновлений и оптимизацию использования дисковой подсистемы.
     a. В блоке **Источник обновлений** вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.

        Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.

     b. В блоке **Оптимизация использования дисковой подсистемы** для задачи Обновление баз программы вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему:

        - **Снизить нагрузку на дисковую систему**

          Флажок включает или выключает функцию оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти.

          Если флажок установлен, функция активна.

          По умолчанию флажок снят.

        - **Объем оперативной памяти, используемый для оптимизации (МБ)**

          Объем оперативной памяти (в мегабайтах), который программа использует для хранения файлов обновлений. По умолчанию установлен объем оперативной памяти 512 МБ. Минимально допустимый объем оперативной памяти 400 МБ.

     c. Нажмите на кнопку **Настройка параметров соединения** и в открывшемся окне **Параметры соединения** настройте параметры использования прокси-сервера для соединения с

серверами обновлений «Лаборатории Касперского» и другими серверами.

- В разделе **Настройка параметров обновления модулей программы** для задачи Обновление модулей программы вы можете указать действия, которые Kaspersky Embedded Systems Security будет совершать при наличии критических обновлений модулей программы, при наличии информации о доступных плановых обновлениях, а также настроить действия программы по завершении установки критических обновлений.
- В блоке **Параметры копирования обновлений** для задачи Копирование обновлений укажите состав обновлений и папку назначения, в которую будут сохранены обновления.

6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз программы).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.

   Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*

8. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

Настроенные параметры групповых задач будут сохранены.

Для задачи Откат обновления баз программы можно настроить только стандартные параметры задачи, регулируемые Kaspersky Security Center, в блоках **Уведомления** и **Исключения из области действия задачи**. Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*

Проверка целостности программы

► *Чтобы настроить групповую задачу Проверка целостности программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой требуется настроить задачи.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню на названии задачи в списке созданных задач и выберите пункт **Свойства**.
4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*

5. В разделе **Устройства** выберите устройства, для которых требуется настроить задачу Проверка целостности программы.

6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз программы).
7. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.
8. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*

9. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

Настройка параметров диагностики сбоев в Kaspersky Security Center

Если в работе Kaspersky Embedded Systems Security возникла проблема (например, Kaspersky Embedded Systems Security завершается аварийно) и вы хотите диагностировать ее, вы можете включить создание файлов трассировки и файла дампа процессов Kaspersky Embedded Systems Security и отправить эти файлы на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Embedded Systems Security не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Embedded Systems Security записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security. Можно настроить права доступа (см. раздел "Управление правами доступа к функциям Kaspersky Embedded Systems Security" на стр. 229) и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

► *Чтобы настроить параметры диагностики сбоев в Kaspersky Security Center, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. 119).
2. Откройте раздел **Диагностика сбоев** и выполните следующие действия:
   - Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.

- В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файлы трассировки.
- Настройте уровень детализации отладочной информации.

  В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Embedded Systems Security сохраняет в файле трассировки.

  Вы можете выбрать один из следующих уровней детализации:

  - **Критические события** – Kaspersky Embedded Systems Security сохраняет в файле трассировки только информацию о критических событиях.
  - **Ошибки** – Kaspersky Embedded Systems Security сохраняет в файле трассировки информацию о критических событиях и ошибках.
  - **Важные события** – Kaspersky Embedded Systems Security сохраняет в файле трассировки информацию о критических событиях, ошибках и важных событиях.
  - **Информационные события** – Kaspersky Embedded Systems Security сохраняет в файле трассировки информацию о критических событиях, ошибках, важных событиях и информационных событиях.
  - **Вся отладочная информация** – Kaspersky Embedded Systems Security сохраняет в файле трассировки всю отладочную информацию.

  Уровень детализации, который требуется установить для решения возникшей проблемы, определяет специалист Службы технической поддержки.

  По умолчанию установлен уровень детализации **Вся отладочная информация**.

  Раскрывающийся список доступен, если установлен флажок **Записывать отладочную информацию в файл трассировки**.
- Укажите максимальный размер файлов трассировки.
- Укажите отлаживаемые компоненты. Коды компонентов требуется вводить через запятую и с соблюдением регистра (см. таблицу ниже).

Таблица 19. Коды подсистем Kaspersky Embedded Systems Security

Код подсистемы	Название подсистемы
*	Все компоненты.
gui	Подсистема пользовательского интерфейса, оснастка Kaspersky Embedded Systems Security в Microsoft Management Console.
ak_conn	Подсистема интеграции с Агентом администрирования Kaspersky Security Center.
bl	Управляющий процесс, реализует задачи управления Kaspersky Embedded Systems Security.
wp	Рабочий процесс; реализует задачи антивирусной защиты.
blgate	Процесс удаленного управления Kaspersky Embedded Systems Security.
ods	Подсистема проверки по требованию.
oas	Подсистема постоянной защиты файлов.
qb	Подсистема карантина и резервного хранилища.
scandll	Вспомогательный модуль антивирусной проверки.
core	Подсистема базовой антивирусной функциональности.

Код подсистемы	Название подсистемы
avscan	Подсистема антивирусной обработки.
avserv	Подсистема управления антивирусным ядром.
prague	Подсистема базовой функциональности.
updater	Подсистема обновления баз и модулей программы.
snmp	Подсистема поддержки SNMP протокола.
perfcount	Подсистема счетчиков производительности.

Параметры трассировки оснастки Kaspersky Embedded Systems Security (gui) и Плагина управления для Kaspersky Security Center (ak_conn) применяются после перезапуска этих компонентов. Параметры трассировки подсистемы поддержки SNMP-протокола (snmp) применяются после перезапуска службы SNMP. Параметры трассировки подсистемы счетчиков производительности (perfcount) применяются после перезапуска всех процессов, использующих счетчики производительности. Параметры трассировки остальных подсистем Kaspersky Embedded Systems Security применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Embedded Systems Security сохраняет отладочную информацию о работе всех подсистем Kaspersky Embedded Systems Security (рекомендуется).

Поле ввода доступно, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Если вы хотите создавать файл дампа, установите флажок **Создавать во время сбоя файл дампа**.
  - В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файл дампа.

3. Нажмите на кнопку **OK**.

Настроенные параметры программы будут применены на защищаемом компьютере.

Работа с расписанием задач

Вы можете настраивать запуск задач Kaspersky Embedded Systems Security по расписанию, а также настраивать параметры запуска по расписанию.

В этом разделе

Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Вы не можете настраивать расписание запуска групповых задач.

► *Чтобы настроить параметры расписания запуска групповой задачи, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемый сервер.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Дважды щелкните мышью на имени задачи.
   - Откройте контекстное меню задачи и выберите пункт Свойства.
5. Выберите раздел **Расписание**.
6. В блоке **Параметры расписания** установите флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задачи проверки по требованию и задачи обновления недоступны, если запуск задачи по расписанию запрещен действием политики Kaspersky Security Center.

7. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
   a. в списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> ч.**;
      - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут.**;
      - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам);
      - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security;
      - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.
   b. В поле **Время запуска** укажите время первого запуска задачи.
   c. В поле **Начать с** укажите дату начала действия расписания.

      После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** появится информация о расчетном времени очередного запуска задачи. Обновленная информация о расчетном времени следующего запуска будет отображаться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.

Значение **Запрещен политикой** отображается в поле **Следующий запуск**, если параметрами действующей политики Kaspersky Security Center запрещен запуск системных задач по расписанию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 98).

8. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.
   - В блоке **Параметры остановки задачи**:
     a. Установите флажок **Длительность** и введите нужное количество часов и минут в полях справа, чтобы указать максимальную длительность выполнения задачи.
     b. Установите флажок **Приостановить с** и введите начальное и конечное значение временного промежутка в полях справа, чтобы указать промежуток времени в пределах суток, в течение которого выполнение задачи будет приостановлено.
   - В блоке **Дополнительные параметры**:
     a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
     b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
     c. Установите флажок **Распределять время запуска задач в интервале** и укажите значение параметра в минутах.
9. Нажмите на кнопку **OK**.
10. Нажмите на кнопку **Применить**, чтобы сохранить параметры запуска задачи.

Если вы хотите настроить параметры программы для отдельной задачи с помощью Kaspersky Security Center, выполните действия, описанные в разделе Настройка локальных задач в окне Параметры программы в Kaspersky Security Center на стр. 119.

Включение и выключение запуска задач по расписанию

Вы можете включать и выключать запуск задач по расписанию как после, так и до настройки параметров расписания.

► *Чтобы включить или выключить расписание запуска задачи, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** выполните одно из следующих действий:
   - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
   - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи

по расписанию.

> Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.

4. Нажмите на кнопку **OK**.
5. Нажмите на кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

Просмотр отчетов в Kaspersky Security Center

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования.

Начиная с Kaspersky Security Center 11, для Kaspersky Embedded Systems Security доступны следующие типы отчетов:

- отчет о статусе компонентов;
- отчет о запрещенных запусках;
- отчет о тестовых запрещенных запусках.

> Подробную информацию о настройке и работе с отчетами Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Отчет о статусе компонентов

Вы можете контролировать состояние защиты всех устройств в сети и получать организованное представление о наборе компонентов на каждом устройстве.

В отчете для каждого компонента может отображаться одно из следующих состояний: *Работает, Приостановлен, Остановлен, Неисправен, Не установлен, Запускается*.

> Состояние *Не установлен* относится к компонентам программы, а не к самой программе. Если программа не установлена, Kaspersky Security Center присваивает статус N/A (недоступно).

Можно создавать выборки компонентов и использовать фильтры, чтобы отображать сетевые устройства с определенным набором компонентов и их состояниями.

> Подробную информацию о создании и использовании выборок см. в *Справке Kaspersky Security Center*.

► *Чтобы просмотреть статусы компонентов в параметрах программы, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
2. Выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).
3. Выберите раздел **Компоненты**.
4. Ознакомьтесь с таблицей состояния компонентов.

► *Чтобы просмотреть стандартный отчет Kaspersky Security Center, выполните следующие действия:*

1. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя компьютера>**.
2. Выберите закладку **Отчеты**.
3. Откройте **Отчет о статусе компонентов программы** двойным щелчком мыши.

   Будет сформирован отчет.
4. Ознакомьтесь со следующими элементами отчета:
   - диаграмма;
   - итоговая таблица с компонентами и суммарным количеством устройств в сети, на которых установлен каждый из компонентов, а также группы, к которым они принадлежат;
   - детальная таблица, показывающая статус, версию, устройство и группу для каждого из компонентов.

Отчеты о запрещенных запусках в активном режиме и в режиме Только статистика

По результатам выполнения задачи Контроль запуска программ можно сформировать два типа отчетов: отчет о запрещенных запусках (если задача запущена в активном режиме) и отчет о тестовых запрещенных запусках (если задача запущена в режиме Только статистика). В этих отчетах приведена информация о заблокированных программах на защищаемых компьютерах сети. Каждый отчет формируется для всех групп администрирования и содержит данные обо всех программах "Лаборатории Касперского", установленных на защищаемых устройствах.

► *Чтобы просмотреть отчет о тестовых запрещенных запусках, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Только статистика (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 308).
2. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя компьютера>**.
3. Выберите закладку **Отчеты**.
4. Откройте **Отчет о запрещенных программах в режиме тестирования** двойным щелчком мыши.

   Будет сформирован отчет.

5. Ознакомьтесь со следующими элементами отчета:
   - диаграмма, показывающий десять программ с самым большим количеством заблокированных запусков;
   - итоговая таблица блокировок программ, содержащая имена исполняемых файлов, причину и время блокировки, а также количество устройств, на которых имела место блокировка программ;
   - детальная таблица, показывающая данные устройства, путь к файлу и причину блокировки.

► *Чтобы просмотреть отчет о запрещенных программах в активном режиме, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме Активный (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 308).
2. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя компьютера>**.
3. Выберите закладку **Отчеты**.
4. Откройте **Отчет о запрещенных программах** двойным щелчком мыши.

   Будет сформирован отчет.

Отчет содержит те же разделы данных, что и отчет о запрещенных запусках в режиме Только статистика.

Работа с Консолью Kaspersky Embedded Systems Security

Этот раздел содержит информацию о Консоли Kaspersky Embedded Systems Security и об управлении программой через Консоль программы, установленную на защищаемом компьютере или другом компьютере.

В этом разделе

Параметры Kaspersky Embedded Systems Security в Консоли программы

Общие параметры и параметры диагностики сбоев Kaspersky Embedded Systems Security определяют общие условия работы программы. Эти параметры позволяют регулировать количество рабочих процессов, используемых Kaspersky Embedded Systems Security, включать восстановление задач Kaspersky Embedded Systems Security после их аварийного завершения, вести журнал трассировки, включать создание файла дампа процессов Kaspersky Embedded Systems Security при их аварийном завершении и настраивать другие общие параметры.

Настройка параметров работы программы недоступна из Консоли программы, если в активной политике Kaspersky Security Center установлен запрет на изменение данных параметров.

► *Чтобы настроить параметры работы Kaspersky Embedded Systems Security, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security** и выполните одно из следующих действий:
   - В панели результатов узла перейдите по ссылке **Свойства программы**.
   - В контекстном меню узла выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.
2. В открывшемся окне настройте общие параметры работы Kaspersky Embedded Systems Security согласно вашим требованиям:
   - На закладке **Масштабируемость и интерфейс** вы можете настроить следующие параметры:
     - В блоке **Параметры масштабируемости**:
       - Максимальное количество активных процессов, которые Kaspersky Embedded Systems Security может запустить.

Таблица 20. Максимальное количество активных процессов

<table>
<tr><th>Параметр</th><th>Максимальное количество активных процессов</th></tr>
<tr><td>Описание</td><td>Этот параметр относится к группе Параметры масштабируемости Kaspersky Embedded Systems Security. Он устанавливает максимальное количество рабочих процессов, которые программа может запустить одновременно.
Увеличение количества параллельно работающих процессов повышает скорость проверки файлов и устойчивость Kaspersky Embedded Systems Security к сбоям. Однако, высокое значение этого параметра может снизить общую производительность компьютера и повысить потребление оперативной памяти.
В Консоли администрирования программы Kaspersky Security Center вы можете устанавливать параметр Максимальное количество активных процессов только для Kaspersky Embedded Systems Security на отдельном компьютере (в диалоговом окне Параметры программы); вы не можете изменять этот параметр в свойствах политики для группы компьютеров.</td></tr>
<tr><td>Возможные значения</td><td>1–8</td></tr>
<tr><td>Значение по умолчанию</td><td>Программа автоматически управляет масштабируемостью, в зависимости от количества процессоров компьютера:
<table>
<tr><th>Количество процессоров</th><th>Максимальное количество активных процессов</th></tr>
<tr><td>1</td><td>1</td></tr>
<tr><td>1 < кол-во процессоров < 4</td><td>2</td></tr>
<tr><td>4 и более</td><td>4</td></tr>
</table></td></tr>
</table>

- Количество процессов для постоянной защиты компьютера.

Таблица 21. Количество процессов для постоянной защиты

Параметр	Количество процессов для постоянной защиты
Описание	Этот параметр относится к группе **Параметры масштабируемости** Kaspersky Embedded Systems Security. С помощью этого параметра вы можете устанавливать фиксированное количество процессов, в которых Kaspersky Embedded Systems Security будет выполнять задачи постоянной защиты. Более высокое значение этого параметра повысит скорость проверки объектов в задачах постоянной защиты. Однако чем больше рабочих процессов задействует Kaspersky Embedded Systems Security, тем больше будет его влияние на общую производительность защищаемого компьютера и его потребление оперативной памяти. В Консоли администрирования программы Kaspersky Security Center вы можете устанавливать параметр **Количество процессов для постоянной защиты** только для Kaspersky Embedded Systems Security на отдельном компьютере (в окне **Параметры программы**); вы не можете изменять этот параметр в свойствах политики для группы компьютеров.
Возможные значения	Возможные значения: 1-N, где N – значение, заданное параметром **Максимальное количество активных процессов**. Если вы установите значение параметра **Количество процессов для постоянной защиты** равным максимальному числу активных процессов, вы снизите влияние Kaspersky Embedded Systems Security на скорость файлового обмена компьютеров с компьютером, еще повысив его быстродействие во время постоянной защиты. Однако задачи обновления и задачи проверки по требованию с базовым приоритетом **Средний (Normal)** будут выполняться в уже запущенных рабочих процессах Kaspersky Embedded Systems Security. Задачи проверки по требованию будут выполняться медленнее. А если выполнение задачи вызовет аварийное завершение процесса, на его перезапуск потребуется больше времени. Задачи проверки по требованию с базовым приоритетом **Низкий** (Low) всегда выполняются в отдельном процессе или процессах.
Значение по умолчанию	Kaspersky Embedded Systems Security выполняет масштабирование автоматически в зависимости от количества процессоров на компьютере:

Количество процессоров	Количество процессов для постоянной защиты
=1	1
>1	2

- Количество рабочих процессов для фоновых задач проверки по требованию.

Таблица 22. Количество процессов для фоновых задач проверки по требованию

Параметр	Количество процессов для фоновых задач проверки по требованию
Описание	Этот параметр относится к группе **Параметры масштабируемости** Kaspersky Embedded Systems Security. С помощью этого параметра можно указать максимальное количество процессов, для которых Kaspersky Embedded Systems Security будет выполнять задачи проверки по требованию в фоновом режиме. Количество процессов, которое вы устанавливаете этим параметром, не входит в общее количество рабочих процессов Kaspersky Embedded Systems Security, заданное параметром **Максимальное количество активных процессов**. Например, если вы установите следующие значения параметров: • максимальное количество активных процессов – 3; • количество процессов для задач постоянной защиты – 3; • количество процессов для фоновых задач проверки по требованию – 1; а затем запустите задачи постоянной защиты и одну задачу проверки по требованию в фоновом режиме, общее количество рабочих процессов kavfswp.exe Kaspersky Embedded Systems Security составит 4. В одном рабочем процессе с низким приоритетом может выполняться несколько задач проверки по требованию. Вы можете повысить количество рабочих процессов, например, если вы запускаете одновременно несколько задач в фоновом режиме, чтобы выделить отдельный процесс для каждой задачи. Выделение отдельных процессов для задач повышает надежность выполнения этих задач и их скорость.
Возможные значения	1-4
Значение по умолчанию	1

  - В блоке **Взаимодействие с пользователем** настройте отображение значка области уведомлений в панели задач (см. раздел "Значок области уведомлений в панели задач" на стр. 147) при каждом запуске программы.

- На закладке **Безопасность и надежность** вы можете настроить следующие параметры:
  - В блоке **Параметры надежности** укажите количество попыток восстановления задач проверки по требованию после их аварийного завершения.

Таблица 23. Восстановление задач

Параметр	Восстановление задач (**Выполнять восстановление задач**).
Описание	Этот параметр относится к группе **Параметры надежности** Kaspersky Embedded Systems Security. Он включает восстановление задач, если они завершаются аварийно, и устанавливает количество попыток восстановления задач проверки по требованию. Когда задача завершается аварийно, процесс kavfs.exe Kaspersky Embedded Systems Security пытается повторно запустить процесс, в котором эта задача выполнялась в момент завершения. Если восстановление задач выключено, Kaspersky Embedded Systems Security не восстанавливает задачи постоянной защиты и проверки по требованию. Если восстановление задач включено, Kaspersky Embedded Systems Security пытается восстановить задачи постоянной защиты, пока они не будут успешно запущены, и пытается восстановить задачи проверки по требованию столько раз, сколько указано этим параметром.
Возможные значения	Включено / выключено. Количество попыток восстановления задач проверки по требованию: 1–10.
Значение по умолчанию	Восстановление задач включено. Количество попыток восстановления задач проверки по требованию: 2.

- В блоке **Действия при переходе на источник бесперебойного питания** укажите действия Kaspersky Embedded Systems Security при работе от источника бесперебойного питания.

Таблица 24. Использование источника бесперебойного питания

Параметр	Действия при переходе на источник бесперебойного питания.
Описание	Этот параметр определяет действия, которые Kaspersky Embedded Systems Security выполнит, когда компьютер перейдет на питание от источника бесперебойного питания.
Возможные значения	Запускать или не запускать задачи проверки по требованию, которые должны быть запущены по расписанию. Выполнять или останавливать все выполняемые задачи проверки по требованию.
Значение по умолчанию	По умолчанию при работе компьютера от источника бесперебойного питания Kaspersky Embedded Systems Security работает в следующем режиме: • не запускает задачи проверки по требованию, которые должны быть запущены по расписанию; • автоматически останавливает все выполняемые задачи проверки по требованию.

- В блоке **Параметры применения пароля** настройте параметры защиты паролем функций программы (см. раздел "Защита доступа к функциям Kaspersky Embedded Systems Security с помощью пароля" на стр. 236).

- На закладке **Параметры соединения**:
  - В блоке **Параметры прокси-сервера** укажите параметры использования прокси-сервера.

- В блоке **Параметры аутентификации на прокси-сервере** укажите тип аутентификации и необходимые данные для аутентификации на прокси-сервере.
- В блоке **Лицензирование** укажите, будет ли Kaspersky Security Center использоваться в качестве прокси-сервера для активации программы.

- На закладке **Диагностика сбоев**:
  - Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.
    - В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файлы трассировки.
    - Настройте уровень детализации отладочной информации.

      В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Embedded Systems Security сохраняет в файле трассировки.

      Вы можете выбрать один из следующих уровней детализации:

      - **Критические события** – Kaspersky Embedded Systems Security сохраняет в файле трассировки только информацию о критических событиях.
      - **Ошибки** – Kaspersky Embedded Systems Security сохраняет в файле трассировки информацию о критических событиях и ошибках.
      - **Важные события** – Kaspersky Embedded Systems Security сохраняет в файле трассировки информацию о критических событиях, ошибках и важных событиях.
      - **Информационные события** – Kaspersky Embedded Systems Security сохраняет в файле трассировки информацию о критических событиях, ошибках, важных событиях и информационных событиях.
      - **Вся отладочная информация** – Kaspersky Embedded Systems Security сохраняет в файле трассировки всю отладочную информацию.

      Уровень детализации, который требуется установить для решения возникшей проблемы, определяет специалист Службы технической поддержки.

      По умолчанию установлен уровень детализации **Вся отладочная информация**.

      Раскрывающийся список доступен, если установлен флажок **Записывать отладочную информацию в файл трассировки**.
    - Укажите максимальный размер файлов трассировки.
    - Укажите отлаживаемые компоненты.

      Список кодов подсистем Kaspersky Embedded Systems Security, о работе которых программа сохраняет отладочную информацию в файле трассировки. Коды компонентов требуется вводить через запятую и с соблюдением регистра (см. таблицу ниже).

Таблица 25. Коды подсистем Kaspersky Embedded Systems Security

Код подсистемы	Название подсистемы
*	Все компоненты.
gui	Подсистема пользовательского интерфейса, оснастка Kaspersky Embedded Systems Security в Microsoft Management Console.
ak_conn	Подсистема интеграции с Агентом администрирования Kaspersky Security Center.

Код подсистемы	Название подсистемы
bl	Управляющий процесс, реализует задачи управления Kaspersky Embedded Systems Security.
wp	Рабочий процесс; реализует задачи антивирусной защиты.
blgate	Процесс удаленного управления Kaspersky Embedded Systems Security.
ods	Подсистема проверки по требованию.
oas	Подсистема постоянной защиты файлов.
qb	Подсистема карантина и резервного хранилища.
scandll	Вспомогательный модуль антивирусной проверки.
core	Подсистема базовой антивирусной функциональности.
avscan	Подсистема антивирусной обработки.
avserv	Подсистема управления антивирусным ядром.
prague	Подсистема базовой функциональности.
updater	Подсистема обновления баз и модулей программы.
snmp	Подсистема поддержки SNMP протокола.
perfcount	Подсистема счетчиков производительности.

Параметры трассировки оснастки Kaspersky Embedded Systems Security (gui) и Плагина управления Kaspersky Embedded Systems Security для Kaspersky Security Center (ak_conn) применяются после перезапуска этих компонентов. Параметры трассировки подсистемы поддержки SNMP-протокола (snmp) применяются после перезапуска службы SNMP. Параметры трассировки подсистемы счетчиков производительности (perfcount) применяются после перезапуска всех процессов, использующих счетчики производительности. Параметры трассировки остальных подсистем Kaspersky Embedded Systems Security применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Embedded Systems Security сохраняет отладочную информацию о работе всех подсистем Kaspersky Embedded Systems Security (рекомендуется).

Поле ввода доступно, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Если вы хотите, чтобы программа создавала файл дампа, установите флажок **Создавать во время сбоя файл дампа**.

Kaspersky Embedded Systems Security не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

- В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файл дампа памяти.

Kaspersky Embedded Systems Security записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security. Можно настроить права доступа (см. раздел "Управление правами доступа к функциям Kaspersky Embedded Systems Security" на стр. 229) и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

3. Нажмите на кнопку **OK**.

Параметры работы Kaspersky Embedded Systems Security будут сохранены.

О Консоли Kaspersky Embedded Systems Security

Консоль Kaspersky Embedded Systems Security представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console.

Вы можете управлять программой через Консоль программы, установленную на защищаемом компьютере или на другом компьютере в сети организации.

После установки Консоли программы на другой компьютер требуется дополнительная настройка.

Если Консоль программы и Kaspersky Embedded Systems Security установлены на разных компьютерах, принадлежащих к разным доменам, возможны ограничения в передаче информации от Kaspersky Embedded Systems Security на Консоль программы. Например, после запуска какой-либо задачи статус этой задачи может не обновиться в Консоли программы.

При установке Консоли программы в папке установки создается файл kavfs.msc, а оснастка Kaspersky Embedded Systems Security добавляется в список изолированных оснасток Microsoft Windows.

Вы можете запустить Консоль программы из меню **Пуск**. Вы можете запустить msc-файл оснастки Kaspersky Embedded Systems Security или добавить оснастку программы в Microsoft Management Console как новый элемент в дереве.

В 64-разрядной версии Microsoft Windows вы можете добавить оснастку Kaspersky Embedded Systems Security только в Microsoft Management Console 32-разрядной версии. Для этого откройте Microsoft Management Console из командной строки с помощью команды mmc.exe /32.

Вы можете добавить несколько оснасток Kaspersky Embedded Systems Security в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких компьютеров, на которых установлена программа Kaspersky Embedded Systems Security.

Интерфейс Консоли Kaspersky Embedded Systems Security

Консоль Kaspersky Embedded Systems Security отображается в дереве Microsoft Management Console в виде узла.

После подключения к программе Kaspersky Embedded Systems Security, установленной на другом компьютере, в название узла добавляется имя компьютера, на котором установлена программа, и имя учетной записи, с правами которой выполнено подключение: **Kaspersky Embedded Systems Security <имя компьютера> как <имя учетной записи>**. При подключении к программе Kaspersky Embedded Systems Security, установленной на том же компьютере, что и Консоль программы, название узла имеет вид: **Kaspersky Embedded Systems Security**.

По умолчанию окно Консоли программы содержит следующие элементы:

- дерево Консоли программы;
- Панель результатов
- панель инструментов.

Дерево Консоли программы

В дереве Консоли программы отображается узел **Kaspersky Embedded Systems Security** и вложенные узлы функциональных компонентов программы.

Узел **Kaspersky Embedded Systems Security** содержит следующие вложенные узлы:

- **Постоянная защита компьютера**: управление задачами постоянной защиты и службами KSN. Узел **Постоянная защита компьютера** позволяет настраивать следующие задачи:
  - **Постоянная защита файлов**
  - **Использование KSN**
- **Контроль компьютера**: контроль запуска программ, установленных на защищаемом компьютере, а также контроль подключаемых устройств. Узел **Контроль компьютера** позволяет настраивать следующие задачи:
  - **Контроль запуска программ**
  - **Контроль устройств**
  - **Управление сетевым экраном**
- **Автоматическое формирование правил**: настройка автоматического формирования групповых и системных правил для задач Контроль запуска программ и Контроль устройств.
  - **Формирование правил контроля запуска программ**
  - **Формирование правил контроля устройств**
  - Групповые задачи формирования правил **<Имена задач>** (если есть).

    Групповые задачи (см. раздел "Категории задач Kaspersky Embedded Systems Security" на стр. 149) создаются с помощью Kaspersky Security Center. Вы не можете управлять групповыми задачами через Консоль программы.
- **Диагностика системы**: настройка контроля файловых операций и анализа журнала событий Windows.

  - **Мониторинг файловых операций**
  - **Анализ журналов**
- **Проверка по требованию**: управление задачами проверки по требованию. Для каждой задачи предусмотрен свой элемент управления:
  - **Проверка при старте операционной системы**
  - **Проверка важных областей**
  - **Проверка объектов на карантине**
  - **Проверка целостности программы**
  - Пользовательские задачи **<Имена задач>** (если есть).

  В узле отображаются системные задачи (см. раздел "Категории задач Kaspersky Embedded Systems Security" на стр. 149), созданные при установке программы, пользовательские задачи и групповые задачи проверки по требованию, сформированные и переданные на компьютер с помощью Kaspersky Security Center.
- **Обновление**: управление обновлением баз и модулей Kaspersky Embedded Systems Security, а также копированием обновлений для сохранения их в папке локального источника обновлений. Узел содержит вложенные узлы для управления всеми задачами обновления, а также задачей Отката обновления баз программы:
  - **Обновление баз программы**
  - **Обновление модулей программы**
  - **Копирование обновлений**
  - **Откат обновления баз программы**

  В узле отображаются все пользовательские и групповые задачи обновлений (см. раздел "Категории задач Kaspersky Embedded Systems Security" на стр. 149), сформированные и переданные на компьютер с помощью Kaspersky Security Center.
- **Хранилища**: управление параметрами карантина и резервного хранилища.
  - **Карантин**
  - **Резервное хранилище**
- **Журналы и уведомления**: управление журналами выполнения локальных задач, журналом безопасности и журналом системного аудита Kaspersky Embedded Systems Security.
  - **Журнал безопасности**
  - **Журнал системного аудита**
  - **Журналы выполнения задач**
- **Лицензирование**: добавление и удаление ключей и кодов активации Kaspersky Embedded Systems Security, просмотр информации о лицензиях.

Панель результатов

В панели результатов отображается информация о выбранном узле. Если выбран узел **Kaspersky Embedded Systems Security**, в панели результатов отображается информация о текущем состоянии защиты компьютера (см. раздел "Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security" на стр. 161), а также информация о Kaspersky Embedded Systems Security, состоянии защиты функциональных компонентов и дата истечения срока действия лицензии.

Контекстное меню узла Kaspersky Embedded Systems Security

С помощью пунктов контекстного меню узла **Kaspersky Embedded Systems Security** можно выполнять следующие операции:

- **Подключиться к другому компьютеру**. Подключиться к другому компьютеру (см. раздел "Управление Kaspersky Embedded Systems Security через Консоль программы на другом компьютере" на стр. 148), чтобы управлять установленной на нем программой Kaspersky Embedded Systems Security. Для выполнения этой операции вы можете также воспользоваться ссылкой в правом нижнем углу панели результатов узла **Kaspersky Embedded Systems Security**.
- **Запустить службу** / **Остановить службу**. Запустить или остановить программу или выбранную задачу (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. 150). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Выполнение этих операций также доступно в контекстных меню задач программы.
- **Настройка параметров проверки съемных дисков**. Настроить проверку съемных дисков (см. раздел "Проверка съемных дисков" на стр. 418), подключенных к защищаемому компьютеру через USB-порт.
- **Защита от эксплойтов: общие параметры защиты**. Настроить режим защиты от эксплойтов и профилактические действия.
- **Защита от эксплойтов: параметры защиты процессов**. Добавить процессы, которые нужно защитить, и выбрать техники защиты от эксплойтов (см. раздел "Техники защиты от эксплойтов" на стр. 481).
- **Настроить параметры доверенной зоны**. Просмотреть и настроить параметры Доверенной зоны (см. раздел "О доверенной зоне" на стр. 457).
- **Изменить права пользователей на управление программой**. Просмотреть и настроить права доступа к функциям Kaspersky Embedded Systems Security (см. раздел "Управление правами доступа к функциям Kaspersky Embedded Systems Security" на стр. 229).
- **Изменить права пользователей на управление службой Kaspersky Security**. Просмотреть и настроить права пользователя на управление службой Kaspersky Security (см. раздел "Настройка прав доступа на управление Kaspersky Embedded Systems Security и службой Kaspersky Security" на стр. 234).
- **Экспортировать параметры**. Сохранить параметры программы в конфигурационный файл в формате XML (см. раздел "Экспорт параметров" на стр. 156). Выполнение этой операции также доступно в контекстных меню задач программы.
- **Импортировать параметры**. Импортировать параметры программы из конфигурационного файла в формате XML (см. раздел "Импорт параметров" на стр. 157). Выполнение этой операции также доступно в контекстных меню задач программы.
- **Данные о программе и доступных обновлениях**. Перейти к просмотру информации о Kaspersky Embedded Systems Security и текущих доступных обновлениях модулей программы.
- **Обновить**. Обновить содержимое окна Консоли программы. Выполнение этой операции также доступно в контекстных меню задач программы.
- **Свойства**. Просмотреть и настроить параметры работы Kaspersky Embedded Systems Security или выбранной задачи. Выполнение этой операции также доступно в контекстных меню задач программы.

> Для выполнения этой операции вы также можете воспользоваться ссылкой **Свойства программы** в панели результатов узла **Kaspersky Embedded Systems Security** или кнопкой на панели инструментов.

- **Справка**. Перейти к просмотру справочной системы Kaspersky Embedded Systems Security. Выполнение этой операции также доступно в контекстных меню задач программы.

Панель инструментов и контекстное меню задач Kaspersky Embedded Systems Security

Вы можете управлять задачами Kaspersky Embedded Systems Security с помощью пунктов контекстного меню каждой задачи в дереве Консоли программы.

С помощью пунктов контекстного меню выбранной задачи вы можете выполнять следующие операции:

- **Запустить** / **Остановить**. Запустить или остановить выполнение задачи (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. 150). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов.
- **Возобновить** / **Приостановить**. Возобновить или приостановить выполнение задачи (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. 150). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Операция доступна для задач постоянной защиты и задач проверки по требованию.
- **Добавить задачу**. Создать новую пользовательскую задачу (см. раздел "Создание и настройка задачи проверки по требованию" на стр. 440). Операция доступна для задач проверки по требованию.
- **Открыть журнал выполнения**. Просматривать журнал выполнения задачи и управлять им (см. раздел "О журналах выполнения задач" на стр. 206). Операция доступна для всех задач.
- **Удалить задачу**. Удалить пользовательскую задачу. Операция доступна для задач проверки по требованию.
- **Шаблоны параметров**. Управлять шаблонами (см. раздел "Использование шаблонов параметров безопасности" на стр. 157). Операция доступна для задач постоянной защиты файлов и проверки по требованию.

Значок области уведомлений в панели задач

Каждый раз, когда Kaspersky Embedded Systems Security автоматически запускается после перезагрузки компьютера, в области уведомлений системной панели задач отображается значок . Он отображается по умолчанию, если при установке программы вы установили компонент Значок области уведомлений.

Вид значка области уведомлений отражает текущий статус защиты компьютера. Возможны два статуса:

- активный (цветной значок), если работает хотя бы одна из задач: Постоянная защита файлов, Контроль запуска программ;
- неактивный (черно-белый значок), если не работает ни одна из задач: Постоянная защита файлов, Контроль запуска программ.

Вы можете открыть контекстное меню значка области уведомлений по правой клавише мыши.

Контекстное меню включает несколько команд, предназначенных для отображения окон программы (см. таблицу ниже).

Таблица 26. Команды контекстного меню, отображаемые с помощью значка области уведомлений

Команда	Описание
Открыть Консоль программы	Открывает Консоль Kaspersky Embedded Systems Security (если она установлена).
Открыть Диагностическое окно	Открывает Диагностическое окно программы.
О программе	Открывает окно О программе с информацией о Kaspersky Embedded Systems Security. Если вы зарегистрированы в качестве пользователя Kaspersky Embedded Systems Security, окно О программе содержит информацию об установленных срочных обновлениях.
Скрыть	Скрывает значок области уведомлений в панели задач.

Скрытый значок области уведомлений можно отобразить в любое время.

► *Чтобы снова отобразить значок программы,*

в меню **Пуск** в Microsoft Windows выберите **Все программы** > **Kaspersky Embedded Systems Security** > **Значок области уведомлений**.

Названия параметров могут отличаться в зависимости от версии установленной операционной системы.

В общих параметрах Kaspersky Embedded Systems Security можно включать и выключать отображение значка области уведомлений при автоматическом запуске программы после перезагрузки компьютера.

Управление Kaspersky Embedded Systems Security через Консоль программы, установленную на другом компьютере

Вы можете управлять Kaspersky Embedded Systems Security через Консоль программы, которая установлена на удаленном компьютере.

Чтобы управление программой с помощью Консоли Kaspersky Embedded Systems Security, установленной на удаленном компьютере, было доступно, убедитесь, что выполняются следующие условия:

- Пользователи Консоли программы на удаленном компьютере добавлены в группу ESS Administrators на защищаемом компьютере.
- Разрешены сетевые соединения для процесса службы Kaspersky Security Management (kavfsgt.exe), если на защищаемом компьютере включен брандмауэр Windows.

- Во время установки Kaspersky Embedded Systems Security был установлен флажок **Разрешить удаленный доступ** в окне мастера установки.

Если программа Kaspersky Embedded Systems Security на удаленном компьютере защищена паролем, введите пароль для получения доступа к управлению программой через Консоль программы.

Управление задачами Kaspersky Embedded Systems Security

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security, их создании, настройке параметров выполнения, запуске и остановке.

В этом разделе

Категории задач Kaspersky Embedded Systems Security

Функции постоянной защиты компьютера, контроля компьютера, проверки по требованию и обновления в Kaspersky Embedded Systems Security реализованы в виде задач.

Вы можете управлять задачами с помощью контекстного меню задачи в дереве Консоли программы, панели инструментов и панели быстрого доступа. Вы можете просматривать информацию о состоянии задачи в панели результатов. Операции по управлению задачами регистрируются в журнале системного аудита.

Существует два типа задач Kaspersky Embedded Systems Security: *локальные* и *групповые*.

Локальные задачи

Локальные задачи выполняются только на том защищаемом компьютере, для которого они созданы. В зависимости от способа запуска существуют следующие типы локальных задач:

- **Локальные системные задачи**. Создаются автоматически при установке Kaspersky Embedded Systems Security. Вы можете изменять параметры всех системных задач, кроме задач Проверка объектов на карантине и Откат обновления баз программы. Вы не можете переименовывать или удалять системные задачи. Вы можете запускать системные и пользовательские задачи проверки по требованию одновременно.

- **Локальные пользовательские задачи**. В Консоли программы вы можете создавать задачи проверки по требованию. В Kaspersky Security Center вы можете создавать задачи проверки по требованию, обновления баз программы, отката обновления баз программы и копирования обновлений. Такие задачи называются пользовательскими. Вы можете переименовывать, настраивать и удалять пользовательские задачи. Вы можете запускать несколько пользовательских задач одновременно.

Групповые задачи

Групповые задачи и задачи для наборов компьютеров, созданные через Kaspersky Security Center, отображаются в Консоли программы. Такие задачи называются групповыми. Вы можете управлять групповыми задачами и настраивать их из программы Kaspersky Security Center. В Консоли программы можно только просматривать состояние групповых задач.

Сохранение задачи после изменения ее параметров

Вы можете изменять параметры как выполняемой, так и остановленной (приостановленной) задачи. Новые значения параметров вступят в силу при следующих условиях:

- если вы изменили параметры выполняемой задачи: новые значения параметров применяются сразу после сохранения задачи;.
- если вы изменили параметры остановленной (приостановленной) задачи: новые значения параметров применяются при следующем запуске задачи.

► *Чтобы сохранить измененные параметры задачи,*

в контекстном меню задачи выберите пункт **Сохранить задачу**.

Если после изменения параметров задачи вы выберете другой узел дерева Консоли программы, не выбрав предварительно команду **Сохранить задачу**, появится окно сохранения параметров.

► *Чтобы сохранить измененные параметры при переходе к другому узлу Консоли программы,*

в окне сохранения параметров нажмите на кнопку **Да**.

Запуск / приостановка / возобновление / остановка задачи вручную

Вы можете приостанавливать и возобновлять только задачи постоянной защиты компьютеров и проверки по требованию.

► *Чтобы запустить / приостановить / возобновить / остановить задачу, выполните следующие действия:*

1. Откройте контекстное меню задачи в Консоли программы.
2. Выберите один из следующих вариантов: **Запустить**, **Приостановить**, **Возобновить** или **Остановить**.

Операция будет выполнена и зарегистрирована в журнале системного аудита (стр. 204).

После возобновления задачи проверки по требованию Kaspersky Embedded Systems Security продолжает проверку с того объекта, на котором выполнение задачи было приостановлено.

Работа с расписанием задач

Вы можете настраивать запуск задач Kaspersky Embedded Systems Security по расписанию, а также настраивать параметры запуска по расписанию.

В этом разделе

Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Вы не можете настраивать расписание запуска групповых задач.

► *Чтобы настроить расписание запуска задачи, выполните следующие действия:*

1. Откройте контекстное меню названия задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** установите флажок **Запускать задачу по расписанию**.
4. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
   a. В списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> ч**.
      - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут**.
      - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед. по**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам);
      - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security;
      - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.
   b. В поле **Время запуска** укажите время первого запуска задачи.

c. В поле **Начать с** укажите дату начала действия расписания.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** появится информация о расчетном времени очередного запуска задачи. Обновленная информация о расчетном времени следующего запуска будет отображаться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.
В поле **Следующий запуск** отображается значение **Запрещен политикой**, если запуск системных задач по расписанию определен параметрами действующей политики Kaspersky Security Center.

5. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.
   - В блоке **Параметры остановки задачи**:
     a. Установите флажок **Длительность** и введите нужное количество часов и минут в полях справа, чтобы указать максимальную длительность выполнения задачи.
     b. Установите флажок **Приостановить с** и введите начальное и конечное значение временного промежутка в полях справа, чтобы указать промежуток времени в пределах суток, в течение которого выполнение задачи будет приостановлено.
   - В блоке **Дополнительные параметры**:
     a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
     b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
     c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.
6. Нажмите на кнопку **ОК**.

Настроенные параметры расписания запуска выбранной задачи будут сохранены.

Включение и выключение запуска задач по расписанию

Вы можете включать и выключать запуск задач по расписанию как после, так и до настройки параметров расписания.

► *Чтобы включить или выключить расписание запуска задачи, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке Расписание выполните одно из следующих действий:
   - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.

- Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

  Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.

4. Нажмите на кнопку **OK**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

Использование учетных записей для запуска задач

Вы можете запускать задачи, используя системную учетную запись пользователя или указать другую учетную запись.

В этом разделе

Об использовании учетных записей для запуска задач

Вы можете указать учетную запись, с правами которой вы хотите запускать выбранную задачу, для следующих функциональных компонентов Kaspersky Embedded Systems Security:

- Задачи Формирование правил контроля запуска программ и Формирование правил контроля устройств
- задачи проверки по требованию;
- Задачи обновления

По умолчанию указанные задачи выполняются с правами системной учетной записи.

Рекомендуется указать другую учетную запись с достаточными правами доступа в следующих случаях:

- в задаче обновления, если в качестве источника обновления вы указали папку общего доступа на другом компьютере в сети;
- в задаче обновления, если для доступа к источнику обновлений используется прокси-сервер со встроенной проверкой подлинности Microsoft Windows (NTLM-authentication);
- в задачах проверки по требованию, если системная учетная запись не обладает правами доступа к проверяемым объектам (например, к файлам в папках общего доступа на компьютере);
- в задаче Формирование правил контроля запуска программ, если после окончания выполнения задачи сформированные правила экспортируются в конфигурационный файл, недоступный для системной учетной записи (например, расположенный в одной из папок общего доступа на компьютере).

Вы можете запускать задачи обновления, проверки по требованию и автоматического формирования разрешающих правил контроля запуска программ с правами системной учетной записи. В ходе выполнения этих задач Kaspersky Embedded Systems Security обращается к папкам общего доступа на другом компьютере в сети, если этот компьютер зарегистрирован в одном домене с защищаемым компьютером. В этом случае системная учетная запись должна обладать правами доступа к этим папкам. Kaspersky Embedded Systems Security будет обращаться к компьютеру с правами учетной записи **<имя домена \ имя компьютера>**.

Указание учетной записи для запуска задачи

► *Чтобы указать учетную запись для запуска задачи, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню задачи, для которой вы хотите настроить запуск с правами учетной записи.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Запуск с правами** выполните следующие действия:
   a. Выберите вариант **Имя пользователя**.
   b. Укажите имя и пароль пользователя, учетную запись которого вы хотите использовать.

      Выбранный пользователь должен быть зарегистрирован на защищаемом компьютере или в одном домене с ним.

   c. Подтвердите введенный пароль.
4. Нажмите на кнопку **OK**.

Измененные параметры запуска задачи с правами учетной записи будут сохранены.

Импорт и экспорт параметров

Этот раздел содержит информацию об экспорте параметров работы Kaspersky Embedded Systems Security или параметров работы отдельных компонентов программы в конфигурационный файл в формате XML и импорте этих параметров из конфигурационного файла в программу.

В этом разделе

Об импорте и экспорте параметров

Вы можете экспортировать параметры Kaspersky Embedded Systems Security в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Embedded Systems Security из конфигурационного файла. Вы можете сохранить в конфигурационный файл как все параметры программы, так и параметры ее отдельных компонентов.

Когда вы экспортируете все параметры Kaspersky Embedded Systems Security, в файл сохраняются общие параметры программы и параметры следующих компонентов и функций Kaspersky Embedded Systems Security:

- Постоянная защита файлов
- Использование KSN
- Контроль устройств
- Контроль запуска программ
- Формирование правил контроля устройств
- Формирование правил контроля запуска программ
- Задачи проверки по требованию
- Мониторинг файловых операций
- Анализ журналов
- Обновление баз и модулей Kaspersky Embedded Systems Security
- Карантин
- Резервное хранилище
- Журналы
- Уведомления администратора и пользователей
- Доверенная зона
- Защита от эксплойтов
- Защита паролем

Также вы можете сохранять в файле общие параметры Kaspersky Embedded Systems Security и права учетных записей пользователей.

Вы не можете экспортировать параметры групповых задач.

Kaspersky Embedded Systems Security экспортирует все пароли, которые используются для работы программы, например учетные данные для запуска задач или соединения с прокси-сервером. Экспортированные пароли хранятся в конфигурационном файле в зашифрованном виде. Вы можете импортировать пароли только с помощью программы Kaspersky Embedded Systems Security, установленной на этом же компьютере, если она не была переустановлена или обновлена.

Вы не можете импортировать ранее сохраненные пароли с помощью Kaspersky Embedded Systems Security, установленного на другом компьютере. После импорта параметров на другом компьютере вам нужно ввести все пароли вручную.

Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует значения, применяемые политикой.

Вы можете импортировать параметры из конфигурационного файла, содержащего параметры только некоторых компонентов Kaspersky Embedded Systems Security (например, созданного в программе Kaspersky Embedded Systems Security, установленной с неполным набором компонентов). После импорта параметров в Kaspersky Embedded Systems Security изменяются только те параметры, которые содержались в конфигурационном файле. Остальные параметры не изменяются.

Заблокированные параметры активной политики Kaspersky Security Center при импорте параметров не изменяются.

Экспорт параметров

► *Чтобы экспортировать параметры в конфигурационный файл, выполните следующие действия:*

1. В дереве Консоли программы выполните одно из следующих действий:
   - В контекстном меню узла **Kaspersky Embedded Systems Security** выберите пункт **Экспортировать параметры**, чтобы экспортировать все параметры Kaspersky Embedded Systems Security.
   - В контекстном меню названия задачи, параметры которой вы хотите экспортировать, и выберите пункт **Экспортировать параметры,** чтобы экспортировать параметры отдельного функционального компонента программы.
   - Чтобы экспортировать параметры компонента Доверенная зона:
     a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
     b. Выберите пункт **Настроить параметры доверенной зоны**.

        Откроется окно **Доверенная зона**.
     c. Нажмите на кнопку **Экспорт**.

        Откроется окно приветствия мастера экспорта параметров.
2. Выполните инструкции в окнах **мастера**: задайте имя конфигурационного файла, в котором вы хотите сохранить параметры, и путь к файлу.

   Указывая путь, вы можете использовать системные переменные окружения, но не можете использовать пользовательские переменные окружения.

   Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует значения параметров в политике.
3. В окне **Экспорт параметров программы завершен** нажмите на кнопку **Закрыть**.

Мастер экспорта параметров будет закрыт; экспорт параметров будет завершен.

Импорт параметров

► *Чтобы импортировать параметры из конфигурационного файла, выполните следующие действия:*

1. В дереве Консоли программы выполните одно из следующих действий:
   - В контекстном меню узла **Kaspersky Embedded Systems Security** выберите пункт **Импортировать параметры**, чтобы импортировать все параметры Kaspersky Embedded Systems Security.
   - В контекстном меню названия задачи, параметры которой вы хотите импортировать, и выберите пункт **Импортировать параметры**, чтобы импортировать параметры отдельного функционального компонента.
   - Чтобы импортировать параметры компонента Доверенная зона:
     a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
     b. Выберите пункт **Настроить параметры доверенной зоны**.

        Откроется окно **Доверенная зона**.
     c. Нажмите на кнопку **Импорт**.

        Откроется окно приветствия мастера импорта параметров.
2. Выполните инструкции в окнах мастера: укажите конфигурационный файл, из которого вы хотите импортировать параметры.

   После импорта общих параметров Kaspersky Embedded Systems Security или функциональных компонентов на компьютер вы не сможете вернуть их прежние значения.
3. В окне **Импорт параметров программы завершен** нажмите на кнопку **Закрыть**.

   Мастер импорта параметров будет закрыт; импортированные параметры будут сохранены.
4. В панели инструментов Консоли программы нажмите на кнопку **Обновить**.

Импортированные параметры отобразятся в окне Консоли программы.

Kaspersky Embedded Systems Security не импортирует пароли (данные учетных записей для запуска задач или для соединения с прокси-сервером) из файла, созданного на другом компьютере или на том же компьютере, после того как на нем была переустановлена или обновлена программа Kaspersky Embedded Systems Security. После завершения импорта вам нужно ввести пароли вручную.

Использование шаблонов параметров безопасности

Этот раздел содержит информацию о работе с шаблонами параметров безопасности в задачах защиты и проверки Kaspersky Embedded Systems Security.

В этом разделе

О шаблонах параметров безопасности

Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов компьютера и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Embedded Systems Security.

Использование шаблонов доступно при настройке параметров безопасности следующих задач Kaspersky Embedded Systems Security:

- Постоянная защита файлов
- Проверка при старте операционной системы
- Проверка важных областей
- Задачи проверки по требованию

Значения параметров безопасности из шаблона, примененного к родительскому узлу в дереве файловых ресурсов компьютера, будут применены ко всем вложенным узлам. Шаблон родительского узла не применяется к вложенным узлам в следующих случаях:

- Если параметры безопасности вложенных узлов настраивались отдельно (см. раздел "Применение шаблона параметров безопасности" на стр. 159).
- Если вложенные узлы виртуальные. Вам нужно применить шаблон для каждого виртуального узла отдельно.

Создание шаблона параметров безопасности

► *Чтобы сохранить параметры безопасности узла вручную и сохранить эти параметры в шаблон, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, для которой требуется применить шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или списке сетевых файловых ресурсов компьютера выберите шаблон, который вы хотите посмотреть.
4. На закладке **Уровень безопасности** нажмите на кнопку **Сохранить как шаблон**.

   Откроется окно **Свойства шаблона**.

5. В поле **Название шаблона** введите название шаблона.
6. В поле **Описание** введите любую дополнительную информацию о шаблоне.
7. Нажмите на кнопку **OK**.

Шаблон с набором значений параметров безопасности будет сохранен.

Просмотр параметров безопасности в шаблоне

► *Чтобы просмотреть значения параметров безопасности в созданном шаблоне, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, шаблон безопасности которой требуется просмотреть.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

   Откроется окно **Шаблоны**.
3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите просмотреть.
4. Нажмите на кнопку **Просмотреть**.

Откроется окно **<Имя шаблона>**. На закладке **Общие** отображается имя шаблона и дополнительная информация о шаблоне; на закладке **Параметры** приводится список значений параметров безопасности, сохраненных в шаблоне.

Применение шаблона параметров безопасности

► *Чтобы применить параметры безопасности из шаблона для выбранного узла, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, для которой требуется применить шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или списке сетевых файловых ресурсов компьютера откройте контекстное меню узла или элемента, к которому требуется применить шаблон.
4. Выберите **Применить шаблон** → **<Название шаблона>**.
5. Нажмите на кнопку **Сохранить**.

Шаблон параметров безопасности будет применен к выбранному узлу в дереве файловых ресурсов компьютера. На закладке **Уровень безопасности выбранного узла будет установлено значение** Другой.

Значения параметров безопасности из шаблона, примененного к родительскому узлу в дереве файловых ресурсов компьютера, будут применены ко всем вложенным узлам.

Если область защиты или область проверки вложенных узлов в дереве файловых ресурсов компьютера настраивалась отдельно, параметры безопасности из шаблона, примененного к родительскому узлу, не установятся автоматически для таких вложенных узлов.

► *Чтобы установить параметры безопасности из шаблона для всех вложенных узлов, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, для которой требуется применить шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве сетевых файловых ресурсов компьютера выберите родительский узел, чтобы применить шаблон к этому узлу и ко всем его вложенным узлам.
4. В контекстном меню выберите **Применить шаблон** → **<Название шаблона>**.
5. Нажмите на кнопку **Сохранить**.

Шаблон параметров безопасности будет применен к родительскому и всем вложенным узлам в дереве файловых ресурсов компьютера. На закладке **Уровень безопасности выбранного узла будет установлено значение** Другой.

Удаление шаблона параметров безопасности

► *Чтобы удалить шаблон параметров безопасности, выполните следующие действия:*

1. В дереве Консоли программы выберите задачу, для настройки которой больше не требуется использовать шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

   Вы можете просмотреть шаблоны параметров для задач проверки по требованию из панели результатов родительского узла **Проверка по требованию**.

   Откроется окно **Шаблоны**.
3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения операции удаления.
5. В открывшемся окне нажмите на кнопку **Да**.

Выбранный шаблон будет удален.

Если шаблон параметров безопасности применялся для защиты или проверки узлов файловых ресурсов компьютера, настроенные параметры безопасности для этих узлов сохраняются после удаления шаблона.

Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security

► *Чтобы просмотреть информацию о состоянии защиты компьютера в Kaspersky Embedded Systems Security,*

в дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security**.

По умолчанию информация в панели результатов Консоли программы обновляется автоматически:

- каждые 10 секунд при локальном подключении;
- каждые 15 секунд при удаленном подключении.

Вы можете обновлять информацию вручную.

► *Чтобы вручную обновить информацию в узле **Kaspersky Embedded Systems Security**,*

в контекстном меню узла **Kaspersky Embedded Systems Security** выберите пункт **Обновить**.

В панели результатов Консоли программы отображается следующая информация о программе:

- статус использования Kaspersky Security Network;
- состояние защиты компьютера;
- данные об обновлении баз и модулей программы;
- актуальные данные диагностики;
- данные о задачах контроля компьютера;
- данные о лицензии;
- статус интеграции с Kaspersky Security Center: данные компьютера с установленным Kaspersky Security Center, к которому подключена программа, и данные о контроле задач программы активной политикой.

Для отображения статуса защиты используется цветовая индикация:

- *Зеленый цвет*. Задача выполняется в соответствии с настроенными параметрами. Защита обеспечивается.
- *Желтый цвет*. Задача не запущена, приостановлена или остановлена. Возможно возникновение угрозы безопасности. Рекомендуется настроить и запустить задачу.
- *Красный цвет*. Задача завершена с ошибкой или при работе задачи была обнаружена угроза безопасности. Рекомендуется запустить задачу или принять меры по устранению обнаруженной угрозы безопасности.

Часть информации в блоке (например, названия задач или количество обнаруженных угроз) являются ссылками, по которым вы можете перейти в узел соответствующей задачи или открыть журнал ее выполнения.

В блоке **Использование Kaspersky Security Network** отображается текущий статус задачи, например, *Выполняется*, *Остановлена* или *Не выполнялась*. Индикатор может принимать следующие значения:

- Зеленый – задача Использование KSN выполняется и запросы о файловой репутации отправляются в KSN.
- Желтый – принято одно из Положений, но задача не выполняется; или задача выполняется, но запросы не отправляются в KSN.

Защите компьютера

Раздел **Защита компьютера** (см. таблицу ниже) отображает информацию о текущем состоянии защиты компьютера.

Таблица 27. Информация о состоянии защиты компьютера

Раздел Защита	Информация
Индикатор состояния защиты компьютера	Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения: • Зеленый – отображается по умолчанию и означает, что компонент Постоянная защита файлов установлен и задача выполняется. • Желтый – компонент Постоянная защита файлов не установлен и задача Проверка важных областей не выполнялась в течение долгого времени. • Красный – задача Постоянная защита файлов не выполняется.
Постоянная защита файлов	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Обнаружено** – количество объектов, обнаруженных Kaspersky Embedded Systems Security. Например, если программа Kaspersky Embedded Systems Security обнаружила одну вредоносную программу в пяти файлах, значение в этом поле увеличится на единицу. Если количество обнаруженных вредоносных программ превышает 0, значение выделяется красным цветом.
Проверка важных областей	**Дата последней проверки** – дата и время последней проверки важных областей компьютера на наличие вирусов и других угроз безопасности. *Не выполнялась* – событие, которое возникает, если задача Проверка важных областей выполнялась 30 или более дней назад (по умолчанию). Вы можете изменять порог формирования этого события.
Защита от эксплойтов	**Статус** – текущий статус техники защиты от эксплойтов, например, *Используется* или *Не используется*. **Режим работы** – один из двух доступных режимов, выбранный при настройке защиты памяти процессов: • Завершать скомпрометированные процессы. • Только статистика. **Процессов защищено** – общее количество процессов, которые были добавлены в область защиты и обрабатываются в соответствие с выбранным режимом.

Раздел Защита	Информация
Резервные копии объектов	*Превышен порог доступного пространства в резервном хранилище* – событие, которое возникает, если объем доступного пространства в резервном хранилище достигает указанного значения. Kaspersky Embedded Systems Security при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется желтым цветом. *Превышен максимальный размер резервного хранилища* – событие, которое возникает, если размер резервного хранилища достигает указанного значения. Kaspersky Embedded Systems Security при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется красным цветом. **Объектов в резервном хранилище** – количество объектов, находящихся в резервном хранилище в текущий момент. **Используемое пространство** – объем используемого пространства в резервном хранилище.

Обновление

Раздел **Обновление** (см. таблицу ниже) отображает информацию об актуальности баз и модулей программы.

Таблица 28. Информация о состоянии баз и модулей Kaspersky Embedded Systems Security

Раздел Обновление	Информация
Индикатор состояния баз и модулей программы	Цвет панели с названием блока является индикатором состояния баз и модулей программы. Индикатор может принимать следующие значения: • Зеленый (по умолчанию) – базы программы актуальны и последняя задача Обновление баз программы завершена успешно. • Желтый – базы программы устарели или последняя задача обновления баз программы завершена с ошибкой. • Красный – возникло событие *Базы программы сильно устарели* или *Базы программы повреждены*.

Раздел Обновление	Информация
Обновление баз программы и **Обновление модулей программы**	**Актуальность баз программы** – оценка статуса обновления баз программы. Параметр может принимать следующие значения: • **Базы программы актуальны** – базы программы были обновлены не более чем 7 дней назад (по умолчанию). • **Базы программы устарели** – базы программы были обновлены 7–14 дней назад (по умолчанию). • **Базы программы сильно устарели** – базы программы были обновлены более чем 14 дней назад (по умолчанию). Вы можете изменять пороги формирования событий *Базы программы устарели* и *Базы программы сильно устарели*. **Дата выпуска баз программы** – дата и время выпуска последнего обновления баз программы. Дата и время указаны в UTC-формате. **Статус последней завершенной задачи обновления баз программы** – дата и время последнего обновления баз программы. Дата и время указаны по местному времени защищаемого компьютера. Поле окрашивается в красный цвет, если возникло событие *Завершена с ошибкой*. **Доступно обновлений модулей программы** – количество обновлений модулей Kaspersky Embedded Systems Security, доступных для загрузки и установки. **Установлено обновлений модулей программы** – количество установленных обновлений модулей Kaspersky Embedded Systems Security.

Контроль

Раздел **Контроль** (см. таблицу ниже) отображает информацию о состоянии задач Контроль запуска программ, Контроль устройств и Управление сетевым экраном.

Таблица 29. Информация о состоянии контроля компьютера

Раздел Контроль	Информация
Индикатор состояния контроля компьютера	Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения: • Зеленый – отображается по умолчанию и означает, что компонент Контроль запуска программ установлен и задача выполняется в активном режиме. • Желтый – задача Контроль запуска программ запущена в режиме **Только статистика**. • Красный – задача Контроль запуска программ не выполняется или завершена с ошибкой.

Раздел Контроль	Информация
Контроль запуска программ	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы** – один из двух доступных режимов работы задачи Контроль запуска программ: • Активный • Только статистика **Заблокировано запусков программ** – количество попыток запуска программ, заблокированных Kaspersky Embedded Systems Security в ходе выполнения задачи Контроль запуска программ. Если количество заблокированных запусков программ превышает 0, поле окрашивается в красный цвет. **Среднее время обработки (мс)** – время, которое потребовалось Kaspersky Embedded Systems Security для обработки попытки запуска программ на защищаемом компьютере.
Контроль устройств	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы** – один из двух доступных режимов работы задачи Контроль устройств: • **Активный** • **Только статистика** **Заблокировано устройств** – количество попыток подключения запоминающих устройств, заблокированных Kaspersky Embedded Systems Security в ходе выполнения задачи Контроль устройств. Если количество заблокированных запоминающих устройств превышает 0, поле окрашивается в красный цвет.
Управление сетевым экраном	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Заблокировано попыток подключения** – количество подключений к защищаемому компьютеру, которые не были разрешены заданными правилами сетевого экрана.

Диагностика

Раздел **Диагностика** (см. таблицу ниже) отображает информацию о состоянии задач Мониторинг файловых операций и Анализ журналов.

Таблица 30. Информация о состоянии диагностики системы

Раздел Диагностика	Информация
Индикатор статуса диагностики	Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения: • Зеленый – отображается по умолчанию и означает, что один или оба компонента диагностики системы установлены и задачи выполняются. • Желтый – оба компонента установлены, но одна из задач диагностики системы не выполняется; возникает событие *Не выполняется*. • Красный – одна из задач завершена с ошибкой.

Раздел Диагностика	Информация
Мониторинг файловых операций	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Несанкционированные файловые операции** – количество изменений в файлах из области мониторинга. Эти изменения могут указывать на нарушение безопасности защищаемого компьютера.
Анализ журналов	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Возможных нарушений** – количество зафиксированных нарушений по данным журнала событий Windows. Это количество определяется на основе заданных правил задачи или применения эвристического анализатора.

Информация о лицензии на Kaspersky Embedded Systems Security отображается в строке в левом нижнем углу панели результатов узла **Kaspersky Embedded Systems Security**.

Вы можете настроить свойства Kaspersky Embedded Systems Security, перейдя по ссылке Свойства программы (см. раздел "Параметры Kaspersky Embedded Systems Security в Консоли программы" на стр. 136).

Вы можете выполнить подключение к другому компьютеру, перейдя по ссылке **Подключиться к другому компьютеру** (см. раздел "Управление Kaspersky Embedded Systems Security через Консоль программы на другом компьютере" на стр. 148).

Диагностическое окно

В этом разделе описано использование диагностического окна для просмотра статуса и текущей активности компьютера, а также настройка записи файлов дампов и файлов трассировки.

В этом разделе

О диагностическом окне

Компонент Диагностическое окно (далее также "CDI") устанавливается и удаляется вместе с компонентом Значок области уведомлений независимо от Консоли программы и может использоваться, даже если Консоль программы не установлена на защищаемом компьютере. Диагностическое окно запускается через значок области уведомлений или при запуске файла kavfsmui.exe из папки программы на компьютере.

В диагностическом окне можно выполнять следующие действия:

- просматривать информацию об общем статусе программы (см. раздел "Просмотр статуса Kaspersky Embedded Systems Security с помощью диагностического окна" на стр. 168);
- просматривать произошедшие инциденты безопасности (см. раздел "Просмотр статистики событий безопасности" на стр. 169);
- просматривать текущую активность на защищаемом компьютере (см. раздел "Просмотр текущей активности программы" на стр. 169);
- запускать и останавливать запись файлов дампов и файлов трассировки (см. раздел "Настройка записи файлов дампов и файлов трассировки" на стр. 171);
- открывать Консоль программы;
- открывать окно **О программе** со списком установленных обновлений и доступных исправлений.

Вы можете просматривать Диагностическое окно, даже если доступ к функциям Kaspersky Embedded Systems Security защищен паролем. Введение пароля не требуется.

Диагностическое окно невозможно настроить через Kaspersky Security Center.

Просмотр статуса Kaspersky Embedded Systems Security с помощью диагностического окна

► *Чтобы открыть диагностическое окно, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
2. Выберите пункт меню **Открыть Диагностическое окно**.

   Откроется **Диагностическое окно**.

На закладке **Статус защиты** можно просмотреть текущий статус ключа, а также статус задач постоянной защиты компьютера и задач обновления. Для отображения статуса защиты используется цветовая индикация (см. таблицу ниже).

Таблица 31. Статус защиты в диагностическом окне

Подраздел	Статус

Постоянная защита компьютера	Панель *зеленого* цвета отображается при любом из следующих сценариев (может быть выполнено любое количество условий):
	• Рекомендуемая конфигурация:
	  • Задача Постоянная защита файлов запущена с параметрами по умолчанию.
	  • Задача Контроль запуска программ запущена в активном режиме с параметрами по умолчанию.
	• Приемлемая конфигурация:
	  • Задача Постоянная защита файлов настроена пользователем.
	  • Параметры задачи Контроль запуска программ изменены.

	Панель *желтого* цвета отображается, если выполнено одно или несколько из следующих условий: • Задача Постоянная защита файлов приостановлена (пользователем или согласно расписанию). • Задача Контроль запуска программ запущена в режиме **Только статистика**. • Задачи Защита от эксплойтов и Контроль запуска программ запущены в режиме **Только статистика**.
	Панель *красного* цвета отображается, если выполнены оба условия: • Компонент Постоянная защита файлов не установлен или задача остановлена / приостановлена. • Компонент Контроль запуска программ не установлен или задача запущена в режиме **Только статистика**.
Лицензирование	Панель *зеленого* цвета отображается при действующей лицензии.

Подраздел	Статус
	Панель *желтого* цвета отображается, если возникло одно из следующих событий: • **Выполняется проверка статуса лицензии**. • **До истечения срока действия лицензии остается 14 дней и не добавлен дополнительный ключ или код активации**. • **Добавленный ключ помещен в черный список и скоро будет заблокирован**.
	Панель *красного* цвета отображается, если возникло одно из следующих событий: • **Программа не активирована.** • **Срок действия лицензии истек.** • **Нарушено Лицензионное соглашение.** • **Ключ помещен в черный список.**
Обновление	Панель *зеленого* цвета отображается, если базы программы актуальны.
	Панель *желтого* цвета отображается, если базы программы устарели.
	Панель *красного* цвета отображается, если базы программы сильно устарели.

Просмотр статистики событий безопасности

На закладке **Статистика** отображаются все события безопасности. Статистика каждой задачи защиты отображается в отдельном блоке, где указано количество инцидентов, а также дата и время возникновения последнего инцидента. При регистрации инцидента цвет блока меняется на красный.

► *Чтобы просмотреть статистику, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
2. Выберите пункт меню **Открыть Диагностическое окно**.

   Откроется **Диагностическое окно**.
3. Выберите закладку **Статистика**.
4. Просмотрите инциденты безопасности для задач защиты.

Просмотр текущей активности программы

На этой закладке вы можете просматривать статус текущих задач и процессов программы, а также оперативно получать сообщения о происходящих критических событиях.

Для отображения статуса активности программы используется цветовая индикация:

- В блоке **Задачи**:
  - *Зеленый цвет*. Не выполнены условия для желтого или красного цветов.
  - *Желтый цвет*. Проверка важных областей не проводилась давно.
  - *Красный цвет*. Выполнено любое из следующих условий:
    - Ни одна задача не запущена и расписание запуска не настроено ни для одной задачи.
    - Ошибки запуска программы зарегистрированы как критические события.
- В блоке **Kaspersky Security Network**:
  - *Зеленый цвет*. Задача Использование KSN запущена.
  - *Желтый цвет*. Положение о KSN принято, но задача не запущена.

► *Чтобы просмотреть текущую активность программы на компьютере, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
2. Выберите пункт меню **Открыть Диагностическое окно**.

   Откроется **Диагностическое окно**.
3. Откройте закладку **Текущая активность программы**.
4. В блоке **Задачи** можно просмотреть следующую информацию:
   - **Проверка важных областей давно не выполнялась.**

     Это поле отображается, только если программа возвращает соответствующее предупреждение о Проверке важных областей.
   - **Выполняются сейчас.**
   - **Завершены с ошибкой.**
   - **Следующий запуск определен по расписанию.**
5. В блоке **Kaspersky Security Network** можно просмотреть следующую информацию:
   - **Использование KSN включено. Включены запросы репутации файлов** или **Защита выключена**.
   - **Статистика программы отправляется в KSN**.

     Программа отправляет данные о вредоносных программах, в том числе мошеннических, обнаруженных в ходе выполнения задачи Постоянная защита файлов и задач проверки по требованию, а также отладочную информацию о сбоях при проверке.

     Поле отображается, если в параметрах задачи Использование KSN установлен флажок **Разрешить отправку статистики Kaspersky Security Network**.

6. В блоке **Интеграция с Kaspersky Security Center** можно просмотреть следующую информацию:
   - Локальное управление разрешено.
   - Применяется политика: <имя сервера Kaspersky Security Center>.

Настройка записи файлов дампов и файлов трассировки

В диагностическом окне можно настроить запись файлов дампов и файлов трассировки.

Вы можете также настроить диагностику сбоев в Консоли программы (см. раздел "Параметры Kaspersky Embedded Systems Security в Консоли программы" на стр. 136).

► *Чтобы запустить запись файлов дампов и файлов трассировки, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
2. Выберите пункт меню **Открыть Диагностическое окно**.

   Откроется **Диагностическое окно**.
3. Откройте закладку **Диагностика сбоев**.
4. Если требуется, настройте следующие параметры трассировки:
   a. Установите флажок **Записывать отладочную информацию в файл трассировки в данной папке**.
   b. Нажмите на кнопку **Обзор** и укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файлы трассировки.

      Трассировка будет включена для всех компонентов с параметрами по умолчанию: с уровнем детализации **Отладка** и максимальным размером файла журнала – 50 МБ.
5. Если требуется, настройте следующие параметры записи файлов дампов:
   a. Установите флажок **Создавать файл дампа по результатам сбоев в этой папке**.
   b. Нажмите на кнопку **Обзор** и укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файл дампа.
6. Нажмите на кнопку **Применить**.

   Новая конфигурация будет применена.

Обновление баз и модулей Kaspersky Embedded Systems Security

Этот раздел содержит информацию о задачах обновления баз и модулей Kaspersky Embedded Systems Security, копировании обновлений и откате обновлений баз Kaspersky Embedded Systems Security, а также инструкции по настройке задач обновления баз и модулей программы.

В этом разделе

О задачах обновления

Kaspersky Embedded Systems Security предоставляет четыре задачи обновления системы: Обновление баз программы, Обновление модулей программы, Копирование обновлений и Откат обновления баз программы.

По умолчанию Kaspersky Embedded Systems Security соединяется с источником обновлений – одним из серверов обновлений "Лаборатории Касперского". Вы можете настраивать все задачи обновления (см. раздел "Настройка задач обновления" на стр. 178), кроме задачи Откат обновления баз программы. После того как вы измените параметры задачи, Kaspersky Embedded Systems Security применит их новые значения при следующем запуске задачи.

Вы не можете приостанавливать и возобновлять задачи обновления.

Обновление баз программы

По умолчанию Kaspersky Embedded Systems Security копирует базы из источника обновлений на защищаемый компьютер и сразу переходит к их использованию в выполняющейся задаче постоянной защиты компьютера. Задачи проверки по требованию переходят к использованию обновленных баз программы при последующем их запуске.

По умолчанию Kaspersky Embedded Systems Security запускает задачу Обновление баз программы каждый час.

Обновление модулей программы

По умолчанию Kaspersky Embedded Systems Security проверяет доступность обновления модулей программы на источнике обновлений. Для использования установленных программных модулей требуется перезагрузка компьютера и / или перезапуск Kaspersky Embedded Systems Security.

По умолчанию Kaspersky Embedded Systems Security запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным параметрам защищаемого компьютера). В ходе выполнения задачи программа проверяет наличие важных и плановых обновлений модулей Kaspersky Embedded Systems Security, не копируя их.

Копирование обновлений

По умолчанию в ходе выполнения задачи Kaspersky Embedded Systems Security загружает файлы обновлений баз программы и сохраняет их в указанную сетевую или локальную папку, не устанавливая их.

По умолчанию задача Копирование обновлений не выполняется.

Откат обновления баз программы

В ходе выполнения задачи Kaspersky Embedded Systems Security возвращается к использованию баз программы с ранее установленными обновлениями.

По умолчанию задача Откат обновления баз программы не выполняется.

Об обновлении программных модулей Kaspersky Embedded Systems Security

"Лаборатория Касперского" может выпускать пакеты обновлений модулей Kaspersky Embedded Systems Security. Пакеты обновлений делятся на *срочные* (или *критические*) и плановые. Срочные пакеты обновлений устраняют уязвимости и ошибки; плановые добавляют новые функции или улучшают существующие.

Срочные пакеты обновлений публикуются на серверах обновлений "Лаборатории Касперского". Вы можете настроить их автоматическую установку с помощью задачи Обновление модулей программы. По умолчанию Kaspersky Embedded Systems Security запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным параметрам защищаемого компьютера).

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматизированной установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Вы можете получать информацию о выходе плановых обновлений Kaspersky Embedded Systems Security с помощью задачи Обновление модулей программы.

Можно загружать критические обновления из интернета на каждый защищаемый компьютер или использовать один компьютер в качестве посредника, копируя на него обновления, а затем распространяя их на компьютеры сети. Чтобы копировать и сохранять обновления без их установки, используйте задачу Копирование обновлений.

Перед тем как установить обновления модулей, Kaspersky Embedded Systems Security создает резервные копии модулей, установленных ранее. Если обновление модулей программы прервется или завершится с ошибкой, Kaspersky Embedded Systems Security автоматически вернется к использованию ранее установленных программных модулей. Вы также можете откатить обновление модулей вручную до предыдущих установленных обновлений.

На время установки полученных обновлений служба Kaspersky Security автоматически останавливается, а затем снова запускается.

Об обновлении баз Kaspersky Embedded Systems Security

Базы Kaspersky Embedded Systems Security, хранящиеся на защищаемом компьютере, быстро становятся неактуальными. Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают сотни новых угроз, создают идентифицирующие их записи и включают их в обновления баз программы. Обновление баз программы представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента создания предыдущего обновления. Чтобы свести риск заражения компьютера к минимуму, рекомендуется регулярно получать обновления баз программы.

По умолчанию, если базы Kaspersky Embedded Systems Security не обновляются в течение недели с момента создания последних установленных обновлений баз, возникает событие *Базы программы устарели.* Если базы программы не обновляются в течение двух недель, возникает событие *Базы программы сильно устарели*. Информация об актуальности баз (см. раздел "Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security" на стр. 161) отображается в панели результатов узла **Kaspersky Embedded Systems Security** дерева Консоли программы. Вы можете использовать общие параметры Kaspersky Embedded Systems Security, чтобы указать другое количество дней до возникновения этих событий. Вы можете также настроить уведомления администратора об этих событиях (см. раздел "Настройка уведомлений администратора и пользователей" на стр. 219).

Kaspersky Embedded Systems Security загружает обновления баз и модулей программы с FTP или HTTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или других источников обновлений.

Можно загружать обновления на каждый защищаемый компьютер или использовать один компьютер в качестве посредника, копируя на него обновления, а затем распространяя их на компьютеры. Если вы используете программу Kaspersky Security Center для централизованного управления защитой компьютеров в организации, можно использовать Сервер администрирования Kaspersky Security Center в качестве посредника для загрузки обновлений.

Вы можете запускать задачи обновления баз программы вручную или по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 151). По умолчанию Kaspersky Embedded Systems Security запускает задачу Обновление баз программы каждый час.

Если загрузка обновлений прервется или завершится с ошибкой, Kaspersky Embedded Systems Security автоматически вернется к использованию баз с последними установленными обновлениями. В случае повреждения баз Kaspersky Embedded Systems Security можно вручную откатить базы до ранее установленных обновлений (см. раздел "Откат обновлений баз Kaspersky Embedded Systems Security" на стр. 184).

Схемы обновления баз и модулей антивирусных программ в организации

Ваш выбор источника обновлений в задачах обновления зависит от того, какую схему обновления баз и модулей антивирусных программ вы используете в организации.

Вы можете обновлять базы и модули Kaspersky Embedded Systems Security на защищаемых компьютерах по следующим схемам:

- загружать обновления напрямую из интернета на каждый защищаемый компьютер (схема 1);
- загружать обновления из интернета на компьютер-посредник и распределять обновления на другие компьютеры с этого компьютера.

Посредником может служить любой компьютер, на котором установлена одна из следующих программ:

- Kaspersky Embedded Systems Security (схема 2).
- Сервер администрирования Kaspersky Security Center (схема 3).

Обновление через компьютер-посредник позволяет не только снизить интернет-трафик, но и обеспечить дополнительную безопасность компьютеров сети..

Перечисленные схемы обновлений описаны ниже.

Схема 1. Обновление баз и модулей программы напрямую из интернета

► *Чтобы настроить получение обновлений Kaspersky Embedded Systems Security напрямую из интернета,*

на каждом защищаемом компьютере в параметрах задач Обновление баз программы и Обновление модулей программы в качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".

Вы можете указать в качестве источника обновлений другие HTTP- или FTP-серверы, которые содержат папку с файлами обновлений.

Схема 2. Обновление баз и модулей программы через один из защищаемых компьютеров

► *Чтобы настроить обновление Kaspersky Embedded Systems Security через один из защищаемых компьютеров, выполните следующие действия:*

1. Скопируйте обновления на выбранный защищаемый компьютер. Для этого выполните следующие действия:
   - На выбранном компьютере настройте параметры задачи Копирование обновлений:
     a. В качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".
     b. Укажите папку общего доступа в качестве папки, в которой будут сохранены обновления.
2. Распределите обновления на остальные защищаемые компьютеры. Для этого выполните следующие действия:
   - На каждом из защищаемых компьютеров настройте параметры задач Обновление баз программы и Обновление модулей программы (см. рис. ниже).
     a. В качестве источника обновлений укажите папку на диске компьютера-посредника, в которую вы скопировали обновления.

Kaspersky Embedded Systems Security будет получать обновления через один из защищаемых компьютеров.

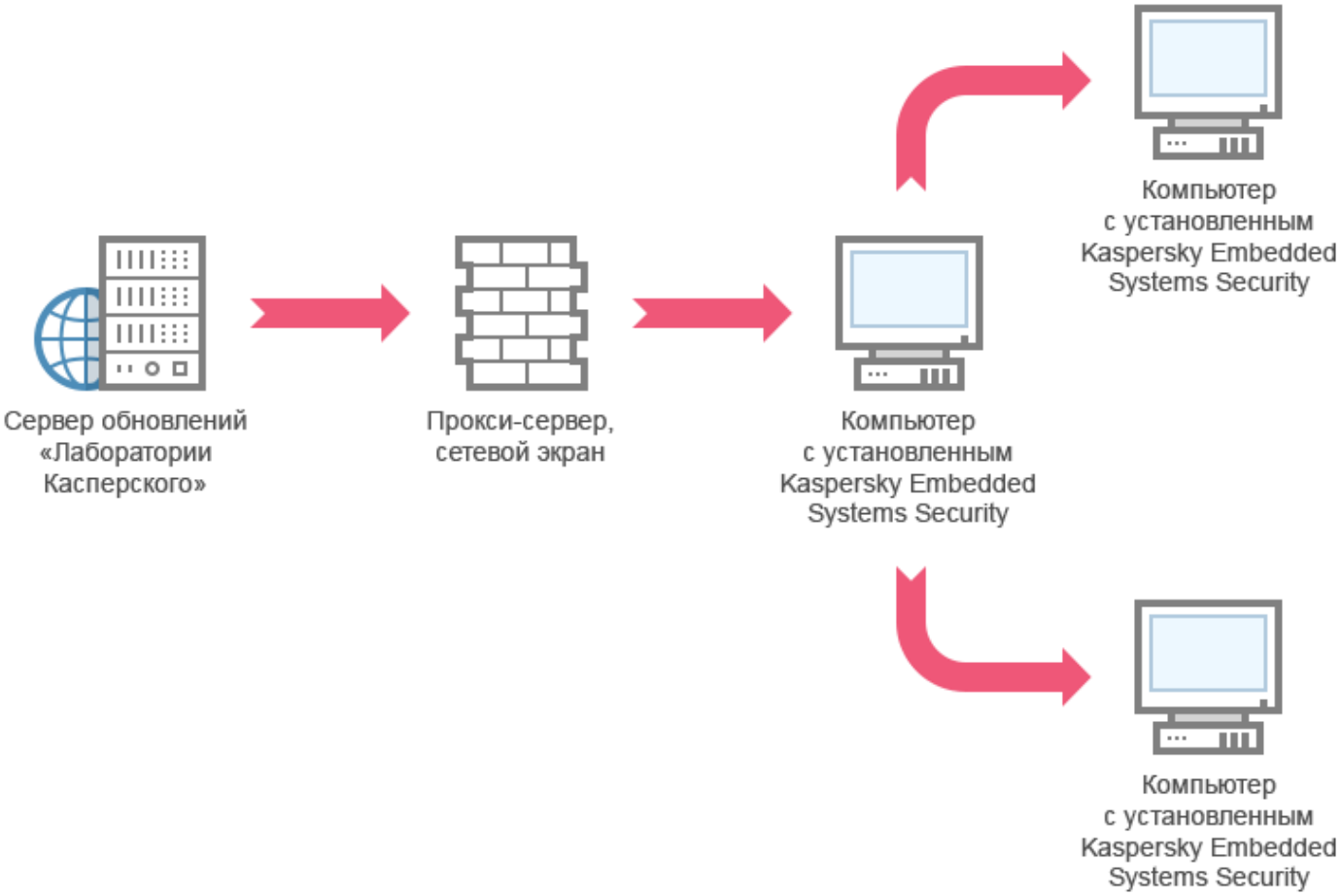

Схема 3. Обновление баз и модулей программы через Сервер администрирования Kaspersky Security Center

Если вы используете Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров, можно загружать обновления через Сервер администрирования Kaspersky Security Center, установленный в локальной сети (см. рис. ниже).

► *Чтобы настроить получение обновлений Kaspersky Embedded Systems Security через Сервер администрирования Kaspersky Security Center, выполните следующие действия:*

1. Загрузите обновления с сервера обновлений "Лаборатории Касперского" на Сервер администрирования Kaspersky Security Center. Для этого выполните следующие действия:
   - Настройте задачу Получение обновлений Сервером администрирования для указанного набора компьютеров:
     a. В качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".
2. Распределите обновления на защищаемые компьютеры. Для этого выполните одно из следующих действий:
   - В Kaspersky Security Center настройте групповую задачу обновления антивирусных баз (программных модулей) для распределения обновлений на защищаемые компьютеры:
     a. В расписании задачи укажите частоту запуска **После получения обновлений Сервером администрирования**.

Сервер администрирования будет запускать задачу каждый раз, как только он получит обновления (этот способ является рекомендуемым).

Частоту запуска **После получения обновлений Сервером администрирования** нельзя указать в Консоли программы.

- Настройте на каждом из защищаемых компьютеров задачи Обновление баз программы и Обновление модулей программы:
  a. В качестве источника обновлений укажите Сервер администрирования Kaspersky Security Center.
  b. Если требуется, настройте расписание задачи.

При редких обновлениях антивирусных баз Kaspersky Embedded Systems Security (от одного раза в месяц до одного раза в год) вероятность обнаружения угроз снижается, повышается частота ложных срабатываний компонентов программы.

Kaspersky Embedded Systems Security будет получать обновления через Сервер администрирования Kaspersky Security Center.

Если вы планируете использовать Сервер администрирования Kaspersky Security Center для распределения обновлений, предварительно установите на каждом из защищаемых компьютеров программный компонент Агент администрирования, который входит в комплект поставки программы Kaspersky Security Center. Он обеспечивает взаимодействие между Сервером администрирования и Kaspersky Embedded Systems Security на защищаемом компьютере. Подробная информация об Агенте администрирования и его настройке с помощью Kaspersky Security Center содержится в *Справке Kaspersky Security Center*.

Настройка задач обновления

Этот раздел содержит инструкции по настройке задач обновления Kaspersky Embedded Systems Security.

В этом разделе

Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security

Для каждой задачи обновления, кроме задачи Откат обновления баз программы, вы можете указать один или несколько источников обновлений, добавить пользовательские источники обновлений и настроить параметры соединения с указанными источниками обновлений.

После изменения параметров задач обновления новые значения не применяются немедленно в выполняющихся задачах обновления. Настроенные параметры вступят в силу только при последующем запуске задач.

► *Чтобы указать тип источника обновлений, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В блоке **Источник обновлений** выберите тип источника обновлений Kaspersky Embedded Systems Security:
   - **Сервер администрирования Kaspersky Security Center**

     Kaspersky Embedded Systems Security использует Сервер администрирования Kaspersky Security Center в качестве источника обновления.

     Вы можете выбрать этот вариант, если в вашей сети управление программами "Лаборатории Касперского" осуществляется с помощью системы удаленного доступа Kaspersky Security Center и на защищаемом компьютере установлен Агент администрирования – компонент Kaspersky Security Center, обеспечивающий связь компьютеров с Сервером администрирования.
   - **Серверы обновлений "Лаборатории Касперского"**

     Kaspersky Embedded Systems Security использует в качестве источника обновлений интернет-сайты "Лаборатории Касперского", на которых публикуются обновления баз и программных модулей для всех программ "Лаборатории Касперского".

     Данный вариант выбран по умолчанию.
   - **Другие HTTP-,FTP-серверы и сетевые ресурсы**

     Kaspersky Embedded Systems Security использует в качестве источника обновлений указанные администратором HTTP- или FTP-серверы или папки на серверах локальной сети.

     Вы можете сформировать список источников, которые содержат актуальный набор обновлений, нажав на ссылку **Другие HTTP-, FTP-серверы или сетевые ресурсы**.
5. Если требуется, настройте дополнительные параметры для пользовательских источников обновления:
   a. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.
      i. В открывшемся окне **Серверы обновлений** установите или снимите флажки рядом с пользовательскими источниками обновлений, чтобы начать или прекратить их использование.
      ii. Нажмите на кнопку **OK**.
   b. В блоке **Источник обновлений** на закладке **Общие** установите или снимите флажок **Использовать серверы обновлений "Лаборатории Касперского", если указанные серверы недоступны**.

      Флажок включает или выключает функцию использования серверов обновлений

"Лаборатории Касперского" в качестве источника обновлений, если выбранные вами источники обновлений недоступны.

Если флажок установлен, функция активна.

По умолчанию флажок установлен.

Вы можете установить флажок **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**, когда выбран вариант **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

6. В окне **Параметры задачи** выберите закладку **Параметры соединения**, чтобы настроить параметры соединения с источником обновлений:

   - Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.

     Флажок включает или выключает использование параметров прокси-сервера, если обновление производится с серверов "Лаборатории Касперского" или если установлен флажок **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**.

     Если флажок установлен, используются параметры прокси-сервера.

     Если флажок не установлен, параметры прокси-сервера не используются.

     По умолчанию флажок установлен.

   - Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**.

     Флажок включает или выключает использование параметров прокси-сервера, если в качестве источника обновлений выбран вариант **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

     Если флажок установлен, используются параметры прокси-сервера.

     По умолчанию флажок снят.

   Информация о настройке дополнительных параметров прокси-сервера и параметров аутентификации для доступа к прокси-серверу приведена в разделе Запуск и настройка задачи Обновление баз программы.

7. Нажмите на кнопку **OK**.

Настроенные параметры источника обновлений Kaspersky Embedded Systems Security будут сохранены и применены при последующем запуске задачи.

Вы можете управлять списком пользовательских источников обновлений Kaspersky Embedded Systems Security.

► *Чтобы отредактировать список пользовательских источников обновлений программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

Откроется окно **Параметры задачи** на закладке **Общие**.

4. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

   Откроется окно **Серверы обновлений**.

5. Выполните следующие действия:

   - Чтобы добавить новый пользовательский источник обновления, в поле ввода укажите адрес папки с файлами обновлений на FTP- или HTTP-сервере; укажите локальную или сетевую папку в формате UNC (Universal Naming Convention). Нажмите на клавишу **ENTER**.

     По умолчанию добавленная папка используется в качестве источника обновлений.

   - Чтобы отключить использование пользовательского источника, снимите флажок рядом с источником в списке.
   - Чтобы включить использование пользовательского источника, установите флажок рядом с источником в списке.
   - Чтобы изменить очередность обращения Kaspersky Embedded Systems Security к пользовательским источникам обновлений, с помощью кнопок **Вверх** и **Вниз** перемещайте выбранный источник к началу или концу списка в зависимости от того, когда он должен использоваться: до или после других источников.
   - Чтобы изменить путь к пользовательскому источнику, выберите источник в списке и нажмите на кнопку **Изменить**, выполните нужные изменения в поле ввода и нажмите на клавишу **ENTER**.
   - Чтобы удалить пользовательский источник, выберите его в списке и нажмите на кнопку **Удалить**.

     Вы не можете удалить единственный пользовательский источник из списка.

6. Нажмите на кнопку **OK**.

Изменения в списке пользовательских источников обновления программы будут сохранены.

Оптимизация использования дисковой подсистемы при выполнении задачи Обновление баз программы

При выполнении задачи Обновление баз программы Kaspersky Embedded Systems Security размещает файлы обновлений на локальном диске компьютера. Вы можете снизить нагрузку на дисковую подсистему компьютера за счет размещения файлов обновлений на виртуальном диске в оперативной памяти во время выполнения задачи обновления.

Эта функция доступна для операционных систем Microsoft Windows 7 и более поздних версий.

При использовании этой функции во время выполнения задачи Обновление баз программы в операционной системе может появиться дополнительный логический диск. Этот логический диск исчезает из операционной системы после завершения задачи.

► *Чтобы снизить нагрузку на дисковую подсистему компьютера при выполнении задачи Обновление баз программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление баз программы**.
3. В панели результатов узла **Обновление баз программы** перейдите по ссылке **Свойства**.
4. Откроется окно **Параметры задачи** на закладке **Общие**.
5. В блоке Оптимизация использования дисковой подсистемы настройте следующие параметры:
   - Снимите или установите флажок **Снизить нагрузку на дисковую подсистему**.

     Флажок включает или выключает функцию оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти.

     Если флажок установлен, функция активна.

     По умолчанию флажок снят.
   - В поле **Объем оперативной памяти, используемый для оптимизации**, укажите объем оперативной памяти в мегабайтах. Операционная система временно выделяет этот объем оперативной памяти для размещения файлов обновлений при выполнении задачи. По умолчанию установлен объем оперативной памяти 512 МБ. Минимально допустимый объем оперативной памяти 400 МБ.
6. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

Настройка параметров задачи Копирование обновлений

► *Чтобы настроить параметры задачи Копирование обновлений, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Копирование обновлений**.
3. В панели результатов узла **Копирование обновлений** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Настройка соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security" на стр. 178).
5. На закладке **Общие** в блоке **Параметры копирования обновлений** выполните следующие действия:
   - Укажите условия копирования обновлений программы:
     - **Копировать обновления баз программы**

       Kaspersky Embedded Systems Security загружает только обновления баз Kaspersky Embedded Systems Security.

       Данный вариант выбран по умолчанию.
     - **Копировать критические обновления модулей программы**

Kaspersky Embedded Systems Security загружает только срочные обновления программных модулей Kaspersky Embedded Systems Security.

- **Копировать обновления баз программы и критические обновления модулей программы**

  Kaspersky Embedded Systems Security загружает обновления баз и срочные обновления программных модулей Kaspersky Embedded Systems Security.

- Укажите локальную или сетевую папку, в которую Kaspersky Embedded Systems Security будет копировать полученные обновления.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. 151).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 154).
8. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

Настройка параметров задачи Обновление модулей программы

► *Чтобы настроить параметры задачи Обновление модулей программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление модулей программы**.
3. Перейдите по ссылке **Свойства** в панели результатов узла **Обновление модулей программы**.

   Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Настройка соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security" на стр. 178).
5. На закладке **Общие** в блоке **Параметры обновления** настройте параметры обновления модулей программы:

   - **Только проверять наличие доступных критических обновлений модулей программы**

     Kaspersky Embedded Systems Security отображает уведомление об имеющихся срочных обновлениях программных модулей без загрузки обновлений. Уведомление отображается, если включено оповещение о событиях этого типа.

     Данный вариант выбран по умолчанию.

   - **Копировать и устанавливать критические обновления модулей программы**

     Kaspersky Embedded Systems Security загружает и устанавливает критические обновления программных модулей.

   - **Разрешать перезагрузку операционной системы**

     Перезагрузка операционной системы после установки обновлений, требующих перезагрузки.

     Если флажок установлен, Kaspersky Embedded Systems Security выполняет перезагрузку операционной системы после установки обновлений, требующих

перезагрузки.

Флажок активен, если выбран вариант **Копировать и устанавливать критические обновления модулей программы**.

По умолчанию флажок снят.

- **Получать информацию о доступных плановых обновлениях модулей программы**

  Получение уведомлений обо всех имеющихся на источнике плановых обновлений программных модулях Kaspersky Embedded Systems Security. Программа отображает уведомление, если для данного типа событий включены уведомления.

  Если флажок установлен, Kaspersky Embedded Systems Security выполняет уведомление обо всех имеющихся на источнике плановых обновлениях программных модулей.

  По умолчанию флажок установлен.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. 151). По умолчанию Kaspersky Embedded Systems Security запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным параметрам защищаемого компьютера).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 154).
8. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете сами загружать их с веб-сайта "Лаборатории Касперского". Вы можете настроить уведомление администратора о событии *Доступно плановое обновление модулей программы*, в котором будет содержаться адрес страницы веб-сайта, с которой вы можете загрузить плановые обновления.

Откат обновления баз Kaspersky Embedded Systems Security

Перед применением обновления баз Kaspersky Embedded Systems Security создает резервные копии баз, которые использовались ранее. Если обновление прервалось или завершилось с ошибкой, Kaspersky Embedded Systems Security автоматически возвращается к использованию баз с ранее установленными обновлениями.

Если после обновления баз у вас возникнут проблемы, вы можете откатить базы до предыдущих установленных обновлений, запустив задачу Откат обновления баз программы.

► *Чтобы запустить задачу Откат обновления баз программы,*

перейдите по ссылке **Запустить** в панели результатов узла **Откат обновления баз программы**.

Откат обновления программных модулей

Названия параметров могут отличаться в разных операционных системах Windows.

Перед применением обновления программных модулей Kaspersky Embedded Systems Security создает резервные копии модулей, используемых в текущий момент. Если обновление модулей прервалось или завершилось с ошибкой, Kaspersky Embedded Systems Security автоматически возвращается к использованию модулей с ранее установленными обновлениями.

Чтобы откатить программные модули, используйте компонент панели управления Microsoft Windows **Установка и удаление программ**.

Статистика задач обновления

Пока выполняется задача обновления, вы можете просматривать в реальном времени информацию об объеме данных, полученных с момента запуска задачи по текущий момент, а также другую информацию о выполнении задачи.

После завершения или остановки задачи эту информацию можно просмотреть в журнале выполнения задачи.

► *Чтобы просмотреть статистику задачи обновления, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче, статистику которой вы хотите просмотреть.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Если вы просматриваете задачу Обновление баз программы или задачу Копирование обновлений, в блоке **Статистика** отображается объем данных, загруженных Kaspersky Embedded Systems Security на текущий момент (**Полученные данные**).

Если вы просматриваете задачу Обновление модулей программы, отображается информация, описанная в следующей таблице.

Таблица 32. Информация о задаче Обновление модулей программы

Поле	Описание
Полученные данные	Общий объем полученных данных
Доступно критических обновлений	Количество критических обновлений, доступных для установки
Доступно плановых обновлений	Количество плановых обновлений, доступных для установки
Ошибок применения обновлений	Если значение этого поля отличается от нуля, обновление не было применено. Вы можете просмотреть название обновления, при применении которого возникла ошибка, в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задаче Kaspersky Embedded Systems Security в журналах выполнения задач" на стр. 208).

Изолирование и резервное копирование объектов

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также информацию об изолировании возможно зараженных объектов.

В этом разделе

Изолирование возможно зараженных объектов. Карантин

Этот раздел содержит информацию об изолировании возможно зараженных объектов, то есть о помещении этих объектов на карантин, и настройке параметров карантина.

В этом разделе

Об изолировании возможно зараженных объектов

Kaspersky Embedded Systems Security перемещает объекты, которые признает возможно зараженными, из исходного местоположения в хранилище *карантина*. В целях безопасности объекты, помещённые на карантин, хранятся в зашифрованном виде.

Просмотр объектов на карантине

Вы можете просматривать объекты на карантине в узле **Карантин** Консоли программы.

► *Чтобы просмотреть объекты на карантине, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.

Информация об объектах, помещенных на карантин, отобразится в панели результатов выбранного узла.

► *Чтобы найти нужный объект в списке объектов на карантине,*

отсортируйте объекты (см. раздел "Сортировка объектов на карантине" на стр. 187) или отфильтруйте их (см. раздел "Фильтрация объектов на карантине" на стр. 187).

В этом разделе

Сортировка объектов на карантине

По умолчанию объекты в списке объектов на карантине отсортированы по дате помещения в обратном хронологическом порядке. Чтобы найти нужный объект, вы можете отсортировать объекты по содержимому столбцов с информацией об объектах. Результат сортировки сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать объекты, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты в списке.

Объекты в списке будут отсортированы по выбранному параметру.

Фильтрация объектов на карантине

Чтобы найти нужный объект на карантине, вы можете отфильтровать объекты в списке – отобразить только те объекты, которые удовлетворяют заданным вами критериям фильтрации (фильтрам). Результат фильтрации сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы задать один или несколько фильтров, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В контекстном меню названия узла выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
4. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите поле, с которым будет сравниваться значение фильтра.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут быть различными в зависимости от того, какое значение вы выберите в списке **Название поля**.

c. В поле **Значение поля** введите или выберите в списке значение фильтра.

d. Нажмите на кнопку **Добавить**.

Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите шаги a-d для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:

- Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
- Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
- Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
- Чтобы изменить фильтр, выберите фильтр из списка в окне **Параметры фильтра**. Затем измените нужные значения в полях **Имя поля**, **Оператор** или **Значение поля** и нажмите кнопку **Заменить**.

5. После добавления всех фильтров нажмите на кнопку **Применить**.

Созданные фильтры будут сохранены.

► *Чтобы снова отобразить все объекты в списке объектов на карантине,*

в контекстном меню узла **Карантин** выберите пункт **Удалить фильтр**.

Проверка объектов на карантине

По умолчанию после каждого обновления баз Kaspersky Embedded Systems Security выполняет системную задачу Проверка объектов на карантине. Параметры задачи приводятся в таблице ниже. Вы не можете изменять параметры задачи Проверка объектов на карантине.

Можно настраивать расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. 151), запускать ее вручную, а также изменять права учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 154), под управлением которой запускается задача.

Проверив объекты на карантине после обновления баз, Kaspersky Embedded Systems Security может признать некоторые из них незараженными: статус таких объектов изменится на **Ложное срабатывание**. Другие объекты Kaspersky Embedded Systems Security может признать зараженными и выполнить над ними действия, предусмотренные параметрами задачи Проверка объектов на карантине: лечить или удалять, если лечение невозможно.

Таблица 33. Параметры задачи Проверка объектов на карантине

Параметр задачи Проверка объектов на карантине	Значение
Область проверки	Папка карантина
Параметры безопасности	Единые для всей области проверки; их значения приводятся в следующей таблице.

Таблица 34. Параметры безопасности в задаче Проверка объектов на карантине

Параметр безопасности	Значение
Проверка объектов	Все объекты области проверки
Оптимизация	Выключено
Действие над зараженными и другими обнаруженными объектами	Лечить, удалять, если лечение невозможно
Действие над возможно зараженными объектами	Пропускать
Исключать объекты	Нет
Не обнаруживать	Нет
Останавливать проверку, если она длится более (сек.)	Не задано
Не проверять объекты размером более (МБ)	Не задано
Альтернативные потоки NTFS	Включена
Загрузочные секторы дисков и MBR	Выключено
Использовать технологию iChecker	Выключено
Использовать технологию iSwift	Выключено
Проверять составные объекты	• Архивы* • SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Проверка только новых и измененных файлов выключена.
Проверка подписи Microsoft у файлов	Не выполняется
Использование эвристического анализатора	Включено с уровнем анализа **Глубокий**
доверенная зона;	Не применяется

Восстановление содержимого карантина

Kaspersky Embedded Systems Security помещает возможно зараженные объекты в папку карантина в зашифрованном виде, чтобы предохранить защищаемый компьютер от их возможного вредоносного действия.

Вы можете восстановить любой объект из карантина. Это может потребоваться в следующих случаях:

- если после проверки карантина с применением обновленных баз статус объекта изменился на **Ложное срабатывание** или **Вылечен**;
- если вы считаете объект безопасным для компьютера и хотите его использовать. Чтобы Kaspersky Embedded Systems Security не изолировал этот объект при последующих проверках, вы можете исключить объект из обработки в задаче Постоянная защита файлов и в задачах проверки по требованию. Для этого укажите объект в качестве значения параметра безопасности **Исключать файлы** (по имени файла) или **Не обнаруживать** в этих задачах либо добавьте его в Доверенную зону (см. стр. 457).

При восстановлении объекта вы можете выбрать, где будет сохранен восстановленный объект: в исходном местоположении (по умолчанию), в специальной папке для восстановленных объектов на защищаемом компьютере, в указанной папке на компьютере, на котором установлена Консоль программы, или на другом компьютере в сети.

Папка для восстановления предназначена для хранения восстановленных объектов на защищаемом компьютере. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами карантина.

Восстановление объектов из карантина может привести к заражению компьютера.

Вы можете восстановить объект, сохранив его копию в папке карантина, чтобы использовать ее в дальнейшем, например, чтобы еще раз проверить объект после обновления баз.

Если объект, помещенный на карантин, входит в составной объект (например, в архив), Kaspersky Embedded Systems Security не включает его снова в составной объект при восстановлении, а сохраняет отдельно, в указанной папке.

Вы можете восстановить один или несколько объектов.

► *Чтобы восстановить объекты из карантина, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выполните одно из следующих действий:
   - Чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**.
   - Чтобы восстановить несколько объектов, выберите нужные объекты, используя клавиши **CTRL** или **SHIFT**, затем откройте контекстное меню одного из выбранных объектов и выберите пункт **Восстановить**.

   Откроется окно **Восстановление объекта**.
4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект.

Имя объекта отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке.

5. Выполните одно из следующих действий:

   - Чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**.
   - Чтобы восстановить объект в папке, которую вы задали в качестве папки для восстановления, в параметрах выберите **Восстановить в папку, используемую по умолчанию**.
   - Чтобы сохранить объект в другой папке на компьютере, на котором установлена Консоль программы, или в общей папке, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, а затем выберите нужную папку или укажите путь к ней.

6. Если вы хотите сохранить копию объекта в папке карантина после его восстановления, снимите флажок **Удалить объекты из хранилища после восстановления**.

7. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные объекты будут восстановлены и сохранены в указанное вами местоположение: если вы выбрали **Восстановить в исходную папку**, каждый из объектов будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе** – все объекты будут сохранены в одну указанную папку.

8. Нажмите на кнопку **OK**.

   Kaspersky Embedded Systems Security начнет восстанавливать первый из выбранных вами объектов.

9. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

   a. Выберите одно из следующих действий Kaspersky Embedded Systems Security:

      - **Заменить**, чтобы сохранить восстановленный объект вместо существующего;
      - **Переименовать**, чтобы сохранить восстановленный объект под другим именем. В поле ввода введите новое имя файла объекта и полный путь к нему;
      - **Переименовать, добавив суффикс**, чтобы переименовать объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

   b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие **Заменить** или **Переименовать**, добавив суффикс к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. (Если вы установили значение **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен).

   c. Нажмите на кнопку **OK**.

   Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

   Если вы не выбрали вариант **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В нем вы можете указать местоположение, в которое будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

Помещение объектов на карантин

Вы можете вручную помещать файлы на карантин.

► *Чтобы поместить файл на карантин, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Карантин**.
2. Выберите пункт **Добавить**.
3. В окне **Открыть** укажите файл, который вы хотите поместить на карантин.
4. Нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security поместит указанный файл на карантин.

Удаление объектов с карантина

Согласно параметрам задачи Проверка объектов на карантине, Kaspersky Embedded Systems Security автоматически удаляет из папки карантина объекты, статус которых при проверке карантина с использованием обновленных баз изменился на *Зараженный* и которые программа Kaspersky Embedded Systems Security не смогла вылечить. Kaspersky Embedded Systems Security не удаляет остальные объекты из карантина.

Вы можете вручную удалить из карантина один или несколько объектов.

► *Чтобы удалить из карантина один или несколько объектов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. Выполните одно из следующих действий:
   - чтобы удалить один объект, в контекстно меню названия объекта выберите пункт **Удалить**.
   - чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню на любом из выбранных объектов и выберите пункт **Удалить**.
4. В открывшемся окне нажмите на кнопку **Да**, чтобы подтвердить операцию.

Выбранные объекты будут удалены из карантина.

Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского"

Если поведение какого-нибудь файла дает вам основание подозревать в нем наличие угрозы, а Kaspersky Embedded Systems Security признает этот файл незараженным, то, возможно, вы встретились с новой, неизвестной угрозой, описание которой еще не добавлено в базы. Вы можете отправить этот файл на исследование в "Лабораторию Касперского". Вирусные аналитики "Лаборатории Касперского" проанализируют его и, если обнаружат в нем новую угрозу, добавят идентифицирующую ее запись и алгоритм лечения в базы. Возможно, когда вы вновь проверите объект после обновления баз, Kaspersky Embedded Systems Security признает его зараженным и сможет его вылечить. Вы сможете не только сохранить объект, но и предотвратить вирусную эпидемию.

Вы можете отправлять на исследование только файлы из карантина. Файлы, находящиеся на карантине, хранятся в зашифрованном виде и при пересылке не удаляются антивирусной программой, установленной на почтовом сервере.

Вы не можете отправлять объекты из карантина на исследование в "Лабораторию Касперского" после окончания срока действия лицензии.

► *Чтобы отправить файл на исследование в "Лабораторию Касперского", выполните следующие действия:*

1. Если файл не находится на карантине, предварительно **поместите его на карантин**.
2. В узле **Карантин**, в списке объектов на карантине, откройте контекстное меню файла, который вы хотите отправить на исследование в "Лабораторию Касперского", и выберите пункт **Отправить объект на исследование**.
3. В открывшемся окне подтверждения операции нажмите на кнопку **Да**, если действительно хотите отправить выбранный объект на исследование.
4. Если на компьютере, на котором установлена Консоль программы, настроен почтовый клиент, будет создано новое сообщение электронной почты. Просмотрите его, а затем нажмите на кнопку **Отправить**.

   Поле **Получатель** сообщения содержит адрес электронной почты "Лаборатории Касперского" newvirus@kaspersky.com. Поле Тема содержит текст "Объект карантина".

   Текст сообщения содержит следующую информацию: "Этот файл будет отправлен на анализ в Лабораторию Касперского". В тело сообщения вы можете включить любую дополнительную информацию о файле: почему он показался вам возможно зараженным или опасным, как он себя ведет или как влияет на систему.

   В сообщение вложен архив <имя объекта>.cab. Он содержит файл <uuid>.klq с зашифрованным объектом, файл <uuid>.txt с информацией об объекте, полученной из Kaspersky Embedded Systems Security, а также файл Sysinfo.txt, который содержит следующую информацию о Kaspersky Embedded Systems Security и операционной системе компьютера:

   - название и версию операционной системы;
   - название и версию Kaspersky Embedded Systems Security;
   - дата выпуска последних установленных обновлений баз программы;
   - активный ключ.

   Эта информация нужна вирусным аналитикам "Лаборатории Касперского", чтобы быстрее и эффективнее проанализировать файл. Однако если вы не хотите передавать ее, вы можете удалить файл Sysinfo.txt из архива.

Если почтовый клиент не установлен на компьютере, на котором установлена Консоль программы, программа предложит сохранить выбранный зашифрованный объект в файл. Этот файл вы можете переслать в "Лабораторию Касперского" самостоятельно.

► *Чтобы сохранить зашифрованный объект в файл, выполните следующие действия:*

1. В открывшемся окне с приглашением сохранить объект нажмите на кнопку **OK**.
2. Выберите папку на диске защищаемого компьютера или сетевую папку, в которую вы хотите сохранить файл с объектом.

Объект будет сохранен в файл формата CAB.

Настройка параметров карантина

Вы можете настраивать параметры карантина. Новые параметры карантина применяются сразу после сохранения.

► *Чтобы настроить параметры карантина, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Карантин**.
3. Выберите пункт **Свойства**.
4. В окне **Параметры карантина** настройте нужные параметры карантина в соответствии с вашими требованиями:
   - В блоке **Параметры карантина**:
     - **Папка карантина**

       Путь к папке карантина в формате UNC (Universal Naming Convention).

       По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Quarantine\.

     - **Максимальный размер карантина**

       Флажок включает или выключает функцию, которая отслеживает суммарный размер объектов, размещенных в карантине. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Embedded Systems Security регистрирует событие *Превышен максимальный размер карантина* и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа.

       Если флажок установлен, Kaspersky Embedded Systems Security отслеживает суммарный размер размещенных в карантине объектов.

       Если флажок снят, Kaspersky Embedded Systems Security не отслеживает суммарный размер объектов в карантине.

       По умолчанию флажок снят.

     - **Порог доступного пространства**

     Если объем объектов на карантине превышает значение максимального размера карантина или превышает порог доступного пространства, Kaspersky Embedded Systems Security уведомит вас об этом, не переставая помещать объекты на карантин.

   - В блоке **Параметры восстановления объектов**:
     - **Папка, в которую восстанавливаются объекты**

5. Нажмите на кнопку **OK**.

Настроенные параметры карантина будут сохранены.

Статистика карантина

Вы можете просматривать информацию о количестве объектов на карантине – статистику карантина.

► *Чтобы просмотреть статистику карантина,*

в дереве Консоли программы в контекстном меню узла **Карантин** выберите пункт **Статистика**.

В окне **Статистика** отображается информация о количестве объектов на карантине в текущий момент (см. таблицу ниже):

Поле	Описание
Возможно зараженных объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security признала возможно зараженными.
Текущий размер карантина	Общий объем данных в папке карантина.
Ложных срабатываний	Количество объектов, которые получили статус *Ложное срабатывание*, так как при проверке карантина с применением обновленных баз были признаны незараженными.
Вылечено объектов	Количество объектов, которые после проверки карантина получили статус *Вылеченный*.
Всего объектов	Общее количество объектов на карантине.

Резервное копирование объектов. Резервное хранилище

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также инструкции по настройке параметров резервного хранилища.

В этом разделе

О резервном копировании объектов перед лечением или удалением

Kaspersky Embedded Systems Security сохраняет зашифрованные копии объектов со статусом *зараженный* в *резервном хранилище* перед тем, как выполнить лечение или удаление этих объектов.

Если объект является частью составного объекта (например, входит в архив), Kaspersky Embedded Systems Security сохраняет составной объект в резервном хранилище полностью. Например, если Kaspersky Embedded Systems Security признал зараженным один из объектов в составе почтовой базы, он сохраняет копию всей почтовой базы.

Если объект, который Kaspersky Embedded Systems Security помещает в резервное хранилище, имеет большой размер, может произойти замедление работы системы и сокращение свободного места на жестком диске.

Вы можете восстановить файлы из резервного хранилища как в исходную папку, так и в другую папку на защищаемом или другом компьютере в локальной сети. Вы можете восстановить файл из резервного хранилища, например, если исходный зараженный или возможно зараженный файл содержал важную информацию, но при лечении этого файла программа Kaspersky Embedded Systems Security не смогла сохранить его целостность, в результате чего информация в нем стала недоступной.

Восстановление файлов из резервного хранилища может привести к заражению компьютера.

Просмотр объектов в резервном хранилище

Вы можете просматривать объекты в папке резервного хранилища только с помощью узла **Резервное хранилище** Консоли программы. Вы не можете просматривать их с помощью файловых менеджеров Microsoft Windows.

► *Чтобы просмотреть объекты в резервном хранилище,*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.

Информация об объектах, помещенных в резервное хранилище, отобразится в панели результатов выбранного узла.

► *Чтобы найти нужный объект в списке объектов в резервном хранилище,*

отсортируйте объекты или отфильтруйте их.

В этом разделе

Сортировка файлов в резервном хранилище

По умолчанию файлы в резервном хранилище отсортированы по дате их сохранения в обратном хронологическом порядке. Чтобы найти нужный файл, вы можете отсортировать файлы по содержимому любой графы в панели результатов.

Результат сортировки сохранится, если вы закроете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать файлы в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. В списке файлов в **резервном хранилище** выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты.

Файлы в резервном хранилище будут отсортированы по выбранному критерию.

Фильтрация файлов в резервном хранилище

Чтобы найти нужный файл в резервном хранилище, вы можете отфильтровать файлы – отобразить в узле **Резервное хранилище** только те файлы, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

Результат сортировки сохранится, если вы закроете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

► *Чтобы отфильтровать файлы в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
2. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите поле, со значениями которого будет сравниваться указанное вами значение фильтра при отборе.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут быть различными в зависимости от того, какое значение вы выберите в поле **Название поля**.
   c. В поле **Значение поля** введите или выберите значение фильтра.
   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите эти действия для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:

   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
   - Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.

- Чтобы отредактировать фильтр, выберите его в списке фильтров в окне **Параметры фильтра**, измените нужные значения в полях **Название поля**, **Оператор** или **Значение поля** и нажмите на кнопку **Заменить**.

После того как вы добавите все фильтры, нажмите на кнопку **Применить**. В списке отобразятся только файлы, отобранные согласно заданным фильтрам.

► *Чтобы снова отобразить все файлы в списке файлов в резервном хранилище,*

в контекстном меню узла **Резервное хранилище** выберите пункт **Снять фильтр**.

Восстановление файлов из резервного хранилища

Kaspersky Embedded Systems Security хранит файлы в папке резервного хранилища в зашифрованном виде, чтобы предохранить защищаемый компьютер от их возможного вредоносного действия.

Вы можете восстанавливать файлы из резервного хранилища.

Вам может потребоваться восстановить файл в следующих случаях:

- если исходный файл, который оказался зараженным, содержал важную информацию, при лечении файла программа Kaspersky Embedded Systems Security не смогла сохранить его целостность, и в результате информация в файле стала недоступной;
- если вы считаете файл безопасным для компьютера и хотите его использовать. Чтобы Kaspersky Embedded Systems Security не признавал файл зараженным или возможно зараженным при последующих проверках, вы можете исключить его из обработки в задаче Постоянная защита файлов и в задачах проверки по требованию. Для этого укажите файл в качестве параметра **Исключать файлы** или **Не обнаруживать** этих задач.

Восстановление файлов из резервного хранилища может привести к заражению компьютера.

При восстановлении файла вы можете выбрать, где он будет сохранен: в исходном местоположении (по умолчанию), в специальной папке для восстановленных объектов на защищаемом компьютере, в указанной папке на компьютере, на котором установлена Консоль программы, или на другом компьютере в сети.

Папка для восстановления предназначена для хранения восстановленных объектов на защищаемом компьютере. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 200).

По умолчанию, когда Kaspersky Embedded Systems Security восстанавливает файл, он сохраняет его копию в резервном хранилище. Вы можете удалить копию файла из резервного хранилища после его восстановления.

► *Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. В панели результатов узла **Резервное хранилище** выполните одно из следующих действий:
   - Чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**.

- Чтобы восстановить несколько объектов, выберите нужные объекты, используя клавиши **CTRL** или **SHIFT**, затем откройте контекстное меню одного из выбранных объектов и выберите пункт **Восстановить**.

Откроется окно **Восстановление объекта**.

4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект.

> Имя объекта отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке.

5. Выполните одно из следующих действий:

   - Чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**.
   - Чтобы восстановить объект в папке, которую вы задали в качестве папки для восстановления, в параметрах выберите **Восстановить в папку, используемую по умолчанию**.
   - Чтобы сохранить объект в другой папке на компьютере, на котором установлена Консоль программы, или в общей папке, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, а затем выберите нужную папку или укажите путь к ней.

6. Если вы не хотите сохранить копию файла в папке резервного хранилища после его восстановления, установите флажок **Удалять объекты из хранилища после восстановления** (по умолчанию флажок снят).

7. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные объекты будут восстановлены и сохранены в указанное вами местоположение: если вы выбрали **Восстановить в исходную папку**, каждый из объектов будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе** – все объекты будут сохранены в одну указанную папку.

8. Нажмите на кнопку **OK**.

   Kaspersky Embedded Systems Security начнет восстанавливать первый из выбранных вами объектов.

9. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

   a. Выберите одно из следующих действий Kaspersky Embedded Systems Security:

      - **Заменить**, чтобы сохранить восстановленный объект вместо существующего;
      - **Переименовать**, чтобы сохранить восстановленный объект под другим именем. В поле ввода введите новое имя файла объекта и полный путь к нему;
      - **Переименовать, добавив суффикс**, чтобы переименовать объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

   b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие **Заменить** или **Переименовать**, добавив суффикс к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. (Если вы установили значение **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен).

c. Нажмите на кнопку **OK**.

Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

Если вы не выбрали вариант **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В нем вы можете указать местоположение, в которое будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

Удаление файлов из резервного хранилища

► *Чтобы удалить из резервного хранилища один или несколько файлов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. Выполните одно из следующих действий:
   - чтобы удалить один объект, в контекстно меню названия объекта выберите пункт **Удалить**.
   - чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню на любом из выбранных объектов и выберите пункт **Удалить**.
4. В открывшемся окне нажмите на кнопку **Да**, чтобы подтвердить операцию.

Выбранные файлы будут удалены из резервного хранилища.

Настройка параметров резервного хранилища

► *Чтобы настроить параметры резервного хранилища, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Резервное хранилище**.
3. Выберите пункт **Свойства**.
4. В окне **Свойства резервного хранилища** настройте нужные параметры резервного хранилища в соответствии с вашими требованиями:

   В блоке **Параметры резервного хранилища**:

   - **Папка резервного хранилища**

     Путь к папке резервного хранилища в формате UNC (Universal Naming Convention).

     По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Backup\.

   - **Максимальный размер резервного хранилища (МБ)**

     Флажок включает или выключает функцию, которая отслеживает суммарный размер объектов, размещенных в папке резервного хранилища. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Embedded Systems Security регистрирует событие *Превышен максимальный размер резервного хранилища* и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа.

Если флажок установлен, Kaspersky Embedded Systems Security отслеживает суммарный размер размещенных в резервном хранилище объектов.

Если флажок снят, Kaspersky Embedded Systems Security не отслеживает суммарный размер объектов в резервном хранилище.

По умолчанию флажок снят.

- **Порог доступного пространства (МБ)**

  Флажок включает или выключает отслеживание минимального размера свободного места в резервном хранилище (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Embedded Systems Security регистрирует событие *Превышен порог свободного места в резервном хранилище* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа.

  Если флажок установлен, Kaspersky Embedded Systems Security отслеживает размер свободного места в резервном хранилище.

  Флажок Порог доступного пространства (МБ) активен, если установлен флажок Максимальный размер резервного хранилища (МБ).

  По умолчанию флажок установлен.

> Если объем объектов в резервном хранилище превышает значение максимального размера резервного хранилища или превышает порог доступного пространства, Kaspersky Embedded Systems Security уведомит вас об этом, не переставая помещать объекты в резервное хранилище.

В блоке **Параметры восстановления объектов**:

- **Папка, в которую восстанавливаются объекты**

  Путь к папке, в которую восстанавливаются объекты, в формате UNC (Universal Naming Convention).

  По умолчанию используется путь: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored\.

5. Нажмите на кнопку **OK**.

Настроенные параметры резервного хранилища будут сохранены.

Статистика резервного хранилища

Вы можете просматривать информацию о состоянии резервного хранилища в текущий момент: статистику резервного хранилища.

► *Чтобы просмотреть статистику резервного хранилища,*

в дереве Консоли программы откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Статистика**. Откроется окно **Статистика резервного хранилища**.

В окне **Статистика резервного хранилища** отображается информация о текущем состоянии резервного хранилища (см. таблицу ниже).

Таблица 35. Информация о текущем состоянии резервного хранилища

Поле	Описание
Текущий размер резервного хранилища	Объем данных в папке резервного хранилища; учитывается размер файлов в зашифрованном виде
Всего объектов	Количество объектов в резервном хранилище в текущий момент

Регистрация событий. Журналы Kaspersky Embedded Systems Security

Этот раздел содержит информацию о работе с журналами Kaspersky Embedded Systems Security: журналом системного аудита, журналами выполнения задач и журналом событий.

В этом разделе

Способы записи событий Kaspersky Embedded Systems Security

События Kaspersky Embedded Systems Security делятся на две группы:

- события, связанные с обработкой объектов в задачах Kaspersky Embedded Systems Security;
- события, связанные с управлением Kaspersky Embedded Systems Security, например: запуск программы, создание или удаление задач, запуск задач, изменение параметров задач.

Kaspersky Embedded Systems Security использует следующие способы для записи событий:

- **Журналы выполнения задач**. Журнал выполнения задачи содержит информацию о параметрах задачи, текущем состоянии задачи и событиях, возникших за время ее выполнения.
- **Журнал системного аудита**. Журнал системного аудита содержит информацию о событиях, связанных с управлением Kaspersky Embedded Systems Security.
- **Журнал событий**. Журнал событий содержит информацию о событиях, которые нужны для диагностики сбоев в работе Kaspersky Embedded Systems Security. Журнал событий доступен в Просмотре событий Microsoft Windows.
- **Журнал безопасности**. Журнал безопасности содержит информацию о событиях, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом компьютере.

Если в работе Kaspersky Embedded Systems Security возникла проблема (например, Kaspersky Embedded Systems Security или отдельная задача завершается аварийно) и вы хотите диагностировать ее, вы можете создать файл трассировки и файл дампа Kaspersky Embedded Systems Security и отправить файлы с этой информацией на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Embedded Systems Security не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Embedded Systems Security записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security. Можно настроить права доступа (см. раздел "Управление правами доступа к функциям Kaspersky Embedded Systems Security" на стр. 229) и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

Журнал системного аудита

Kaspersky Embedded Systems Security ведет системный аудит событий, связанных с управлением Kaspersky Embedded Systems Security. Программа сохраняет информацию, например, о запуске программы, запуске и остановке задач Kaspersky Embedded Systems Security, изменении параметров задач, создании и удалении задач проверки по требованию. Записи об этих событиях отображаются в панели результатов при выборе узла **Журнал системного аудита** в Консоли программы.

По умолчанию Kaspersky Embedded Systems Security хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете указать папку, в которой Kaspersky Embedded Systems Security сохраняет файлы журнала системного аудита, отличную от папки, установленной по умолчанию.

В этом разделе

Сортировка событий в журнале системного аудита

По умолчанию события отображаются в журнале системного аудита в обратном хронологическом порядке.

Вы можете отсортировать события по содержимому любой графы, кроме графы **Событие**.

► *Чтобы отсортировать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журнал системного аудита**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите

отсортировать события в списке.

Результат сортировки сохранится до следующего просмотра журнала системного аудита.

Фильтрация событий в журнале системного аудита

Вы можете отобразить в журнале системного аудита записи только о тех событиях, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

► *Чтобы отфильтровать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
3. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите графу, по которой выполняется фильтрация событий.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от пункта, выбранного в списке **Название поля**.
   c. В списке **Значение поля** выберите значение фильтра.
   d. Нажмите на кнопку **Добавить**.

      Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.
4. Если требуется, выполните одно из следующих действий:
   - Если вы хотите объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Если вы хотите объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий в журнале системного аудита.

   В списке событий журнала системного аудита отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журнала системного аудита.

► *Чтобы отключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Снять фильтр**.

   В списке событий журнала системного аудита отобразятся все события.

Удаление событий из журнала системного аудита

По умолчанию Kaspersky Embedded Systems Security хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете вручную удалить все события из журнала системного аудита.

► *Чтобы удалить события из журнала системного аудита, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Очистить**.
3. Выполните одно из следующих действий:
   - Если вы хотите перед удалением событий из журнала системного аудита сохранить содержимое журнала в файл в формате CSV или TXT, в окне подтверждения удаления нажмите на кнопку **Да**. В открывшемся окне укажите имя и местоположение файла.
   - Если вы не хотите сохранить содержимое журнала в файл, в окне подтверждения удаления нажмите на кнопку **Нет**.

Журнал системного аудита будет очищен.

Журналы выполнения задач

Этот раздел содержит информацию о журналах выполнения задач Kaspersky Embedded Systems Security и инструкции по работе с ними.

В этом разделе

О журналах выполнения задач

Информация о выполнении задач Kaspersky Embedded Systems Security отображается в панели результатов при выборе узла **Журналы выполнения задач** в Консоли программы.

В журнале выполнения каждой задачи вы можете просмотреть статистику выполнения задачи, информацию о каждом объекте, который был обработан программой с момента запуска задачи по текущий момент, а также параметры задачи.

По умолчанию Kaspersky Embedded Systems Security хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Вы можете указать папку, в которой Kaspersky Embedded Systems Security сохраняет файлы журналов выполнения задач, отличную от папки, установленной по умолчанию. Также вы можете выбрать события, записи о которых Kaspersky Embedded Systems Security сохраняет в журналах выполнения задач.

Просмотр списка событий в журналах выполнения задач

► *Чтобы просмотреть список событий в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.

Список событий, сохраненных в журналах выполнения задач Kaspersky Embedded Systems Security, отобразится в панели результатов.

Вы можете отсортировать события по содержимому любой графы или применить фильтр.

Сортировка событий в журналах выполнения задач

По умолчанию события отображаются в журналах выполнения задач в обратном хронологическом порядке. Вы можете отсортировать события по содержимому любой графы.

► *Чтобы отсортировать события в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать события в журналах выполнения задач Kaspersky Embedded Systems Security.

Результат сортировки сохранится до следующего просмотра журналов выполнения задач.

Фильтрация событий в журналах выполнения задач

Вы можете отобразить в списке событий журналов выполнения задач только записи о тех событиях, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

► *Чтобы отфильтровать события в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
3. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите графу, по которой выполняется фильтрация событий.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от пункта, выбранного в списке **Название поля**.

c. В списке **Значение поля** выберите значение фильтра.

d. Нажмите на кнопку **Добавить**.

Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.

4. Если требуется, выполните одно из следующих действий:

- Если вы хотите объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
- Если вы хотите объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.

5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий в списке событий журналов выполнения задач.

В списке событий журналов выполнения задач отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журналов выполнения задач.

► *Чтобы отключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Снять фильтр**.

В списке событий журналов выполнения задач отобразятся все события.

Просмотр статистики и информации о задачах Kaspersky Embedded Systems Security в журналах выполнения задач

В журналах выполнения задач вы можете просмотреть подробную информацию обо всех событиях, возникших в задачах с момента их запуска по текущий момент, а также статистику выполнения задач и параметры задач.

► *Чтобы просмотреть статистику и информацию о задаче Kaspersky Embedded Systems Security, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:

- двойным щелчком мыши на событии, которое возникло в задаче, журнал которой вы хотите просмотреть;
- откройте контекстное меню события, которое возникло в задаче, журнал которой вы хотите просмотреть, и выберите пункт **Просмотреть журнал**.

4. В открывшемся окне отображается следующая информация:

- на закладке **Статистика** отображается время запуска и завершения задачи и ее статистика;
- на закладке **События** отображается список событий, зафиксированных при выполнении задачи;
- на закладке **Параметры** отображаются параметры задачи.

5. Если требуется, нажмите на кнопку **Фильтр**, чтобы отфильтровать события в журнале выполнения задачи.
6. Если требуется, нажмите на кнопку **Экспорт**, чтобы экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.
7. Нажмите на кнопку **Закрыть**.

Окно **Журнал выполнения** будет закрыто.

Экспорт информации из журнала выполнения задачи

Вы можете экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.

► *Чтобы экспортировать информацию из журнала выполнения задачи, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:
   - двойным щелчком мыши на событии, которое возникло в задаче, журнал которой вы хотите просмотреть;
   - откройте контекстное меню события, которое возникло в задаче, журнал которой вы хотите просмотреть, и выберите пункт **Просмотреть журнал**.
4. В нижней части окна **Журнал выполнения** нажмите на кнопку **Экспорт**.

   Откроется окно **Сохранить как**.
5. Укажите имя, местоположение, тип и кодировку файла, в который вы хотите экспортировать информацию из журнала выполнения задачи.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры будут сохранены.

Удаление событий из журналов выполнения задач

По умолчанию Kaspersky Embedded Systems Security хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Вы можете вручную удалить все события из журналов выполнения задач, завершившихся на данный момент.

> События из журналов для задач, выполняющихся в данный момент, и для задач, используемых другими пользователями, удалены не будут.

► *Чтобы удалить события из журналов выполнения задач, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. Выполните одно из следующих действий:
   - Если вы хотите удалить события из всех журналов выполнения задач, завершившихся на данный момент, откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Очистить**.
   - Если вы хотите очистить журнал выполнения отдельной задачи, в панели результатов откройте контекстное меню события, произошедшего в задаче, журнал выполнения которой вы хотите очистить, и выберите пункт **Удалить**.
   - Если вы хотите очистить журналы выполнения нескольких задач, выполните следующие действия:
     a. В панели результатов с помощью клавиш **Ctrl** или **Shift** выберите события, произошедшие в задачах, журналы выполнения которых вы хотите очистить.
     b. Откройте контекстное меню любого выбранного события и выберите пункт **Удалить**.
4. В окне подтверждения удаления нажмите на кнопку **Да**, чтобы подтвердить удаление.

Выбранные журналы выполнения задач будут очищены. Удаление событий из журналов выполнения задач будет зарегистрировано в журнале системного аудита.

Журнал безопасности

Kaspersky Embedded Systems Security ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом компьютере. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.
- Критические события компонента Анализ журналов.
- Критические события, свидетельствующие о попытке нарушения безопасности (для задач постоянной защиты компьютера, проверки по требованию, мониторинга файловых операций, контроля запуска программ и контроля устройств).

Вы можете очистить журнал безопасности и журнал системного аудита (см. раздел "Удаление событий из журнала системного аудита" на стр. 205). При этом Kaspersky Embedded Systems Security регистрирует событие системного аудита об очистке журнала безопасности.

Просмотр журнала событий Kaspersky Embedded Systems Security в оснастке Просмотр событий

С помощью оснастки Просмотр событий для Microsoft Management Console вы можете просматривать журнал событий Kaspersky Embedded Systems Security. В нем Kaspersky Embedded Systems Security регистрирует события, которые нужны для диагностики сбоев в работе Kaspersky Embedded Systems Security.

Вы можете выбирать события для записи в журнал событий на основе следующих критериев:

- **по типам событий;**
- **по уровню детализации**. Уровень детализации соответствует уровню важности событий, которые регистрируются в журнале (информационные, важные или критические события). Наиболее подробным является уровень Информационные события, при котором регистрируются события всех уровней важности; наименее подробным является уровень Критические события, при котором регистрируются только критические события. По умолчанию для всех компонентов кроме компонента Обновление установлен уровень детализации Важные события (регистрируются только важные и критические события); для компонента Обновление установлен уровень Информационные события.

► *Чтобы просмотреть журнал событий Kaspersky Embedded Systems Security, выполните следующие действия:*

1. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.

   Откроется окно Microsoft Management Console.

2. Выберите **Файл** > **Добавить или удалить оснастку**.

   Откроется окно **Добавление и удаление оснасток**.

3. В списке доступных оснасток выберите оснастку **Просмотр событий** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор компьютера**.

4. В окне **Выбор компьютера** укажите компьютер, на котором установлен Kaspersky Embedded Systems Security, и нажмите на кнопку **ОК**.

5. В окне **Добавление и удаление оснасток** нажмите на кнопку **ОК**.

   В дереве Microsoft Management Console появится узел **Просмотр событий**.

6. В дереве Консоли раскройте узел **Просмотр событий** и выберите вложенный узел **Журналы приложений и служб** > **Kaspersky Embedded Systems Security.**

Откроется журнал событий Kaspersky Embedded Systems Security.

Настройка параметров журналов в Консоли Kaspersky Embedded Systems Security

Вы можете настраивать следующие параметры журналов Kaspersky Embedded Systems Security:

- длительность хранения событий в журналах выполнения задач и журнале системного аудита;
- местоположение папки, в которой Kaspersky Embedded Systems Security сохраняет файлы журналов выполнения задач и журнала системного аудита;
- пороги формирования событий *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей давно не выполнялась*;

- события, которые Kaspersky Embedded Systems Security сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Embedded Systems Security в оснастке Просмотр событий.
- параметры публикации событий аудита и событий выполнения задач по протоколу syslog на syslog-сервер.

► *Чтобы настроить параметры журналов Kaspersky Embedded Systems Security, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. В окне **Параметры журналов и уведомлений** настройте параметры журналов в соответствии с вашими требованиями. Для этого выполните следующие действия:

   - На закладке **Общие**, если требуется, выберите события, которые Kaspersky Embedded Systems Security сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Embedded Systems Security в оснастке Просмотр событий. Для этого выполните следующие действия:

     - В списке **Компонент** выберите функциональный компонент Kaspersky Embedded Systems Security, уровень детализации событий которого вы хотите указать.

     Для задач Постоянная защита файлов и задач проверки по требованию, а также для компонента Обновление предусмотрена запись событий в журналы выполнения задач и журнал событий. Для этих компонентов таблица событий содержит графы **Журнал выполнения задачи** и **Журнал событий Windows**. Для компонентов Карантин и Резервное хранилище события записываются в журнал системного аудита и журнал событий. Для этих компонентов таблица событий содержит графы **Аудит** и **Журнал событий Windows**.

     - В списке **Уровень важности** выберите уровень детализации событий в журналах выполнения задач, журнале системного аудита и журнале событий для выбранного функционального компонента.

       В таблице списка событий ниже установлены флажки рядом с событиями, которые регистрируются в журналах выполнения задач, журнале системного аудита и журнале событий в соответствии с выбранным уровнем детализации.

     - Если вы хотите вручную включить запись отдельных событий для выбранного функционального компонента, выполните следующие действия:

     a. В списке **Уровень важности** выберите **Другой**.

     b. В таблице списка событий установите флажки рядом с теми событиями, запись которых в журналы выполнения задач, журнал системного аудита и журнал событий вы хотите включить.

- На закладке **Дополнительно** настройте параметры хранения журналов и пороги формирования событий о статусе защиты компьютера:
  - В блоке **Хранение журналов**:
    - **Папка журналов**

      Путь к папке с журналами в формате UNC (Universal Naming Convention).

      По умолчанию используется путь C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports\.

      Если используемый по умолчанию путь изменен, создается папка с соответствующим именем. Новые файлы журнала будут сохранены в новую папку. Созданные ранее файлы журнала останутся в старой папке.
    - **Удалять журналы выполнения задач старше чем (дни)**

      Флажок включает или выключает функцию, которая удаляет журналы с результатами выполнения завершенных задач и событиями, опубликованными в журналах выполняющихся задач, по истечении заданного периода времени (по умолчанию 30 дней).

      Если флажок установлен, Kaspersky Embedded Systems Security удаляет журналы с результатами выполнения завершенных задач и событиями, опубликованными в журналах выполняющихся задач, по истечении заданного периода времени.

      По умолчанию флажок установлен.
    - **Удалять из журнала системного аудита события старше чем (дни)**

      Флажок включает или выключает функцию, которая удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени (по умолчанию 60 дней).

      Если флажок установлен, Kaspersky Embedded Systems Security удаляет события, зарегистрированные в журнале системного аудита, по истечении заданного периода времени.

      По умолчанию флажок снят.
  - В блоке **Пороги формирования событий**:
    - Укажите количество дней, по истечении которого будут регистрироваться события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей давно не выполнялась*.

Таблица 36. Пороги формирования событий

Параметр	Пороги формирования событий.
Описание	Вы можете указать пороги формирования событий следующих типов: *Базы программы устарели* и *Базы программы сильно устарели*. Событие возникает, если базы Kaspersky Embedded Systems Security не обновлялись в течение указанного параметром количества дней с момента выпуска последних установленных обновлений баз. Вы можете настроить уведомление администратора об этих событиях. *Проверка важных областей давно не выполнялась*. Событие возникает, если в течение указанного количества дней не выполнялась ни одна из задач, отмеченных флажком **Считать выполнение задачи проверкой важных областей**.

Возможные значения	Количество дней от 1 до 365.
Значение по умолчанию	Базы программы устарели – 7 дней. Базы программы сильно устарели – 14 дней. Проверка важных областей давно не выполнялась – 30 дней.

- На закладке **Интеграция с SIEM** настройте параметры публикации событий аудита и событий выполнения задач (см. раздел "Настройка параметров интеграции с SIEM" на стр. 215) на syslog-сервере.

3. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

В этом разделе

Об интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и снизить риск деградации системы в результате увеличения объемов журналов программы, вы можете настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он собирает и анализирует полученные события, а также выполняет другие действия в рамках управления журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: этот режим предполагает, что все события выполнения задач, публикация которых настроенная в параметрах журналов, а также все события системного аудита продолжают храниться на локальном компьютере даже после отправки в SIEM.

  Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемый компьютер.

- Удалять локальные копии событий: этот режим предполагает, что все события, зарегистрированные в ходе работы программы и опубликованные в SIEM, будут удалены с локального компьютера.

  Программа никогда не удаляет локальные версии журнала безопасности.

Kaspersky Embedded Systems Security может конвертировать события в журналах программы в форматы, поддерживаемые syslog-сервером, для передачи событий и их успешного распознавания на стороне SIEM. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Рекомендуется выбирать формат событий на основе конфигурации используемой SIEM.

Параметры надежности

Вы можете снизить риск неудачной отправки событий в SIEM задав параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если не удается подключиться к основному syslog-серверу или использовать его.

Также Kaspersky Embedded Systems Security уведомляет вас о неудачной попытке подключения к SIEM и об ошибках отправки событий в SIEM с помощью событий системного аудита.

Настройка параметров интеграции с SIEM

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и отключать интеграцию с SIEM, а также настраивать параметры функциональности (см. таблицу ниже).

Таблица 37. Параметры интеграции с SIEM

Параметр	Значение по умолчанию	Описание
Отправлять события по протоколу syslog на внешний syslog-сервер	Не применяется	Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка.
Удалять локальные копии событий при записи на внешний syslog-сервер	Не применяется	Вы можете настраивать параметры хранения локальных копий журналов, после их отправки в SIEM с помощью установки или снятия флажка.
Формат событий	Структурированные данные	Вы можете выбирать один из двух форматов, в которые программа конвертирует свои события перед их отправкой на syslog-сервер для лучшего распознавания этих событий на стороне SIEM.
Протокол подключения	TCP	Вы можете настроить подключение к основному и дополнительному syslog-серверам по протоколам UPD или TCP с помощью выпадающего списка.
Параметры подключения к основному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.
Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен	Не применяется	Вы можете включать и отключать применение зеркального syslog-сервера с помощью флажка.

Параметр	Значение по умолчанию	Описание
Параметры подключения к дополнительному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к дополнительному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.

► *Чтобы настроить параметры интеграции с SIEM, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления**.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.
3. Выберите закладку **Интеграция с SIEM**.
4. В блоке **Параметры интеграции** установите флажок **Отправлять события по протоколу syslog на внешний syslog-сервер**.

   Флажок включает или отключает использование функциональности отправки публикуемых событий на внешний syslog-сервер.

   Если флажок установлен, программа выполняет отправку публикуемых событий в SIEM в соответствии с настроенными параметрами интеграции с SIEM.

   Если флажок снят, программа не выполняет интеграцию с SIEM. Вы не можете настраивать параметры интеграции SIEM, если флажок снят.

   По умолчанию флажок снят.
5. Если требуется, установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер** в блоке **Параметры интеграции**.

   Флажок включает или отключает удаление локальных копий журналов по их отправке в SIEM.

   Если флажок установлен, программа удаляет локальные копии событий после того, как они были успешно опубликованы в SIEM. Рекомендуется использовать этот режим на маломощных компьютерах.

   Если флажок снят, программа только отправляет события в SIEM. Копии журналов продолжают храниться локально.

   По умолчанию флажок снят.

   Статус флажка **Удалять локальные копии событий при записи на внешний syslog-сервер** не влияет на параметры хранения событий журнала безопасности: программа никогда не удаляет события журнала безопасности автоматически.
6. В блоке **Формат событий** укажите формат, в который вы хотите конвертировать события по работе программы для их отправки в SIEM.

   По умолчанию программа выполняет конвертацию в формат структурированных данных.
7. В блоке **Параметры соединения**:

- Укажите протокол подключения к SIEM.
- Укажите параметры соединения с основным syslog-сервером.

  Вы можете указать IP-адрес только в формате IPv4.
- Установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если вы хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер недоступна.
  - Укажите следующие параметры подключения к зеркальному syslog-серверу: **IP-адрес** и **Порт**.

    Поля **IP-адрес** и **Порт** для зеркального syslog-сервера недоступны для редактирования, если снят флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**.

    Вы можете указать IP-адрес только в формате IPv4.

8. Нажмите на кнопку **OK**.

   Настроенные параметры интеграции с SIEM будут применены.

Настройка уведомлений

Этот раздел содержит информацию о возможных способах уведомления пользователей и администраторов Kaspersky Embedded Systems Security о событиях программы и состоянии защиты компьютера, а также инструкцию по настройке уведомлений.

В этом разделе

Способы уведомления администратора и пользователей

Вы можете настроить уведомление администратора и пользователей, которые обращаются к защищаемому компьютеру, о событиях, связанных с работой Kaspersky Embedded Systems Security и состоянием антивирусной защиты компьютера.

Программа обеспечивает выполнение следующих задач:

- Администратор может получать информацию о событиях выбранных типов.
- Пользователи локальной сети, которые обращаются к защищаемому компьютеру, и пользователи терминальных компьютеров могут получать информацию о событиях типа *Обнаружен объект*, возникших в задаче Постоянная защита файлов.

В Консоли программы можно активировать уведомления администратора или пользователей несколькими способами:

- Способы уведомления пользователей:
  a. Средства службы терминалов.

     Вы можете применять этот способ для оповещения пользователей терминалов, если защищаемый компьютер используется в качестве терминала.

  b. Средства службы сообщений.

     Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows.
- Способы уведомления администраторов:
  a. Средства службы сообщений.

     Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows.

  b. Запуск исполняемого файла.

     При возникновении события запускается исполняемый файл, который хранится на локальном диске защищаемого компьютера.

  c. Отправка по электронной почте.

     Этот способ использует для передачи сообщений электронную почту.

Вы можете создавать текст сообщений для отдельных типов событий. В него вы можете включать поля с информацией о событии. По умолчанию для уведомлений пользователей используется стандартный текст сообщений.

Настройка уведомлений администратора и пользователей

Настройка уведомлений о событии предполагает выбор и настройку способа уведомлений, а также составление текста сообщения.

► *Чтобы настроить уведомления о событиях, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. На закладке **Уведомления** укажите способы уведомлений:

   a. В списке **Тип события** выберите событие, для которого вы хотите выбрать способ уведомления.

   b. В группе параметров **Уведомление администраторов** или **Уведомление пользователей** установите флажок рядом со способами уведомлений, которые вы хотите использовать.

   > Уведомление пользователя можно настроить только для следующих событий: **Обнаружен объект**, **Обнаружено и заблокировано недоверенное запоминающее устройство** и **Недоверенный узел в списке**.

3. Если вы хотите составить текст сообщения, выполните следующие действия:

   a. Нажмите на кнопку **Текст сообщения**.

   b. В открывшемся окне введите текст, который будет отображаться в сообщении о событии.

   > Вы можете составить один текст сообщения для нескольких типов событий: после того как вы выбрали способ уведомлений для одного типа событий, выберите остальные типы событий, для которых вы хотите составить такой же текст сообщения, используя клавиши **Ctrl** или **Shift**, а затем нажмите на кнопку **Текст сообщения**.

   c. Чтобы добавить поля с информацией о событии, нажмите на кнопку **Макрос** и выберите нужные пункты из раскрывающегося списка. Поля с информацией о событиях описаны в таблице в этом разделе.

   d. Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **По умолчанию**.

4. Чтобы настроить способы уведомления администраторов о выбранном событии, в блоке **Уведомление администраторов** выберите закладку **Уведомления**, нажмите на кнопку **Настройка** и в окне **Дополнительные параметры** выполните настройку выбранных способов. Для этого выполните следующие действия:

   a. Для уведомлений по электронной почте откройте закладку **Электронная почта** и в соответствующих полях укажите адреса электронной почты получателей (разделяйте адреса символом "точка с запятой"), имя или сетевой адрес SMTP-сервера, а также его порт. Если требуется, укажите текст, который будет отображаться в полях **Тема** и **От**. В текст поля **Тема** можно также добавлять переменные с информацией о событии (см. таблицу ниже).

      Если вы хотите использовать проверку подлинности по учетной записи при соединении с SMTP-сервером, в группе **Параметры аутентификации** установите флажок **Использовать SMTP-аутентификацию** и укажите имя и пароль пользователя, учетная запись которого будет проверяться.

b. Для уведомлений средствами службы сообщений Windows на закладке **Служба сообщений Windows** составьте список компьютеров-получателей уведомлений: для каждого компьютера, который вы хотите добавить, нажмите на кнопку **Добавить** и в поле ввода введите его сетевое имя.

c. Для запуска исполняемого файла на закладке **Исполняемый файл** выберите на локальном диске защищаемого компьютера файл, который будет выполняться на компьютере при возникновении события, или введите полный путь к нему. Введите имя и пароль пользователя, под учетной записью которого файл будет выполняться.

   Указывая путь к исполняемому файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

   Если вы хотите ограничить количество уведомлений по событиям одного типа в единицу времени, на закладке **Дополнительно** установите флажок **Не отправлять одно и то же уведомление чаще** и укажите нужное количество раз и единицу времени.

5. Нажмите на кнопку **OK**.

Настроенные параметры уведомлений будут сохранены.

Таблица 38. Поля с информацией о событии

Переменная	Описание
%EVENT_TYPE%	Тип события.
%EVENT_TIME%	Время возникновения события.
%EVENT_SEVERITY%	Уровень важности события.
%OBJECT%	Имя объекта (в задачах постоянной защиты компьютера и проверки по требованию). В задаче Обновление модулей программы включает название обновления и адрес страницы в интернете с информацией об обновлении.
%VIRUS_NAME%	Имя объекта согласно классификации Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/. Это имя входит в полное название обнаруженного объекта, которое Kaspersky Embedded Systems Security возвращает при обнаружении объекта. Вы можете просмотреть полное имя обнаруженного объекта в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задаче Kaspersky Embedded Systems Security в журналах выполнения задач" на стр. 208).
%VIRUS_TYPE%	Тип обнаруженного объекта по классификации "Лаборатории Касперского", например, "вирус" или "троянская программа". Входит в полное название обнаруженного объекта, которое Kaspersky Embedded Systems Security возвращает, признав объект зараженным или возможно зараженным. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.
%USER_COMPUTER%	В задаче постоянной защиты файлов имя компьютера пользователя, который обратился к объекту на компьютере.
%USER_NAME%	В задаче постоянной защиты файлов имя пользователя, который обратился к объекту на компьютере.

Переменная	Описание
%FROM_COMPUTER%	Имя защищаемого компьютера, с которого поступило уведомление.
%EVENT_REASON%	Причина возникновения события (некоторые события не имеют этого поля).
%ERROR_CODE%	Код ошибки (применяется только для события "внутренняя ошибка задачи").
%TASK_NAME%	Название задачи (имеется только у событий, связанных с выполнением задач).

Запуск и остановка Kaspersky Embedded Systems Security

Этот раздел содержит информацию о запуске Консоли программы, а также о запуске и остановке службы Kaspersky Security.

В этом разделе

Запуск Плагина управления Kaspersky Embedded Systems Security

Для запуска Плагина управления Kaspersky Embedded Systems Security в Kaspersky Security Center дополнительных действий не требуется. После установки Плагина управления на компьютер администратора, он запускается одновременно с Kaspersky Security Center. Подробная информация о запуске Kaspersky Security Center содержится в *Справке Kaspersky Security Center*.

Запуск Консоли Kaspersky Embedded Systems Security из меню Пуск

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы запустить Консоль программы из меню **Пуск**,*

1. в меню **Пуск** выберите **Программы** > **Kaspersky Embedded Systems Security** > **Средства администрирования** > **Консоль Kaspersky Embedded Systems Security**.

Чтобы добавить в Консоль программы другие оснастки, запустите Консоль программы в авторском режиме.

► *Чтобы запустить Консоль программы в авторском режиме, выполните следующие действия:*

1. В меню **Пуск** выберите **Программы** > **Kaspersky Embedded Systems Security** > **Средства администрирования**.
2. В контекстном меню Консоли программы выберите команду **Автор**.

Консоль программы будет запущена в авторском режиме.

При запуске Консоли программы на защищаемом компьютере откроется окно Консоли программы.

Если вы запустили Консоль программы не на защищаемом, а на другом компьютере, подключитесь к защищаемому компьютеру.

► *Чтобы подключиться к защищаемому компьютеру, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите команду **Подключиться к другому компьютеру**.

   Откроется окно **Выбор компьютера**.
3. В открывшемся окне выберите **Другой компьютер**.
4. В поле ввода справа укажите сетевое имя защищаемого компьютера.
5. Нажмите на кнопку **OK**.

Консоль программы будет подключена к защищаемому компьютеру.

Если учетная запись, которую вы использовали для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management на компьютере, установите флажок **Установить соединение с правами учетной записи** и укажите другую учетную запись, которая обладает такими правами.

Запуск и остановка службы Kaspersky Security

По умолчанию служба Kaspersky Security запускается автоматически сразу после операционной системы. Служба Kaspersky Security управляет рабочими процессами, в которых выполняются задачи постоянной защиты компьютера, контроля компьютера, проверки по требованию и обновления.

По умолчанию при запуске Kaspersky Embedded Systems Security запускаются задачи Постоянная защита файлов и Проверка при запуске операционной системы, а также другие задачи, в расписании которых указана частота запуска **При запуске программы**.

Если вы остановите службу Kaspersky Security, все выполняющиеся задачи будут остановлены. После того как вы снова запустите службу Kaspersky Security, программа автоматически запустит только задачи, в расписании которых указана частота запуска **При запуске программы**, остальные задачи требуется запустить вручную.

Вы можете запускать и останавливать службу Kaspersky Security с помощью контекстного меню узла **Kaspersky Embedded Systems Security** или с помощью оснастки "Службы Microsoft Windows".

Вы можете запускать и останавливать Kaspersky Embedded Systems Security, если вы входите в группу "Администраторы" на защищаемом компьютере.

► *Чтобы остановить или запустить программу с помощью Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите одну из следующих команд:
   - **Остановка службы**
   - **Запуск службы**

Служба Kaspersky Security будет запущена или остановлена.

Запуск компонентов Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы

В этом разделе приведена информация о работе Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы.

В этом разделе

О работе Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы

Компоненты Kaspersky Embedded Systems Security можно запустить при загрузке операционной системы в безопасном режиме. При загрузке операционной системы наряду со службой Kaspersky Security (kavfs.exe) загружается драйвер klam.sys, используемый для регистрации службы Kaspersky Security как защищённой службы. Дополнительные сведения приведены в разделе Регистрация службы Kaspersky Security как защищённой службы.

Kaspersky Embedded Systems Security можно запустить при загрузке операционной системы в следующих безопасных режимах:

- Безопасный режим с типом загрузки "Минимальная" – стандартный вариант безопасного режима загрузки операционной системы. При этом Kaspersky Embedded Systems Security может запускать следующие компоненты:
  - Постоянная защита файлов.
  - Проверка по требованию.
  - Контроль запуска программ и Формирование правил контроля запуска программ.
  - Анализ журналов.
  - Мониторинг файловых операций.
  - Проверка целостности программы.
- Безопасный режим с типом загрузки "Сеть" – загрузка операционной системы в безопасном режиме с поддержкой сетевых драйверов. Помимо компонентов, запускаемых в безопасном режиме с типом загрузки "Минимальная", Kaspersky Embedded Systems Security может запускать следующие компоненты:
  - Обновление баз программы.
  - Обновление модулей программы.

Запуск Kaspersky Embedded Systems Security в безопасном режиме

По умолчанию, Kaspersky Embedded Systems Security не запускается при загрузке операционной системы в безопасном режиме.

► *Чтобы запустить Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы, выполните следующие действия:*

1. Запустите редактор реестра Windows (C:\Windows\regedit.exe).
2. В системном реестре откройте ключ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Откройте параметр LoadInSafeMode.
4. Задайте значение `1`.
5. Нажмите на кнопку **OK**.

► *Чтобы отменить запуск Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы, выполните следующие действия:*

1. Запустите редактор реестра Windows (C:\Windows\regedit.exe).
2. В системном реестре откройте ключ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Откройте параметр LoadInSafeMode.
4. Задайте значение `0`.
5. Нажмите на кнопку **OK**.

Механизмы самозащиты Kaspersky Embedded Systems Security

Этот раздел содержит информацию о механизмах самозащиты Kaspersky Embedded Systems Security.

В этом разделе

О механизмах самозащиты Kaspersky Embedded Systems Security

В Kaspersky Embedded Systems Security реализованы механизмы самозащиты, обеспечивающие защиту от изменения или удаления с жесткого диска папок программы, процессов памяти и записей системного реестра.

Защита от изменений папок с установленными компонентами Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security запрещает всем пользователям переименовывать и удалять папки с установленными компонентами программы. По умолчанию используются следующие пути к папкам установки программы:

- В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- В 64-х разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

Защита от изменений ключей реестра Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security ограничивает доступ к следующим ключам и ветвям реестра, обеспечивающим загрузку драйверов и служб программы:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\CrashDump] (в 64-разрядной версии Microsoft Windows)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace] (в 64-разрядной версии Microsoft Windows)

Права на изменение этих ветвей и ключей реестра имеют только пользователи с учетной записью Локальная система (SYSTEM). Пользователи с учетными записями Пользователь и Администратор имеют права только на чтение.

Регистрация службы Kaspersky Security как защищённой службы

Технология *Protected Process Light* (далее также "PPL") гарантирует, что операционная система выполняет загрузку только доверенных служб и процессов. Для того чтобы запустить службу как доверенную, необходимо, чтобы на защищаемом компьютере был установлен драйвер *Early Launch Antimalware*.

Драйвер *Early Launch Antimalware* (далее также "ELAM") обеспечивает защиту компьютеров в сети при их включении и при инициализации драйверов сторонних производителей.

Драйвер ELAM устанавливается автоматически во время установки Kaspersky Embedded Systems Security и используется для регистрации службы Kaspersky Security как защищённой во время запуска операционной системы. Когда служба Kaspersky Security (KAVFS) запускается как системный защищенный процесс, другие незащищенные процессы в системе не могут внедрять потоки, записывать в виртуальную память защищённого процесса и останавливать службу.

При запуске процесса как защищённого пользователь не может управлять им, независимо от прав пользователя. Регистрация службы Kaspersky Security как защищённой с помощью драйвера ELAM поддерживается операционной системой Microsoft Windows 10 и более поздними версиями. Если программа Kaspersky Embedded Systems Security установлена на сервер под управлением операционной системы, поддерживающей PPL, управление правами пользователей для службы Kaspersky Security (KAVFS) будет недоступно.

► *Чтобы установить Kaspersky Embedded Systems Security как защищённый процесс, выполните следующую команду:*

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Управление правами доступа к функциям Kaspersky Embedded Systems Security

Этот раздел содержит информацию о правах на управление Kaspersky Embedded Systems Security и службами Windows, которые регистрирует программа, а также инструкции по настройке этих прав.

В этом разделе

О правах на управление Kaspersky Embedded Systems Security

По умолчанию доступ ко всем функциям Kaspersky Embedded Systems Security имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере, пользователи группы ESS Administrators, созданной на защищаемом компьютере при установке Kaspersky Embedded Systems Security, а также группа SYSTEM.

Пользователи, которые имеют доступ к функции **Изменение прав** Kaspersky Embedded Systems Security, могут предоставлять доступ к функциям Kaspersky Embedded Systems Security другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Пользователи, не зарегистрированные в списке пользователей Kaspersky Embedded Systems Security, не могут открыть Консоль программы.

Вы можете выбрать для пользователя или группы пользователей один из следующих стандартных уровней доступа:

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры Kaspersky Embedded Systems Security, параметры компонентов и права пользователей Kaspersky Embedded Systems Security, а также возможность просматривать статистику Kaspersky Embedded Systems Security.
- **Изменение** – доступ ко всем функциям программы, за исключением изменения прав пользователей: возможность просматривать и изменять общие параметры Kaspersky Embedded Systems Security и параметры компонентов Kaspersky Embedded Systems Security.
- **Чтение** – возможность просматривать общие параметры Kaspersky Embedded Systems Security, параметры компонентов Kaspersky Embedded Systems Security, статистику Kaspersky Embedded Systems Security и права пользователей Kaspersky Embedded Systems Security.

Вы также можете настроить расширенные права доступа: разрешить или запретить доступ к конкретным функциям Kaspersky Embedded Systems Security.

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы будет установлен уровень доступа **Особые разрешения**.

Таблица 39. Права доступа к функциям Kaspersky Embedded Systems Security

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Embedded Systems Security.
Создание и удаление задач проверки по требованию	Возможность создавать и удалять задачи проверки по требованию.
Изменение параметров	Возможности: • Импортировать в конфигурационный файл параметры работы Kaspersky Embedded Systems Security. • Редактировать настройки программы.
Чтение параметров	Возможности: • просматривать общие параметры Kaspersky Embedded Systems Security и параметры задач; • экспортировать в конфигурационный файл параметры Kaspersky Embedded Systems Security; • просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Управление хранилищами	Возможности: • помещать объекты на карантин; • удалять объекты из карантина и резервного хранилища; • восстанавливать объекты из карантина и резервного хранилища.
Управление журналами	Возможность удалять журналы выполнения задач и очищать журнал системного аудита.
Чтение журналов	Возможность просматривать события в журналах выполнения задач и журнале системного аудита.
Чтение статистики	Возможность просматривать статистику работы каждой задачи Kaspersky Embedded Systems Security.
Лицензирование программы	Возможность активировать Kaspersky Embedded Systems Security.
Удаление программы	Возможность удалить Kaspersky Embedded Systems Security.
Чтение прав	Возможность просматривать список и права доступа пользователей Kaspersky Embedded Systems Security.
Изменение прав	Возможности: • изменять список пользователей, имеющих доступ к управлению программой; • изменять права доступа пользователей к функциям Kaspersky Embedded Systems Security.

О правах на управление регистрируемыми службами

При установке Kaspersky Embedded Systems Security регистрирует в Windows службу Kaspersky Security (KAVFS), службу Kaspersky Security Management (KAVFSGT) и службу Kaspersky Security Exploit Prevention (KAVFSSLP).

Регистрация службы Kaspersky Security как PPL с помощью драйвера ELAM поддерживается операционной системой Microsoft Windows 10 и более поздних версий. При запуске процесса как защищённого пользователь не может управлять им, независимо от прав пользователя. Если программа Kaspersky Embedded Systems Security установлена на компьютер под управлением операционной системы, поддерживающей PPL, управление правами пользователей для службы Kaspersky Security (KAVFS) будет недоступно.

Служба Kaspersky Security

По умолчанию доступ к управлению службой Kaspersky Security имеют пользователи, входящие в группу Администраторы на защищаемом компьютере, а также в группы SERVICE и INTERACTIVE с правами на чтение и в группу SYSTEM с правами на чтение и исполнение.

Пользователи, имеющие доступ к функциям уровня Изменение прав (см. раздел "Защита доступа к функциям Kaspersky Embedded Systems Security с помощью пароля" на стр. 236), могут предоставлять доступ к управлению службой Kaspersky Security другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Служба Kaspersky Security Management

Для управления программой через Консоль программы, установленную на другом компьютере, требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Embedded Systems Security, имела полный доступ к службе Kaspersky Security Management на защищаемом компьютере.

По умолчанию доступ к службе Kaspersky Security Management имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере, и пользователи группы ESS Administrators, созданной на защищаемом компьютере при установке Kaspersky Embedded Systems Security.

Вы можете управлять службой Kaspersky Security Management только через оснастку Службы Microsoft Windows.

Служба Kaspersky Security Exploit Prevention

По умолчанию доступ к управлению службой Kaspersky Security Exploit Prevention имеют пользователи, входящие в группу Администраторы на защищаемом компьютере, а также в группу SYSTEM с правами на чтение и исполнение.

О правах на управление службой Kaspersky Security

При установке Kaspersky Embedded Systems Security регистрирует в Windows службу Kaspersky Security (KAVFS), а также включает функциональные компоненты, запускаемые при запуске операционной системы. Чтобы снизить риск стороннего доступа к функциям программы и параметрам безопасности на защищаемом компьютере с помощью службы Kaspersky Security, можно ограничить права на управление службой Kaspersky Security с помощью Консоли программы или Плагина управления.

По умолчанию доступ к управлению службой Kaspersky Security имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере. Права на чтение имеют группы SERVICE и INTERACTIVE, а права на чтение и исполнение имеет группа SYSTEM.

Вы не можете удалить учетную запись пользователя SYSTEM или изменять права этой учетной записи. Если права учетной записи SYSTEM были изменены, то при сохранении изменений для этой учетной записи восстанавливаются максимальные права.

Пользователи, имеющие доступ уровня Изменение прав к функциям программы (см. раздел "О правах на управление Kaspersky Embedded Systems Security" на стр. 229), могут предоставлять доступ к управлению службой Kaspersky Security другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Embedded Systems Security один из следующих стандартных уровней доступа для управления службой Kaspersky Security:

- **Полный контроль** – возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Security, а также запускать и останавливать работу службы Kaspersky Security.
- **Чтение** – возможность просматривать общие параметры работы и права пользователей для службы Kaspersky Security.
- **Изменение** – возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Security.
- **Исполнение** – возможность запускать и останавливать работу службы Kaspersky Security.

Также вы можете выполнять расширенную настройку прав доступа: разрешить или запретить доступ к определенным функциям Kaspersky Embedded Systems Security (см. таблицу ниже).

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы будет установлен уровень доступа **Особые разрешения**.

Таблица 40. Права доступа к функциям службы Kaspersky Security

Функция	Описание
Просмотр параметров службы	Возможность просматривать общие параметры и права пользователей для службы Kaspersky Security.
Запрос статуса службы у Диспетчера управления службами	Возможность запрашивать статус выполнения службы Kaspersky Security у Диспетчера управления службами Microsoft Windows.
Запрос статуса у службы	Возможность запрашивать статус выполнения у службы Kaspersky Security.
Перечисление зависимых служб	Возможность просматривать список служб, от которых зависит служба Kaspersky Security, а также служб, зависимых от службы Kaspersky Security.
Изменение параметров службы	Возможность просматривать и изменять общие параметры работы и права пользователей для служб Kaspersky Security.
Запуск службы	Возможность запускать выполнение службы Kaspersky Security.

Функция	Описание
Остановка службы	Возможность останавливать выполнение службы Kaspersky Security.
Приостановка / Возобновление службы	Возможность приостанавливать и возобновлять выполнение службы Kaspersky Security.
Чтение прав	Возможность просматривать список пользователей службы Kaspersky Security и права доступа каждого пользователя.
Изменение прав	Возможности: • добавлять и удалять пользователей службы Kaspersky Security; • изменять права доступа пользователей к службе Kaspersky Security.
Удаление службы	Возможность отмены регистрации службы Kaspersky Security в диспетчере управления службами Microsoft Windows.
Пользовательские запросы к службе	Возможность создавать и отправлять пользовательские запросы к службе Kaspersky Security.

О правах доступа к службе Kaspersky Security Management

Вы можете просмотреть список служб Kaspersky Embedded Systems Security.

При установке Kaspersky Embedded Systems Security регистрирует службу Kaspersky Security Management (KAVFSGT). Для управления программой через Консоль программы, установленную на другом компьютере, требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Embedded Systems Security, имела полный доступ к службе Kaspersky Security Management на защищаемом компьютере.

По умолчанию доступ к службе Kaspersky Security Management имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере, и пользователи группы ESS Administrators, созданной на защищаемом компьютере при установке Kaspersky Embedded Systems Security.

Вы можете управлять службой Kaspersky Security Management только через оснастку Службы Microsoft Windows.

Вы не можете разрешать или запрещать пользователям доступ к службе Kaspersky Security Management, настраивая параметры Kaspersky Embedded Systems Security.

Вы можете подключиться к Kaspersky Embedded Systems Security с локальной учетной записью, если на защищаемом компьютере зарегистрирована учетная запись с такими же именем пользователя и паролем.

Настройка прав доступа на управление Kaspersky Embedded Systems Security и службой Kaspersky Security

Можно настраивать список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Embedded Systems Security и к управлению службой Kaspersky Security Service. Можно также настраивать права доступа для этих пользователей и групп пользователей.

► *Чтобы добавить в список или удалить из списка пользователя или группу, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Дополнительно** выполните одно из следующих действий:
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security.
   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению службой Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Embedded Systems Security**.
5. В открывшемся окне выполните следующие действия:
   - Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу, которым вы хотите предоставить права.
   - Чтобы удалить пользователя или группу из списка, выберите пользователя или группу, для которых вы хотите ограничить права доступа, и нажмите на кнопку **Удалить**.

6. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Embedded Systems Security или службой Kaspersky Security, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Дополнительно** выполните одно из следующих действий:
   - Нажмите на кнопку **Настройка** в блоке **Изменить права пользователей на управление программой**, если требуется изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security.
   - Нажмите на кнопку **Настройка** в блоке **Изменить права пользователей для службы Kaspersky Security Management**, если требуется изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Embedded Systems Security**.
5. В открывшемся окне в списке **Имена групп и пользователей** выберите пользователя или группу пользователей, права которых вы хотите изменить.
6. В блоке **Разрешения для <Пользователь (Группа)>** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
   - **Полный контроль**: полный набор прав на управление Kaspersky Embedded Systems Security или службой Kaspersky Security Service.
   - **Чтение**:
     - Следующие разрешения на управление Kaspersky Embedded Systems Security: **Чтение статистики**, **Чтение параметров**, **Чтение журналов** и **Чтение прав**.
     - Следующие разрешения на управление службой Kaspersky Security: **Чтение параметров службы**, **Запрос статуса службы у Диспетчера управления службами**, **Запрос статуса у службы**, **Перечисление зависимых служб**, **Чтение прав**.

- **Изменение**:
  - Все права на управление Kaspersky Embedded Systems Security, кроме **Изменение прав**.
  - Следующие разрешения на управление службой Kaspersky Security: **Изменение параметров службы**, **Чтение прав**.
- **Особые разрешения**: следующие разрешения на управление службой Kaspersky Security: **Запуск службы**, **Остановка службы**, **Остановка / возобновление службы**, **Чтение прав**, **Пользовательские запросы к службе**.

7. Чтобы выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.
   a. В открывшемся окне **Дополнительные параметры безопасности для Kaspersky Embedded Systems Security**, выберите нужного пользователя или нужную группу.
   b. Нажмите на кнопку **Изменить**.
   c. В раскрывающемся списке в верхней части окна выберите тип контроля доступа: **Разрешить** или **Запретить**.
   d. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или выбранной группе.
   e. Нажмите на кнопку **ОК**.
   f. В окне **Дополнительные параметры безопасности для Kaspersky Embedded Systems Security** нажмите на кнопку **ОК**.
8. В окне **Разрешения для Kaspersky Embedded Systems Security** нажмите на кнопку **Применить**.
9. Настроенные права на управление Kaspersky Embedded Systems Security или службой Kaspersky Security будут сохранены.

Защита доступа к функциям Kaspersky Embedded Systems Security с помощью пароля

Вы можете ограничивать доступ к управлению программой и регистрируемыми службами с помощью настройки прав пользователей (см. раздел "Управление правами доступа к функциям Kaspersky Embedded Systems Security" на стр. 229). Для дополнительной защиты можно также установить защиту паролем в параметрах Kaspersky Embedded Systems Security. Защита паролем позволяет дополнительно ограничить доступ к управлению через Консоль программы и выполнение команд из командной строки. Если используется защита паролем, Kaspersky Embedded Systems Security запрашивает у всех пользователей пароль при запуске Консоли программы и при выполнении команд из командной строки.

► *Чтобы защитить доступ к функциям Kaspersky Embedded Systems Security, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security** и выполните одно из следующих действий:
   - В панели результатов узла перейдите по ссылке **Свойства программы**.
   - В контекстном меню узла выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.

2. На закладке **Безопасность и надежность** в блоке **Параметры применения пароля** установите флажок **Использовать защиту паролем**.

   Поля **Пароль** и **Подтверждение пароля** станут активными.

3. В поле **Пароль** введите значение, которое вы хотите использовать для защиты доступа к функциям Kaspersky Embedded Systems Security.
4. В поле **Подтверждение пароля** введите пароль повторно.
5. Нажмите на кнопку **ОК**.

Установленный пароль невозможно восстановить. Утеря пароля ведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого компьютера.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет отключена, и контрольная сумма старого пароля будет удалена. Повторите процесс ввода пароля с новым паролем.

Настройка прав доступа в Kaspersky Security Center

Вы можете настроить права доступа к управлению программой и службой Kaspersky Security в Kaspersky Security Center для группы компьютеров или для отдельного компьютера.

► *Чтобы настроить права доступа к управлению программой и службой Kaspersky Security, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. Откройте раздел **Дополнительные возможности** и выполните следующие действия:
   - Если вы хотите настроить права доступа к управлению Kaspersky Embedded Systems Security для пользователей или группы пользователей, в блоке **Права пользователей на управление программой** нажмите кнопку **Настройка**.

- Если вы хотите настроить права доступа на управление службой Kaspersky Security для пользователей или группы пользователей, в блоке **Права пользователей на управление службой Kaspersky Security** нажмите кнопку **Настройка**.

5. В открывшемся окне настройте права доступа в соответствии с вашими требованиями (см. раздел "Управление правами доступа к функциям Kaspersky Embedded Systems Security" на стр. 229).

Настроенные параметры будут сохранены.

Постоянная защита файлов

Этот раздел содержит информацию о задаче Постоянная защита файлов и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Постоянная защита файлов

В ходе выполнения задачи Постоянная защита файлов Kaspersky Embedded Systems Security проверяет следующие объекты защищаемого компьютера при доступе к ним:

- файлы;
- альтернативные потоки файловых систем (NTFS-streams);
- основную загрузочную запись и загрузочные секторы локальных жестких дисков и внешних устройств.

При записи или считывании записанного файла любой программой на компьютере Kaspersky Embedded Systems Security перехватывает этот файл, проверяет его на наличие угроз и при обнаружении угрозы выполняет действия, указанные в параметрах задачи или заданные по умолчанию: пытается вылечить файл, перемещает файл на карантин или удаляет его, если лечение невозможно. Перед лечением или удалением, Kaspersky Embedded Systems Security сохраняет зашифрованную копию исходного файла в папку резервного хранилища. Kaspersky Embedded Systems Security восстанавливает файл с карантина в исходную папку, если он был успешно вылечен.

Kaspersky Embedded Systems Security также обнаруживает вредоносную активность в процессах подсистемы Windows Subsystem for Linux®. Для таких процессов задача Постоянная защита файлов применяет действие, указанное в текущих настройках.

Об области защиты и параметрах безопасности задачи

По умолчанию под действие задачи Постоянная защита файлов подпадают все объекты файловой системы компьютера. Если по требованиям к безопасности нет необходимости защищать все объекты файловой системы или вы намеренно хотите исключить некоторые объекты из области действия задачи постоянной защиты, вы можете ограничить область защиты.

В Консоли программы область защиты представляет собой дерево или список файловых ресурсов компьютера, которые может контролировать Kaspersky Embedded Systems Security. По умолчанию сетевые файловые ресурсы защищаемого компьютера отображаются в виде списка.

В Плагине управления доступно только представление в виде списка.

► *Чтобы включить отображение сетевых файловых ресурсов в виде дерева в Консоли программы,*

в раскрывающемся списке, расположенном в левом верхнем углу окна **Настройка области защиты**, выберите пункт **Показывать в виде дерева**.

Элементы и узлы в дереве или списке файловых ресурсов компьютера отображаются следующим образом:

☑ – узел включен в область защиты.

☐ Узел исключен из области защиты.

☑ – по крайней мере один из узлов, вложенных в этот узел, исключен из области защиты, или параметры безопасности вложенных узлов отличаются от параметров безопасности этого узла (только для режима отображения в виде дерева).

Значок ☑ отображается, если выбраны все вложенные узлы, но не выбран родительский узел. В этом случае изменения состава файлов и папок родительского узла не учитываются автоматически при формировании области защиты для выбранного вложенного узла.

С помощью Консоли программы можно также добавлять в область защиты виртуальные диски (см. раздел "Создание виртуальной области защиты" на стр. 270). Имена виртуальных узлов отображаются шрифтом синего цвета.

Параметры безопасности

Можно настроить как единые параметры безопасности задачи для всех узлов или элементов, входящих в область защиты, так и отдельные для каждого узла или элемента в дереве или списке файловых ресурсов компьютера.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты одним из следующих способов:

- выбрать один из трех стандартных уровней безопасности (см. стр. 242);
- настроить параметры безопасности вручную (см. Раздел "Настройка параметров безопасности вручную" на стр. 255) для выбранных узлов или элементов в дереве или списке файловых ресурсов (уровень безопасности примет значение **Другой**).

Вы можете сохранить набор параметров узла или элемента в шаблон, чтобы потом применять этот шаблон для других узлов или элементов.

О виртуальной области защиты

Kaspersky Embedded Systems Security может проверять не только существующие папки и файлы на жестких и съемных дисках, но и объекты, которые динамически создаются на компьютере различными программами и службами.

Если вы включили в область защиты все объекты компьютера, эти динамические узлы автоматически войдут в область защиты. Однако если вы хотите задать специальные значения параметров безопасности для динамических узлов или если вы выбрали для защиты не весь компьютер, а отдельные области, то, для того чтобы включить в область защиты динамические диски, файлы или папки, необходимо предварительно создать их в Консоли программы, то есть задать виртуальную область защиты. Созданные диски, файлы и папки существуют только в Консоли программы, но не в структуре файловой системы защищаемого компьютера.

Если, формируя область защиты, вы выберете все вложенные папки или файлы, но не выберете родительскую папку, динамические папки или файлы, которые появятся в ней, не будут автоматически включены в область защиты. Вам нужно создать их виртуальные копии в Консоли программы и добавить их в область защиты.

Стандартные области защиты

Дерево или список файловых ресурсов отображает узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Embedded Systems Security предусмотрены следующие стандартные области защиты:

- **Локальные жесткие диски**. Kaspersky Embedded Systems Security защищает файлы на жестких дисках компьютера.
- **Съемные диски**. Kaspersky Embedded Systems Security защищает файлы на внешних устройствах, например, на компакт-дисках или флеш-накопителях. Вы можете включать в область защиты или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.
- **Сетевое окружение**. Kaspersky Embedded Systems Security защищает файлы, которые записываются в сетевые папки или считываются из них программами, выполняемыми на компьютере. Kaspersky Embedded Systems Security не защищает файлы в сетевых папках, когда к ним обращаются программы с других компьютеров.
- **Виртуальные диски**. Вы можете включать в область защиты динамические папки и файлы, а также диски, которые временно подключены к компьютеру, например, общие диски кластера.

Стандартные области защиты по умолчанию отображаются и доступны для изменения в списке областей; можно также добавлять стандартные области защиты в список при его формировании в параметрах области защиты.

По умолчанию в область защиты включены все стандартные области, кроме виртуальных дисков.

Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов компьютера в Консоли программы. Чтобы включить в область защиты объекты на виртуальном диске, включите в область защиты папку компьютера, с которой связан этот виртуальный диск.

Подключенные сетевые диски также не отображаются в списке файловых ресурсов компьютера. Чтобы включить в область защиты объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

Стандартные уровни безопасности

Для выбранных в дереве или списке файловых ресурсов компьютера узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**. Каждый из этих уровней имеет свой стандартный набор параметров безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, помимо использования Kaspersky Embedded Systems Security на компьютерах, применяются дополнительные меры компьютерной безопасности, например, сетевые экраны и политики безопасности.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых компьютеров. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты компьютеров в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если предъявляются повышенные требования к безопасности в сети организации.

Таблица 41. Стандартные уровни безопасности и соответствующие им значения параметров

Параметры	Уровень безопасности		
	Максимальное быстродействие	Рекомендуемый	Максимальная защита
Защита объектов	По расширению	По формату	По формату
Проверка только новых и измененных файлов	Включена	Включена	Выключено
Действия над зараженными и другими обнаруженными объектами	Блокировать доступ и лечить. Удалить, если не удалось вылечить.	Блокировать доступ и выполнить рекомендуемое действие.	Блокировать доступ и лечить. Удалить, если не удалось вылечить.
Действия над возможно зараженными объектами	Блокировать доступ и поместить на карантин.	Блокировать доступ и выполнить рекомендуемое действие.	Блокировать доступ и поместить на карантин.
Исключать файлы	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.)	60 сек.	60 сек.	60 сек.
Не проверять составные объекты размером более (МБ)	8 МБ	8 МБ	Не установлен
Альтернативные потоки NTFS	Да	Да	Да
Загрузочные секторы дисков и MBR	Да	Да	Да
Защита составных объектов	• Упакованные объекты* * Только новые и измененные	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Только новые и измененные	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Все объекты
Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой	Нет	Нет	Да

Параметры **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift** и **Использовать эвристический анализатор** не входят в набор параметров стандартных уровней безопасности. Если, выбрав один из стандартных уровней безопасности, вы измените параметры безопасности **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift** или **Использовать эвристический анализатор**, выбранный вами стандартный уровень безопасности не изменится.

Расширения файлов, проверяемые по умолчанию в задаче Постоянная защита файлов

По умолчанию Kaspersky Embedded Systems Security проверяет файлы, имеющие следующие расширения:

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*

- *exe;*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*
- *htt;*
- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*

- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?*

Параметры задачи Постоянная защита файлов по умолчанию

По умолчанию в задаче Постоянная защита файлов используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 42. Параметры задачи Постоянная защита файлов по умолчанию

Параметр	Значение по умолчанию	Описание
Область защиты	Весь компьютер, исключая виртуальные диски.	Вы можете ограничить область защиты.
Режим защиты объектов	**При открытии и изменении**	Вы можете выбрать режим защиты объектов – указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security проверяет их.
Эвристический анализатор	Применяется уровень безопасности **Средний**.	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.
Применять доверенную зону	Применяется.	Единый список исключений, который вы можете применять в выбранных задачах.
Использовать KSN для защиты	Применяется.	Вы можете увеличить эффективность защиты сервера с помощью инфраструктуры облачных служб Kaspersky Security Network (доступно, только если принято Положение о KSN).
Расписание запуска задачи	При запуске программы.	Вы можете настроить запуск задачи по расписанию.
Блокировать доступ к сетевым файловым ресурсам для узлов, с которых ведется вредоносная активность	Не применяется.	Вы можете добавлять узлы, со стороны которых выявлена вредоносная активность, в список заблокированных узлов.

Управление задачей Постоянная защита файлов с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для одного или всех компьютеров сети.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

В этом разделе

Переход к параметрам политики для задачи Постоянная защита файлов

► *Чтобы перейти к параметрам задачи Постоянная защита файлов в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую требуется настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита компьютера**.
6. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**.

   Откроется окно **Постоянная защита файлов**.

Если компьютер работает под управлением активной политики Kaspersky Security Center и в этой политике запрещено изменение параметров программы, эти параметры недоступны для изменения в Консоли программы.

Переход к параметрам задачи Постоянная защита файлов

► *Чтобы перейти к окну параметров задачи Постоянная защита файлов для отдельного компьютера, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя компьютера>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого компьютера;
   - Выберите пункт **Свойства** в контекстном меню защищаемого компьютера.

   Откроется окно **Свойства: <Имя компьютера>**.
5. В разделе **Задачи** выберите задачу **Постоянная защита файлов**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: Постоянная защита файлов**.

Настройка задачи Постоянная защита файлов

► *Чтобы настроить параметры задачи Постоянная защита файлов, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. 248).
2. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - **Режим защиты объектов** (см. раздел "**Выбор режима защиты**" на стр. 250).
     - **Эвристический анализатор**
     - **Интеграция с другими компонентами** (см. раздел "**Настройка эвристического анализатора и интеграции с другими компонентами программы**" на стр. 251)
   - На закладке **Управление задачей**:
     - Запуск задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 130).
3. Выберите закладку **Область защиты** и выполните следующие действия:
   - Нажмите на кнопку **Добавить** или **Изменить**, чтобы изменить область защиты (см. раздел "Создание области защиты" на стр. 268).
     - В открывшемся окне выберите, что требуется включить в область защиты задачи:
       - **Предопределенная область**
       - **Диск, папка или сетевой объект**
       - **Файл**

- Выберите один из стандартных уровней безопасности (см. стр. 242) или настройте параметры защиты вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 255).

4. Нажмите на кнопку **ОК** в окне **Постоянная защита файлов**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

В этом разделе

Выбор режима защиты объектов

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. В блоке **Режим защиты объектов** можно указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security проверяет эти объекты.

Параметр **Режим защиты объектов** имеет единое значение для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

► *Чтобы выбрать режим защиты, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. 248).
2. В открывшемся окне на закладке **Общие** выберите режим защиты объектов, который вы хотите установить:
   - **Интеллектуальный режим**

     Kaspersky Embedded Systems Security выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс во время своей работы многократно обращается к объекту и изменяет его, Kaspersky Embedded Systems Security повторно проверяет объект только после его последнего сохранения этим процессом.
   - **При открытии и изменении**

     Kaspersky Embedded Systems Security проверяет объект при открытии и проверяет его повторно при сохранении, если объект был изменен.

     Данный вариант выбран по умолчанию.
   - **При открытии**

     Kaspersky Embedded Systems Security проверяет все объекты при их открытии как на чтение, так и на выполнение или изменение.

- **При выполнении**

  Kaspersky Embedded Systems Security проверяет файл только при открытии на выполнение.

3. Нажмите на кнопку **ОК**.

Выбранный режим защиты объектов будет установлен.

Настройка эвристического анализатора и интеграции с другими компонентами программы

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

► *Чтобы настроить эвристический анализатор и интеграцию с другими компонентами, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. 248).
2. На закладке **Общие** снимите или установите флажок **Использовать эвристический анализатор**.

   Флажок включает или выключает использование эвристического анализатора при проверке объектов.

   Если флажок установлен, эвристический анализатор включен.

   Если флажок снят, эвристический анализатор выключен.

   По умолчанию флажок установлен.
3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Ползунок позволяет регулировать уровень эвристического анализа. Уровень детализации проверки обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни детализации проверки:

   - **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
   - **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

     Этот уровень выбран по умолчанию.
   - **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

     Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.

4. В блоке **Интеграция с другими компонентами** настройте следующие параметры:
   - Установите или снимите флажок **Применять доверенную зону**.

     Флажок включает или выключает применение доверенной зоны в работе задачи.

     Если флажок установлен, Kaspersky Embedded Systems Security добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

     Если флажок снят, Kaspersky Embedded Systems Security не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

     По умолчанию флажок установлен.
   - Установите или снимите флажок **Использовать KSN для защиты**.

     Этот флажок включает или выключает использование служб KSN.

     Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

     Если флажок снят, задача не использует службы KSN.

     По умолчанию флажок установлен.

     Флажок **Разрешить отправку данных о проверяемых файлах** должен быть установлен в параметрах задачи Использование KSN.
   - Установите или снимите флажок **Блокировать доступ к сетевым файловым ресурсам для узлов, с которых ведется вредоносная активность**.
5. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Вы не можете настраивать расписание запуска групповых задач.

► *Чтобы настроить параметры расписания запуска групповой задачи, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемый сервер.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Дважды щелкните мышью на имени задачи.
   - Откройте контекстное меню задачи и выберите пункт Свойства.
5. Выберите раздел **Расписание**.

6. В блоке **Параметры расписания** установите флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задачи проверки по требованию и задачи обновления недоступны, если запуск задачи по расписанию запрещен действием политики Kaspersky Security Center.

7. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

   a. в списке **Частота запуска** выберите одно из следующих значений:

      - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> ч.**;
      - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут.**;
      - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам);
      - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security;
      - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.

   b. В поле **Время запуска** укажите время первого запуска задачи.

   c. В поле **Начать с** укажите дату начала действия расписания.

      После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** появится информация о расчетном времени очередного запуска задачи. Обновленная информация о расчетном времени следующего запуска будет отображаться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.
      Значение **Запрещен политикой** отображается в поле **Следующий запуск**, если параметрами действующей политики Kaspersky Security Center запрещен запуск системных задач по расписанию (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 98).

8. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.

   - В блоке **Параметры остановки задачи**:

     a. Установите флажок **Длительность** и введите нужное количество часов и минут в полях справа, чтобы указать максимальную длительность выполнения задачи.

     b. Установите флажок **Приостановить с** и введите начальное и конечное значение временного промежутка в полях справа, чтобы указать промежуток времени в пределах суток, в течение которого выполнение задачи будет приостановлено.

   - В блоке **Дополнительные параметры**:

     a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание

перестанет действовать.

b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.

c. Установите флажок **Распределять время запуска задач в интервале** и укажите значение параметра в минутах.

9. Нажмите на кнопку **OK**.

10. Нажмите на кнопку **Применить**, чтобы сохранить параметры запуска задачи.

Если вы хотите настроить параметры программы для отдельной задачи с помощью Kaspersky Security Center, выполните действия, описанные в разделе Настройка локальных задач в окне Параметры программы в Kaspersky Security Center на стр. 119.

Создание и настройка области защиты задачи

► *Чтобы создать и настроить область защиты задачи в Kaspersky Security Center, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. 248).

2. Выберите закладку **Область защиты**.

3. Все элементы, на которые распространяется область защиты задачи, перечислены в таблице Область защиты.

4. Нажмите на кнопку **Добавить**, чтобы добавить в список новый элемент.

   Откроется окно **Добавление в область защиты**.

5. Выберите тип объекта для добавления в область защиты:

   - **Предопределенная область**, если вы хотите включить в область защиты одну из стандартных областей на защищаемом сервере. Затем в раскрывающемся списке выберите требуемую область защиты.
   - **Диск, папка или сетевой объект**, если вы хотите включить в область защиты отдельный диск, папку или сетевой объект. Затем выберите нужную область защиты по кнопке **Обзор**.
   - **Файл**, если вы хотите включить в область защиты отдельный файл. Затем выберите нужную область защиты по кнопке **Обзор**.

   Вы не можете добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.

6. Чтобы исключить отдельные элементы из области защиты, снимите флажки рядом с именами этих элементов или выполните следующие действия:

   a. Откройте контекстное меню области защиты по правой клавише мыши.

   b. В контекстном меню выберите пункт **Добавить исключение**.

   c. В открывшемся окне **Добавление исключения** выберите тип объекта, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в

область защиты.

7. Чтобы изменить добавленную область защиты или исключение, в контекстном меню требуемой области защиты выберите пункт **Изменить область**.
8. Чтобы скрыть отображение ранее добавленной области защиты или исключения в списке сетевых файловых ресурсов, в контекстном меню требуемой области выберите пункт **Удалить область**.

   Область защиты исключается из области действия задачи Постоянная защита файлов при ее удалении из списка сетевых файловых ресурсов.

9. Нажмите на кнопку **Сохранить**.

Окно параметров области защиты закроется. Настроенные параметры будут сохранены.

Вы можете запустить задачу **Постоянная защита файлов**, если по крайней мере один узел файловых ресурсов компьютера включен в область защиты.

Настройка параметров безопасности вручную

По умолчанию в задаче Постоянная защита файлов применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый** (см. раздел "Стандартные уровни безопасности" на стр. 242).

Вы можете изменять заданные по умолчанию значения параметров безопасности, настроив их как едиными для всей области защиты, так и различными для разных элементов / узлов в списке / дереве файловых ресурсов компьютера.

► *Чтобы вручную настроить параметры безопасности выбранного узла, выполните следующие действия:*

1. Откройте окно **Постоянная защита файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. 248).
2. На закладке **Область защиты** выберите узел, параметры безопасности которого вы хотите настроить, и нажмите на кнопку **Настроить**.

   Откроется окно **Настройка параметров постоянной защиты файлов**.
3. На закладке **Уровень безопасности** нажмите на кнопку **Настройка**, чтобы настроить пользовательские параметры.
4. Вы можете настроить пользовательские параметры безопасности для выбранного узла в соответствии с вашими требованиями.
   - Общие параметры (см. раздел "Настройка общих параметров задачи" на стр. 256)
   - Действия (см. раздел "Настройка действий" на стр. 258)
   - Производительность (см. раздел "Настройка производительности" на стр. 261)
5. Нажмите на кнопку **ОК** в окне **Постоянная защита файлов**.

Новые параметры области защиты будут сохранены.

В этом разделе

Настройка общих параметров задачи

► *Чтобы настроить общие параметры безопасности задачи Постоянная защита файлов, выполните следующие действия.*

1. Откройте окно **Настройка параметров постоянной защиты файлов** (см. раздел "Переход к параметрам политики для задачи Постоянная защита файлов" на стр. 248).
2. Выберите закладку **Общие**.
3. В блоке **Защита объектов** укажите типы объектов, которые вы хотите включить в область защиты:
   - **Все объекты**

     Kaspersky Embedded Systems Security проверяет все объекты.
   - **Объекты, проверяемые по формату**

     Kaspersky Embedded Systems Security проверяет только потенциально заражаемые файлы на основании формата файла.

     Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security.
   - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

     Kaspersky Embedded Systems Security проверяет только потенциально заражаемые файлы на основании расширения файла.

     Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security.
   - **Объекты, проверяемые по указанному списку расширений**

     Kaspersky Embedded Systems Security проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.
   - **Загрузочные секторы дисков и MBR**

     Включение защиты загрузочных секторов дисков и основных загрузочных записей.

     Если флажок установлен, Kaspersky Embedded Systems Security проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках компьютера.

     По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках файловой системы NTFS.

  Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

  Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

  По умолчанию флажок установлен.

4. В блоке **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security новыми или измененными с момента последней проверки.

   Если флажок установлен, Kaspersky Embedded Systems Security проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

   Если флажок не установлен, можно выбрать, требуется ли проверка и защита только новых файлов или всех файлов, независимо от того, когда они были изменены.

   По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**. Если выбран уровень безопасности **Максимальная защита** или **Рекомендуемый**, флажок не установлен.

   Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

5. В блоке **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область защиты:

   - **Все / Только новые архивы**

     Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

     Если флажок установлен, Kaspersky Embedded Systems Security проверяет архивы.

     Если флажок снят, Kaspersky Embedded Systems Security пропускает архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня защиты.

   - **Все / Только новые SFX-архивы**

     Проверка самораспаковывающихся архивов.

     Если флажок установлен, Kaspersky Embedded Systems Security проверяет SFX-архивы.

     Если флажок снят, Kaspersky Embedded Systems Security пропускает SFX-архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня защиты.

     Параметр доступен, если снят флажок **Архивы**.

- **Все / Только новые почтовые базы**

  Проверка файлов почтовых баз Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает файлы почтовых баз при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые упакованные объекты**

  Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Embedded Systems Security при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

  Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые файлы почтовых форматов**

  Проверка файлов почтовых форматов, например, сообщения форматов Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые вложенные OLE-объекты**

  Проверка встроенных в файл объектов (например, макрос Microsoft Word или вложение сообщения электронной почты).

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает встроенные в файл объекты при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка действий

► *Чтобы настроить действия, которые задача Постоянная защита файлов выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:*

1. Откройте окно **Настройка параметров постоянной защиты файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 248).

2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**

     Когда выбран этот режим, Kaspersky Embedded Systems Security не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** требуется настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security автоматически изменит уровень безопасности на **Другой**.

   - **Блокировать доступ**

     Если выбран этот вариант, Kaspersky Embedded Systems Security блокирует доступ к зараженным или другим обнаруженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

   - **Выполнять дополнительное действие**

     Выберите действие из раскрывающегося списка:

     - **Лечить**
     - **Лечить. Лечить. Удалять, если лечение невозможно**
     - **Удалять**
     - **Рекомендуемое**
4. Выберите действие над возможно зараженными объектами:
   - **Только сообщать**

     Когда выбран этот режим, Kaspersky Embedded Systems Security не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** требуется настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security автоматически изменит уровень безопасности на **Другой**.

   - **Блокировать доступ**

     Если выбран этот вариант, Kaspersky Embedded Systems Security блокирует доступ к зараженным или другим обнаруженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

- **Выполнять дополнительное действие**

  Выберите действие из раскрывающегося списка:

  - **Помещать на карантин**
  - **Удалять**
  - **Рекомендуемое**

5. Настройте действия над объектами в зависимости от типа обнаруженного объекта:

   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

      Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. При этом Kaspersky Embedded Systems Security не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Embedded Systems Security выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

      По умолчанию флажок снят.

   b. Нажмите на кнопку **Настройка**.

   c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.

   d. Нажмите на кнопку **OK**.

6. Выберите действие над неизменяемыми составными файлами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

   Флажок включает или выключает форсированное удаление родительского составного файла при обнаружении вложенного вредоносного, возможно зараженного или другого обнаруживаемого объекта.

   Если флажок установлен и задача настроена на удаление зараженных или возможно зараженных объектов, Kaspersky Embedded Systems Security принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление составного объекта со всем его содержимым выполняется в случае, если программа не может удалить только вложенный обнаруженный объект (например, если составной объект неизменяем).

   Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security не выполняет выбранное действие, если родительский объект неизменяем.

7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

► *Чтобы настроить производительность задачи Постоянная защита файлов, выполните следующие действия:*

1. Откройте окно **Настройка параметров постоянной защиты файлов** (см. раздел "**Переход к параметрам политики для задачи Постоянная защита файлов**" на стр. 248).
2. Выберите закладку **Производительность**.
3. В блоке **Исключения**:
   - Снимите или установите флажок **Исключать файлы**.

     Исключение файлов из проверки по имени файла или маске имени файла.

     Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security проверяет все объекты.

     По умолчанию флажок снят.
   - Снимите или установите флажок **Не обнаруживать**.

     Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

     Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.
   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.
4. В блоке **Дополнительные параметры**:
   - **Останавливать проверку, если она длится более (сек.)**

     Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

     Если флажок установлен, максимальная продолжительность проверки объекта ограничена указанным значением.

     Если флажок снят, максимальная продолжительность проверки не ограничена.

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.
   - **Не проверять составные объекты размером более (МБ)**

     Исключение из проверки составных объектов больше указанного размера.

     Если флажок установлен, Kaspersky Embedded Systems Security пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

Если флажок снят, Kaspersky Embedded Systems Security проверяет составные объекты, не учитывая размер.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет только новые файлы и файлы, изменившиеся с момента последней проверки системных объектов NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы во время выполнения задачи проверки и проверяет только новые файлы и файлы, измененные с момента последней проверки.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Embedded Systems Security проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

Управление задачей Постоянная защита файлов с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи для локального компьютера.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к настройке области задачи Постоянная защита файлов

► *Чтобы перейти к окну параметров области защиты для задачи Постоянная защита файлов, выполните следующие действия.*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.

Переход к параметрам задачи Постоянная защита файлов

► *Чтобы перейти к окну общих параметров задачи, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

Настройка задачи Постоянная защита файлов

► *Чтобы настроить параметры задачи Постоянная защита файлов, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Постоянная защита файлов" на стр. 263).
2. На закладке **Общие** настройте следующие параметры задачи:
   - **Режим защиты объектов** (см. раздел "**Выбор режима защиты**" на стр. 264).
   - **Эвристический анализатор**
   - **Интеграция с другими компонентами** (см. раздел "**Настройка эвристического анализатора и интеграции с другими компонентами программы**" на стр. 265).
3. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. 151).
4. В окне **Параметры задачи** нажмите на кнопку **OK**.

   Изменения параметров задачи будут сохранены.
5. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.
6. Выполните следующие действия:
   - В дереве или списке файловых ресурсов компьютера выберите узлы или элементы, которые вы хотите включить в область защиты задачи.
   - Выберите один из стандартных уровней безопасности или настройте параметры защиты объекта вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 446).
7. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

В этом разделе

Выбор режима защиты объектов

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. В блоке **Режим защиты объектов** можно указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security проверяет эти объекты.

Параметр **Режим защиты объектов** имеет единое значение для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

► *Чтобы выбрать режим защиты объектов, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Постоянная защита файлов" на стр. 263).
2. В открывшемся окне на закладке **Общие** выберите режим защиты объектов, который вы хотите установить:
   - **Интеллектуальный режим**

     Kaspersky Embedded Systems Security выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс во время своей работы многократно обращается к объекту и изменяет его, Kaspersky Embedded Systems Security повторно проверяет объект только после его последнего сохранения этим процессом.
   - **При открытии и изменении**

     Kaspersky Embedded Systems Security проверяет объект при открытии и проверяет его повторно при сохранении, если объект был изменен.

     Данный вариант выбран по умолчанию.
   - **При открытии**

     Kaspersky Embedded Systems Security проверяет все объекты при их открытии как на чтение, так и на выполнение или изменение.
   - **При выполнении**

     Kaspersky Embedded Systems Security проверяет файл только при открытии на выполнение.
3. Нажмите на кнопку **OK**.

Выбранный режим защиты объектов будет установлен.

Настройка эвристического анализатора и интеграции с другими компонентами программы

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

► *Чтобы настроить эвристический анализатор и интеграцию с другими компонентами, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Постоянная защита файлов**" на стр. 263).
2. На закладке **Общие** снимите или установите флажок **Использовать эвристический анализатор**.

   Флажок включает или выключает использование эвристического анализатора при проверке объектов.

   Если флажок установлен, эвристический анализатор включен.

   Если флажок снят, эвристический анализатор выключен.

   По умолчанию флажок установлен.

3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Ползунок позволяет регулировать уровень эвристического анализа. Уровень детализации проверки обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни детализации проверки:

   - **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
   - **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

     Этот уровень выбран по умолчанию.
   - **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

     Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.

4. В блоке **Интеграция с другими компонентами** настройте следующие параметры:

   - Установите или снимите флажок **Применять доверенную зону**.

     Флажок включает или выключает применение доверенной зоны в работе задачи.

     Если флажок установлен, Kaspersky Embedded Systems Security добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

     Если флажок снят, Kaspersky Embedded Systems Security не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

     По умолчанию флажок установлен.

     По ссылке **Доверенная зона** перейдите к параметрам доверенной зоны.

   - Установите или снимите флажок **Использовать KSN для защиты**.

     Этот флажок включает или выключает использование служб KSN.

     Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

     Если флажок снят, задача не использует службы KSN.

     По умолчанию флажок установлен.

     Флажок **Разрешить отправку данных о проверяемых файлах** должен быть установлен в параметрах задачи Использование KSN.

   - Установите или снимите флажок **Блокировать доступ к сетевым файловым ресурсам для узлов, с которых ведется вредоносная активность**.

5. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены.

Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Вы не можете настраивать расписание запуска групповых задач.

► *Чтобы настроить расписание запуска задачи, выполните следующие действия:*

1. Откройте контекстное меню названия задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** установите флажок **Запускать задачу по расписанию**.
4. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
   a. В списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> ч**.
      - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут**.
      - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед. по**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам);
      - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security;
      - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.
   b. В поле **Время запуска** укажите время первого запуска задачи.
   c. В поле **Начать с** укажите дату начала действия расписания.

   После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** появится информация о расчетном времени очередного запуска задачи. Обновленная информация о расчетном времени следующего запуска будет отображаться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.
   В поле **Следующий запуск** отображается значение **Запрещен политикой**, если запуск системных задач по расписанию определен параметрами действующей политики Kaspersky Security Center.

5. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.
   - В блоке **Параметры остановки задачи**:
     a. Установите флажок **Длительность** и введите нужное количество часов и минут в полях справа, чтобы указать максимальную длительность выполнения задачи.
     b. Установите флажок **Приостановить с** и введите начальное и конечное значение временного промежутка в полях справа, чтобы указать промежуток времени в пределах суток, в течение которого выполнение задачи будет приостановлено.
   - В блоке **Дополнительные параметры**:
     a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
     b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
     c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.
6. Нажмите на кнопку **OK**.

Настроенные параметры расписания запуска выбранной задачи будут сохранены.

Формирование области защиты

Этот раздел содержит информацию о формировании и использовании области защиты в задаче Постоянная защита файлов и дальнейшей работе с ней.

В этом разделе

Формирование области защиты

Процедура формирования области защиты в задаче Постоянная защита файлов зависит от типа отображения сетевых файловых ресурсов (см. раздел "Об области защиты и параметрах безопасности задачи" на стр. 240). Вы можете настроить отображение сетевых файловых ресурсов в виде дерева или в виде списка (по умолчанию).

Чтобы применить к задаче новые настройки области защиты, необходимо перезапустить задачу Постоянной защиты файлов.

► *Чтобы сформировать область защиты с помощью дерева сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "Переход к настройке области задачи Постоянная защита файлов" на стр. 263).
2. В левой части окна разверните дерево сетевых файловых ресурсов, чтобы отобразить все узлы.
3. Выполните следующие действия:
   - Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
     - Если вы хотите включить в область защиты все диски одного типа, установите флажок рядом с названием нужного типа дисков (например, чтобы включить все съемные диски компьютера, установите флажок **Съемные диски**).
     - Если вы хотите включить в область защиты отдельный диск определенного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем нужного диска. Например, чтобы выбрать съемный диск F:, разверните узел **Съемные диски** и установите флажок для диска **F:**.
     - если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.
4. Нажмите на кнопку **Сохранить**.

Окно параметров области защиты закроется. Настроенные параметры задачи будут сохранены.

► *Чтобы сформировать область защиты с помощью списка сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "Переход к настройке области задачи Постоянная защита файлов" на стр. 263).
2. Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
   a. Откройте контекстное меню области защиты по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область защиты**.
   c. В открывшемся окне **Добавление области защиты** выберите тип объекта, который вы хотите включить в область защиты:
      - **Предопределенная область**, если вы хотите включить в область защиты одну из стандартных областей на защищаемом компьютере. Затем в раскрывающемся списке выберите требуемую область защиты.
      - **Диск, папка или сетевой объект**, если вы хотите включить в область защиты отдельный диск, папку или сетевой объект. Затем выберите нужную область защиты по кнопке **Обзор**.
      - **Файл**, если вы хотите включить в область защиты отдельный файл. Затем выберите нужную область защиты по кнопке **Обзор**.

Вы не можете добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.

3. Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов или выполните следующие действия:
   a. Откройте контекстное меню области защиты по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В открывшемся окне **Добавление исключения** выберите тип объекта, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в область защиты.
4. Чтобы изменить добавленную область защиты или исключение, в контекстном меню требуемой области защиты выберите пункт **Изменить область**.
5. Чтобы скрыть отображение ранее добавленной области защиты или исключения в списке сетевых файловых ресурсов, в контекстном меню нужной области защиты выберите пункт **Удалить из списка**.

   Область защиты исключается из области действия задачи Постоянная защита файлов при ее удалении из списка сетевых файловых ресурсов.
6. Нажмите на кнопку **Сохранить**.

Окно параметров области защиты закроется. Настроенные параметры задачи будут сохранены.

Вы можете запустить задачу *Постоянная защита файлов*, если по крайней мере один узел файловых ресурсов компьютера включен в область защиты.

Если вы укажете сложную область защиты, например, установите различные значения параметров безопасности для нескольких узлов в дереве файловых ресурсов компьютера, это может замедлить проверку объектов при доступе.

Создание виртуальной области защиты

Вы можете включить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов (см. раздел "Настройка параметров отображения сетевых файловых ресурсов" на стр. 442).

► *Чтобы добавить виртуальный диск в область защиты, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "Переход к настройке области задачи Постоянная защита файлов" на стр. 263).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. Откройте контекстное меню узла **Виртуальные диски**.
4. Выберите пункт **Добавить виртуальный диск**.
5. В списке доступных имен выберите имя создаваемого виртуального диска.
6. Установите флажок рядом с добавленным диском, чтобы включить этот диск в область защиты.
7. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены.

► *Чтобы включить в область защиты виртуальную папку или виртуальный файл, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "Переход к настройке области задачи Постоянная защита файлов" на стр. 263).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. Откройте контекстное меню виртуального диска, в который вы хотите добавить папку или файл, и выберите один из следующих пунктов:
   - **Добавить виртуальную папку**, если требуется добавить виртуальную папку в область защиты;
   - **Добавить виртуальный файл**, если требуется добавить виртуальный файл в область защиты.
4. В поле ввода задайте имя для папки или файла.
5. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область защиты.
6. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Настройка параметров безопасности вручную

По умолчанию в задачах постоянной защиты компьютера применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый** (см. раздел "Стандартные уровни безопасности" на стр. 242).

Вы можете изменять заданные по умолчанию значения параметров безопасности, настроив их как едиными для всей области защиты, так и различными для разных элементов / узлов в списке / дереве файловых ресурсов компьютера.

При работе с деревом файловых ресурсов сервера параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

► *Чтобы настроить параметры безопасности вручную, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "Переход к настройке области задачи Постоянная защита файлов" на стр. 263).
2. В левой части окна выберите узел, параметры безопасности которого вы хотите настроить.

   К выбранному в области защиты узлу или элементу можно применить стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 158).

3. Настройте требуемые параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
   - **Общие** (см. раздел "**Настройка общих параметров задачи**" на стр. 272).
   - **Действия** (см. раздел "**Настройка действий**" на стр. 275).
   - **Производительность** (см. раздел "**Настройка производительности**" на стр. 277).
4. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Новые параметры области защиты будут сохранены.

В этом разделе

Настройка общих параметров задачи

► *Чтобы настроить общие параметры безопасности задачи Постоянная защита файлов, выполните следующие действия.*

1. Откройте окно **Настройка области защиты** (см. раздел "Переход к настройке области задачи Постоянная защита файлов" на стр. 263).
2. Выберите закладку **Общие**.
3. В блоке **Защита объектов** укажите объекты, которые требуется включить в область защиты:
   - **Все объекты**

     Kaspersky Embedded Systems Security проверяет все объекты.
   - **Объекты, проверяемые по формату**

     Kaspersky Embedded Systems Security проверяет только потенциально заражаемые файлы на основании формата файла.

     Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

  Kaspersky Embedded Systems Security проверяет только потенциально заражаемые файлы на основании расширения файла.

  Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security.

- **Объекты, проверяемые по указанному списку расширений**

  Kaspersky Embedded Systems Security проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Загрузочные секторы дисков и MBR**

  Включение защиты загрузочных секторов дисков и основных загрузочных записей.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках компьютера.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках файловой системы NTFS.

  Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

  Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

  По умолчанию флажок установлен.

4. В блоке **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security новыми или измененными с момента последней проверки.

   Если флажок установлен, Kaspersky Embedded Systems Security проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

   Если флажок не установлен, можно выбрать, требуется ли проверка и защита только новых файлов или всех файлов, независимо от того, когда они были изменены.

   По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**. Если выбран уровень безопасности **Максимальная защита** или **Рекомендуемый**, флажок не установлен.

   Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

5. В блоке **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область защиты:

- **Все / Только новые архивы**

  Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет архивы.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые SFX-архивы**

  Проверка самораспаковывающихся архивов.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет SFX-архивы.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает SFX-архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

  Параметр доступен, если снят флажок **Архивы**.

- **Все / Только новые почтовые базы**

  Проверка файлов почтовых баз Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает файлы почтовых баз при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые упакованные объекты**

  Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Embedded Systems Security при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

  Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые файлы почтовых форматов**

  Проверка файлов почтовых форматов, например, сообщения форматов Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые вложенные OLE-объекты**

  Проверка встроенных в файл объектов (например, макрос Microsoft Word или вложение сообщения электронной почты).

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает встроенные в файл объекты при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка действий

► *Чтобы настроить действия, которые задача Постоянная защита файлов выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "Переход к настройке области задачи Постоянная защита файлов" на стр. 263).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**

     Когда выбран этот режим, Kaspersky Embedded Systems Security не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** требуется настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security автоматически изменит уровень безопасности на **Другой**.

   - **Блокировать доступ**

     Если выбран этот вариант, Kaspersky Embedded Systems Security блокирует доступ к зараженным или другим обнаруженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

   - **Выполнять дополнительное действие**

     Выберите действие из раскрывающегося списка:

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

4. Выберите действие над возможно зараженными объектами:

   - **Только сообщать**

     Когда выбран этот режим, Kaspersky Embedded Systems Security не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен*. *Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** требуется настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security автоматически изменит уровень безопасности на **Другой**.

   - **Блокировать доступ**

     Если выбран этот вариант, Kaspersky Embedded Systems Security блокирует доступ к зараженным или другим обнаруженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

   - **Выполнять дополнительное действие**

     Выберите действие из раскрывающегося списка:

     - **Помещать на карантин**
     - **Удалять**
     - **Рекомендуемое**

5. Настройте действия над объектами в зависимости от типа обнаруженного объекта:

   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

      Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. При этом Kaspersky Embedded Systems Security не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Embedded Systems Security выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

      По умолчанию флажок снят.

   b. Нажмите на кнопку **Настройка**.

   c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.

   d. Нажмите на кнопку **OK**.

6. Выберите действие над неизменяемыми составными файлами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

   Флажок включает или выключает форсированное удаление родительского составного файла при обнаружении вложенного вредоносного, возможно

зараженного или другого обнаруживаемого объекта.

Если флажок установлен и задача настроена на удаление зараженных или возможно зараженных объектов, Kaspersky Embedded Systems Security принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление составного объекта со всем его содержимым выполняется в случае, если программа не может удалить только вложенный обнаруженный объект (например, если составной объект неизменяем).

Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security не выполняет выбранное действие, если родительский объект неизменяем.

7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

► *Чтобы настроить производительность задачи Постоянная защита файлов, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. Раздел "Переход к настройке области задачи Постоянная защита файлов" на стр. 263).
2. Выберите закладку **Производительность**.
3. В блоке **Исключения**:
   - Снимите или установите флажок **Исключать файлы**.

     Исключение файлов из проверки по имени файла или маске имени файла.

     Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security проверяет все объекты.

     По умолчанию флажок снят.
   - Снимите или установите флажок **Не обнаруживать**.

     Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

     Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.
   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.

4. В блоке **Дополнительные параметры**:

   - **Останавливать проверку, если она длится более (сек.)**

     Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

     Если флажок установлен, максимальная продолжительность проверки объекта ограничена указанным значением.

     Если флажок снят, максимальная продолжительность проверки не ограничена.

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

   - **Не проверять составные объекты размером более (МБ)**

     Исключение из проверки составных объектов больше указанного размера.

     Если флажок установлен, Kaspersky Embedded Systems Security пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

     Если флажок снят, Kaspersky Embedded Systems Security проверяет составные объекты, не учитывая размер.

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

   - **Использовать технологию iSwift**

     iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

     Если флажок установлен, Kaspersky Embedded Systems Security проверяет только новые файлы и файлы, изменившиеся с момента последней проверки системных объектов NTFS.

     Если флажок снят, Kaspersky Embedded Systems Security проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

     По умолчанию флажок установлен.

   - **Использовать технологию iChecker**

     iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы во время выполнения задачи проверки и проверяет только новые файлы и файлы, измененные с момента последней проверки.

     Если флажок установлен, Kaspersky Embedded Systems Security проверяет только новые и измененные файлы.

     Если флажок снят, Kaspersky Embedded Systems Security проверяет файлы независимо от даты их создания и изменения.

     По умолчанию флажок установлен.

Статистика задачи Постоянная защита файлов

Пока выполняется задача Постоянная защита файлов, вы можете просматривать в реальном времени информацию о количестве объектов, которые программа Kaspersky Embedded Systems Security обработала с момента запуска задачи до текущего момента.

► *Чтобы просмотреть статистику задачи Постоянная защита файлов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, обработанных Kaspersky Embedded Systems Security с момента запуска задачи до текущего момента (см. таблицу ниже).

Таблица 43. Статистика задачи Постоянная защита файлов

Поле	Описание
Обнаружено	Количество объектов, которые обнаружила программа Kaspersky Embedded Systems Security. Например, если программа Kaspersky Embedded Systems Security обнаружила в пяти файлах одну вредоносную программу, значение в этом поле увеличится на единицу.
Зараженных и других обнаруживаемых объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security признала зараженными, или количество обнаруженных легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или персональным данным.
Возможно зараженных объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security признала возможно зараженными.
Объектов не вылечено	Количество объектов, которые программа Kaspersky Embedded Systems Security не вылечила по следующим причинам: • тип обнаруженного объекта не предполагает лечения; • при лечении возникла ошибка.
Объектов не помещено на карантин	Количество объектов, которые программа Kaspersky Embedded Systems Security попыталась поместить на карантин, но безуспешно, например, из-за отсутствия доступного пространства на диске.
Объектов не удалено	Количество объектов, которые программа Kaspersky Embedded Systems Security попыталась удалить, но безуспешно, например, если доступ к объекту был заблокирован другой программой.
Объектов не проверено	Количество объектов в области защиты, которые программа Kaspersky Embedded Systems Security не смогла проверить, например, если доступ к объекту был заблокирован другой программой.

Поле	Описание
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых программа Kaspersky Embedded Systems Security попыталась сохранить в резервном хранилище, но безуспешно, например, из-за отсутствия доступного пространства на диске.
Ошибок обработки	Количество объектов, во время обработки которых возникла ошибка задачи.
Вылечено объектов	Количество объектов, которые вылечила программа Kaspersky Embedded Systems Security.
Помещено на карантин	Количество объектов, которые поместила на карантин программа Kaspersky Embedded Systems Security.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Embedded Systems Security сохранила в резервном хранилище.
Удалено объектов	Количество объектов, которые удалила программа Kaspersky Embedded Systems Security.
Защищенных паролем объектов	Количество объектов (например, архивов), которые программа Kaspersky Embedded Systems Security пропустила, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security пропустила, так как их формат искажен.
Обработано объектов	Общее количество объектов, которые обработала программа Kaspersky Embedded Systems Security.

Вы также можете посмотреть статистику задачи Постоянная защита файлов в журнале выполнения задачи по ссылке **Открыть журнал выполнения** в блоке **Управление** панели результатов.

Если значение в поле **Всего событий:** в окне журнала выполнения задачи Постоянная защита файлов больше 0, рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

Использование KSN

Этот раздел содержит информацию о задаче Использование KSN и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Использование KSN

Kaspersky Security Network (далее также "KSN") – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программ. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Embedded Systems Security на новые угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

Kaspersky Embedded Systems Security получает от Kaspersky Security Network только информацию о репутации программ.

Участие пользователей в KSN позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний компонентов программы.

Более подробная информация о передаче, обработке, хранении и уничтожении информации об использовании программы приведена в окне **Передача данных** задачи Использование KSN и в Политике конфиденциальности на веб-сайте "Лаборатории Касперского".

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается после установки Kaspersky Embedded Systems Security. Вы можете изменить свое решение об участии в Kaspersky Security Network в любой момент.

Kaspersky Security Network может использоваться в следующих задачах Kaspersky Embedded Systems Security:

- Постоянная защита файлов.
- Проверка по требованию.
- Контроль запуска программ.

Kaspersky Private Security Network

Подробнее о том, как настроить Kaspersky Private Security Network (далее также "Локальный KSN"), см. в *Справке Kaspersky Security Center*.

Если вы используете Локальный KSN на защищаемом компьютере, в окне **Обработка данных** (см. раздел "Настройка обработки данных с помощью Плагина управления" на стр. 286) задачи Использование KSN можно ознакомиться с Положением о KSN и включить использование компонента, установив флажок **Я принимаю условия Положения о Kaspersky Private Security Network**. Принимая условия, вы соглашаетесь отправлять все типы данных, упомянутые в Положении о KSN (запросы безопасности, статистические данные), в службы KSN.

После принятия условий Локального KSN флажки, регулирующие использование Глобального KSN, недоступны.

Если вы отключаете Локальный KSN во время выполнения задачи Использование KSN, происходит ошибка *Нарушение лицензии* и выполнение задачи прекращается. Чтобы продолжить защищать компьютер, требуется принять Положение о KSN в окне **Обработка данных** и перезапустить задачу.

Отзыв согласия с Положением о KSN

Вы можете отозвать свое согласие и прекратить обмен данными с Kaspersky Security Network в любой момент. Следующие действия считаются полным или частичным отзывом согласия с Положением о KSN:

- Вы сняли флажок **Разрешить отправку данных о проверяемых файлах**: программа перестает отправлять контрольные суммы проверенных файлов в службу KSN для анализа.
- Вы сняли флажок **Разрешить отправку статистики Kaspersky Security Network**: программа прекращает обрабатывать данные с дополнительной статистикой KSN.
- Вы сняли флажок **Я принимаю условия Положения о Kaspersky Security Network**: программа прекращает обрабатывать все связанные с KSN данные, выполнение задачи Использование KSN прекращается.
- Вы удалили компонент Использование KSN: обработка всех связанных с KSN данных останавливается.
- Вы удалили Kaspersky Embedded Systems Security: обработка всех связанных с KSN данных останавливается.

Параметры по умолчанию для задачи Использование KSN

Можно изменять параметры задачи Использование KSN, заданные по умолчанию (см. таблицу ниже).

Таблица 44. Параметры по умолчанию для задачи Использование KSN

Параметр	Значение по умолчанию	Описание
Действие над объектами, недоверенными в KSN	Удалить	Можно указать действия, которые Kaspersky Embedded Systems Security будет выполнять над объектами, имеющими репутацию недоверенных в KSN.
Отправка данных	Контрольная сумма файла (MD5-хеш) рассчитывается для файлов, размер которых не превышает 2 МБ.	Вы можете указывать максимальный размер файлов, для которых рассчитывается контрольная сумма по алгоритму MD5 для отправки в KSN. Если флажок снят, Kaspersky Embedded Systems Security рассчитывает MD5-хеш для файлов любого размера.
Расписание запуска задачи	Первый запуск не определен.	Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.
Использовать Kaspersky Security Center как прокси-сервер KSN	Выбрано.	По умолчанию все данные отправляются в KSN через Kaspersky Security Center. Этот параметр можно изменять только с помощью Плагина управления.
Я принимаю условия Положения о Kaspersky Security Network	Флажок снят	Если флажок установлен, будет принято согласие на участие в KSN после установки. Вы можете изменить свое решение в любой момент.
Разрешить отправку статистики Kaspersky Security Network	Установлен (применяется, только если принято Положение о KSN).	Если вы приняли Положение о KSN, статистика будет отправляться автоматически, пока вы не снимете флажок.
Разрешить отправку данных о проверяемых файлах	Установлен (применяется, только если принято Положение о KSN).	Если Положение о KSN принято, данные о файлах, которые были проверены и проанализированы с момента запуска задачи, отправляются. Снять флажок можно в любой момент.
Разрешить отправку данных о проверяемых веб-адресах	Установлен (применяется, только если принято Положение о KSN).	Если принято положение о KSN, программа отправляет данные о веб-адресах, к которым осуществлялся доступ, в "Лабораторию Касперского".

Параметр	Значение по умолчанию	Описание
Принять условия Положения о Kaspersky Managed Protection	Флажок снят	Вы можете включать и выключать службу KMP. Служба доступна, только если во время приобретения программы был подписан дополнительный договор.

Управление использованием KSN с помощью Плагина управления

В этом разделе описана настройка использования KSN и обработки данных с помощью Плагина управления.

В этом разделе

Настройка задачи Использование KSN с помощью Плагина управления

► *Чтобы настроить параметры задачи Использование KSN, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в блоке **Использование KSN**.

   Откроется окно **Использование KSN**.

5. На закладке **Общие** настройте следующие параметры задачи:

   - В блоке **Действия над объектами, недоверенными в KSN** укажите действие, которое Kaspersky Embedded Systems Security необходимо совершить при обнаружении объекта, имеющего репутацию недоверенного в KSN:

     - **Удалить**

       Kaspersky Embedded Systems Security удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.

       Данный вариант выбран по умолчанию.

     - **Фиксировать информацию в отчете**

       Kaspersky Embedded Systems Security фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Embedded Systems Security не удаляет недоверенный объект.

   - В блоке **Отправка данных** ограничьте размер файлов, для которых вычисляется контрольная сумма:

     - Снимите или установите флажок **Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает (МБ)**.

       Флажок включает или выключает расчет контрольной суммы файлов установленного размера для отправки этой информации в службы KSN.

       Продолжительность расчета контрольной суммы зависит от размера файла.

       Если флажок установлен, Kaspersky Embedded Systems Security не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ).

       Если флажок снят, Kaspersky Embedded Systems Security рассчитывает контрольную сумму для файлов любого размера.

       По умолчанию флажок установлен.

     - Если требуется, в поле справа измените значение максимального размера файлов, для которых Kaspersky Embedded Systems Security будет рассчитывать контрольную сумму.

   - В блоке **Прокси-сервер KSN** снимите или установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера KSN**.

     Флажок позволяет управлять передачей данных от защищаемых компьютеров в KSN.

     Если флажок снят, данные с Сервера администрирования и защищаемых компьютеров отправляются напрямую в KSN (минуя Kaspersky Security Center). Активная политика определяет, какой тип данных отправляется в KSN напрямую.

     Если флажок установлен, все данные отправляются в KSN через Kaspersky Security Center.

     По умолчанию флажок установлен.

Чтобы включить прокси-сервер KSN, необходимо принять Положение о KSN и настроить Kaspersky Security Center. Подробнее см. в *Справке Kaspersky Security Center*.

6. Если требуется, настройте расписание запуска задачи на закладке **Управление задачей**. Например, вы можете включить запуск задачи по расписанию и указать частоту запуска задачи **При запуске программы**, если вы хотите, чтобы задача автоматически запускалась после перезагрузки сервера.

   Программа будет запускать задачу Использование KSN по расписанию.

7. Перед запуском задачи настройте обработку данных (см. раздел "Настройка обработки данных с помощью Плагина управления" на стр. 286).

8. Нажмите на кнопку **OK**.

Изменения параметров задачи будут применены. Дата и время изменения параметров, а также информация о параметрах задачи до и после их изменения будут сохранены в журнале системного аудита.

Настройка обработки данных с помощью Плагина управления

► *Чтобы настроить типы данных, которые будут обрабатываться службами KSN, и принять Положение о KSN, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

   > Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Обработка данных** в блоке **Использование KSN**.

   Откроется окно **Обработка данных**.

5. На закладке **Службы и статистика** прочитайте текст Положения и установите флажок **Я принимаю условия Положения о Kaspersky Security Network**.
6. Для повышения уровня защиты, следующие флажки установлены по умолчанию:
   - **Отправлять данные о проверяемых файлах**.

     Если флажок установлен, Kaspersky Embedded Systems Security отправляет контрольные суммы проверенных файлов в "Лабораторию Касперского". Заключение о безопасности каждого файла основано на репутации, полученной от KSN.

Если флажок снят, Kaspersky Embedded Systems Security не отправляет контрольные суммы файлов в KSN.

Обратите внимание, что запросы файловой репутации могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом сценарии параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом компьютере. Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если ограниченный режим применяется, в статистике задачи Использование KSN отображается статус *Отправка запросов репутации в ограниченном режиме: применено "Лабораторией Касперского" с целью защиты репутационных серверов от DDoS*.

По умолчанию флажок установлен.

- **Разрешить отправку статистики Kaspersky Security Network**

  Если флажок установлен, Kaspersky Embedded Systems Security отправляет дополнительную статистику, которая может содержать персональные данные. Список данных, отправляемых в качестве статистики KSN, указан в Положении о KSN. Данные, полученные "Лабораторией Касперского", используются для улучшения качества программ и повышения скорости обнаружения угроз.

  Если флажок снят, Kaspersky Embedded Systems Security не отправляет дополнительную статистику.

  По умолчанию флажок установлен.

Вы можете снять флажки и прекратить передачу дополнительных данных в любой момент.

7. На закладке **Kaspersky Managed Protection** ознакомьтесь с Положением и установите флажок **Я принимаю условия Положения о Kaspersky Managed Protection**.

   Если флажок установлен, вы соглашаетесь отправлять статистику активности защищаемого компьютера специалистам "Лаборатории Касперского". Полученные данные используются для круглосуточного анализа и отчетности, необходимых для предотвращения нарушений безопасности.

   По умолчанию флажок снят.

При изменении состояния флажка **Я принимаю условия Положения о Kaspersky Managed Protection** не происходит немедленный запуск или остановка обработки данных. Для того чтобы изменения вступили в силу, необходимо перезапустить Kaspersky Embedded Systems Security.

Для использования KMP-сервиса необходимо подписать соответствующее соглашение и запустить исполнение конфигурационных файлов на защищаемом компьютере.

Для использования службы KMP необходимо принять условия обработки данных Положения о KSN на закладке **Службы и статистики KSN**.

8. Нажмите на кнопку **OK**.

   Конфигурация обработки данных будет сохранена.

Управление использованием KSN с помощью Консоли программы

В этом разделе описана настройка использования KSN и обработки данных с помощью Консоли программы.

В этом разделе

Настройка задачи Использование KSN с помощью Консоли программы

► *Чтобы настроить параметры задачи Использование KSN, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Настройте параметры задачи:
   - В блоке **Действия над объектами, недоверенными в KSN** укажите действие, которое Kaspersky Embedded Systems Security необходимо совершить при обнаружении объекта, имеющего репутацию недоверенного в KSN:
     - **Удалить**

       Kaspersky Embedded Systems Security удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.

       Данный вариант выбран по умолчанию.
     - **Фиксировать информацию в отчете**

       Kaspersky Embedded Systems Security фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Embedded Systems Security не удаляет недоверенный объект.

- В блоке **Отправка данных** ограничьте размер файлов, для которых вычисляется контрольная сумма:
  - Снимите или установите флажок **Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает (МБ)**.

    Флажок включает или выключает расчет контрольной суммы файлов установленного размера для отправки этой информации в службы KSN.

    Продолжительность расчета контрольной суммы зависит от размера файла.

    Если флажок установлен, Kaspersky Embedded Systems Security не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ).

    Если флажок снят, Kaspersky Embedded Systems Security рассчитывает контрольную сумму для файлов любого размера.

    По умолчанию флажок установлен.
  - Если требуется, в поле справа измените значение максимального размера файлов, для которых Kaspersky Embedded Systems Security будет рассчитывать контрольную сумму.

5. Если требуется, настройте расписание запуска задачи на закладках **Расписание** и **Дополнительно**. Например, вы можете включить запуск задачи по расписанию и указать частоту запуска задачи **При запуске программы**, если хотите, чтобы задача автоматически запускалась после перезагрузки компьютера.

   Программа будет запускать задачу Использование KSN по расписанию.

6. Перед запуском задачи настройте обработку данных (см. раздел "Настройка обработки данных с помощью Консоли программы" на стр. 289).

7. Нажмите на кнопку **OK**.

Изменения параметров задачи будут применены. Дата и время изменения параметров, а также информация о параметрах задачи до и после их изменения будут сохранены в журнале системного аудита.

Настройка обработки данных с помощью Консоли программы

► *Чтобы настроить типы данных, которые будут обрабатываться службами KSN, и принять Положение о KSN, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Обработка данных**.

   Откроется окно **Обработка данных**.

4. На закладке **Службы и статистика** прочитайте текст Положения и установите флажок **Я принимаю условия Положения о Kaspersky Security Network**.

5. Для повышения уровня защиты, следующие флажки установлены по умолчанию:

   - **Отправлять данные о проверяемых файлах**.

     Если флажок установлен, Kaspersky Embedded Systems Security отправляет контрольные суммы проверенных файлов в "Лабораторию Касперского". Заключение о безопасности каждого файла основано на репутации, полученной от KSN.

     Если флажок снят, Kaspersky Embedded Systems Security не отправляет контрольные суммы файлов в KSN.

     Обратите внимание, что запросы файловой репутации могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом сценарии параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом компьютере. Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если ограниченный режим применяется, в статистике задачи Использование KSN отображается статус *Отправка запросов репутации в ограниченном режиме: применено "Лабораторией Касперского" с целью защиты репутационных серверов от DDoS*.

     По умолчанию флажок установлен.

   - **Разрешить отправку статистики Kaspersky Security Network**

     Если флажок установлен, Kaspersky Embedded Systems Security отправляет дополнительную статистику, которая может содержать персональные данные. Список данных, отправляемых в качестве статистики KSN, указан в Положении о KSN. Данные, полученные "Лабораторией Касперского", используются для улучшения качества программ и повышения скорости обнаружения угроз.

     Если флажок снят, Kaspersky Embedded Systems Security не отправляет дополнительную статистику.

     По умолчанию флажок установлен.

   Вы можете снять флажки и прекратить передачу дополнительных данных в любой момент.

6. На закладке **Kaspersky Managed Protection** ознакомьтесь с Положением и установите флажок **Я принимаю условия Положения о Kaspersky Managed Protection**.

   Если флажок установлен, вы соглашаетесь отправлять статистику активности защищаемого компьютера специалистам "Лаборатории Касперского". Полученные данные используются для круглосуточного анализа и отчетности, необходимых для предотвращения нарушений безопасности.

   По умолчанию флажок снят.

При изменении состояния флажка **Я принимаю условия Положения о Kaspersky Managed Protection** не происходит немедленный запуск или остановка обработки данных. Для того чтобы изменения вступили в силу, необходимо перезапустить Kaspersky Embedded Systems Security.

Для использования KMP-сервиса необходимо подписать соответствующее соглашение и запустить исполнение конфигурационных файлов на защищаемом компьютере.

Для использования службы KMP необходимо принять условия обработки данных Положения о KSN на закладке **Службы и статистики KSN**.

7. Нажмите на кнопку **OK**.

Конфигурация обработки данных будет сохранена.

Настройка передачи дополнительных данных

В Kaspersky Embedded Systems Security можно настроить отправку в "Лабораторию Касперского" следующих данных:

- контрольных сумм проверенных файлов (флажок **Разрешить отправку данных о проверенных файлах**);
- дополнительной статистики, включая персональные данные (флажок **Разрешить отправку статистики Kaspersky Security Network**).

Подробнее о данных, отправляемых в "Лабораторию Касперского", см. в разделе "Локальная обработка данных" этого руководства.

Соответствующие флажки можно установить или снять (см. раздел "Настройка обработки данных с помощью Консоли программы" на стр. 289), только если установлен флажок **Я принимаю условия Положения о Kaspersky Security Network**.

По умолчанию Kaspersky Embedded Systems Security отправляет контрольные суммы файлов и дополнительную статистику после принятия Положения о KSN.

Таблица 45. Возможные состояния флажков и соответствующие условия

Состояние флажка	**Условия для состояния флажка** Разрешить отправку данных о проверяемых файлах	**Условия для состояния флажка** Разрешить отправку статистики Kaspersky Security Network	**Условия для состояния флажка** Разрешить отправку данных о запрашиваемых веб-адресах	**Условия для состояния флажка** Я принимаю условия Положения о Kaspersky Managed Protection	**Условия для состояния флажка** Я принимаю условия Положения о Kaspersky Managed Protection
☑	• отправляются запросы репутации • действия с флажком доступны	• отправляется дополнительная статистика • действия с флажком доступны	• отправляются данные о проверенных веб-адресах • действия с флажком доступны	• принимаются условия Положения о Kaspersky Managed Protection • действия с флажком доступны	• принимаются условия Положения о Kaspersky Security Network • действия с флажком доступны
☑	• отправляются запросы репутации • действия с флажком недоступны	• отправляется дополнительная статистика • действия с флажком недоступны	• отправляются данные о проверенных веб-адресах • действия с флажком недоступны	• принимаются условия Положения о Kaspersky Managed Protection • действия с флажком недоступны	• принимаются условия Положения о Kaspersky Security Network • действия с флажком недоступны
☐	• не отправляются запросы репутации • действия с флажком доступны	• не отправляется дополнительная статистика • действия с флажком доступны	• не отправляются данные о проверенных веб-адресах • действия с флажком доступны	• не принимаются условия Положения о Kaspersky Managed Protection • действия с флажком доступны	• не принимаются условия Положения о Kaspersky Security Network • действия с флажком доступны
☐	• не отправляются запросы репутации • действия с флажком недоступны	• не отправляется дополнительная статистика • действия с флажком недоступны	• не отправляются данные о проверенных веб-адресах • действия с флажком недоступны	• не принимаются условия Положения о Kaspersky Managed Protection • действия с флажком недоступны	• не принимаются условия Положения о Kaspersky Security Network • действия с флажком недоступны

Статистика задачи Использование KSN

Пока выполняется задача Использование KSN, вы можете просматривать в реальном времени информацию о количестве объектов, которые программа Kaspersky Embedded Systems Security обработала с момента ее запуска до текущего момента. Информация обо всех событиях, произошедших во время выполнения задачи, регистрируется в журнале выполнения задачи (см. раздел "О журналах выполнения задач" на стр. 206).

► *Чтобы просмотреть статистику задачи Использование KSN, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Использование KSN**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, которые программа Kaspersky Embedded Systems Security обработала за время выполнения задачи (см. таблицу ниже).

Таблица 46. Статистика задачи Использование KSN

Поле	Описание
Ошибки отправки запросов	Количество запросов в KSN, во время обработки которых возникла ошибка задачи.
Пакетов статистик сформировано	Количество пакетов с данными, которые были отправлены на обработку в KSN.
Удалено объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security удалила в результате выполнения задачи Использование KSN.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Embedded Systems Security сохранила в резервном хранилище.
Объектов не удалено	Количество объектов, которые программа Kaspersky Embedded Systems Security попыталась удалить, но безуспешно, например, если доступ к объекту был заблокирован другой программой. Информация о таких объектах записывается в журнал выполнения задачи.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых программа Kaspersky Embedded Systems Security попыталась сохранить в резервном хранилище, но безуспешно, например, из-за отсутствия доступного пространства на диске. Программа не лечит и не удаляет файлы, которые не удалось поместить в резервное хранилище. Информация о таких объектах записывается в журнал выполнения задачи.
Ограниченный режим	Статус отправки запросов файловой репутации в ограниченном режиме.

Контроль запуска программ

Этот раздел содержит информацию о задаче Контроль запуска программ и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Контроль запуска программ

Во время выполнения задачи Контроль запуска программ Kaspersky Embedded Systems Security проверяет попытки пользователей запускать различные программы и разрешает или запрещает запуск этих программ. Задача Контроль запуска программ работает по принципу запрета по умолчанию: все программы, не указанные в качестве разрешенных в параметрах задачи, автоматически блокируются.

Вы можете разрешить запуск программ одним из следующих способов:

- задать разрешающие правила для доверенных программ;
- проверять репутацию доверенных программ в KSN при их запуске.

Запрет запуска программы имеет в задаче более высокий приоритет. Например, если запуск программы запрещен одним из правил, программа не будет запущена, независимо от заключения KSN о доверенности программы. При этом если программа признана недоверенной службами KSN, но подпадает под действие разрешающего правила, запуск такой программы будет запрещен.

Все попытки запуска программ фиксируются в журнале выполнения задач (см. раздел "О журналах выполнения задач" на стр. 206).

Задача Контроль запуска программ может выполняться в одном из двух режимов:

- **Активный**. Kaspersky Embedded Systems Security с помощью набора правил контролирует запуск программ, которые попадают под действия правил контроля запуска программ. Область применения правил контроля запуска программ указывается в параметрах этой задачи. Если программа удовлетворяет правилам контроля запуска программ, а параметры задачи не удовлетворяют ни одному из указанных правил, то запуск такой программы будет запрещен.

Запуск программ, которые не подпадают под действие правил, указанных в параметрах задачи Контроль запуска программ, разрешен, независимо от параметров задачи Контроль запуска программ.

Задачу **Контроль запуска программ** нельзя запустить в активном режиме, если не создано ни одного правила или если для одного компьютера создано более 65535 правил.

- **Только статистика**. В Kaspersky Embedded Systems Security не используются правила контроля запуска программ для запрета или разрешения запуска программ. Выполняется только запись информации обо всех запусках программ, правилах, выполненных при запуске программ, и действиях, которые были бы выполнены, если бы задача выполнялась в режиме **Активный**. Разрешен запуск всех программ. Этот режим установлен по умолчанию.

  Вы можете использовать этот режим для формирования правил контроля запуска программ (см. раздел "Формирование разрешающих правил по событиям задачи Контроль запуска программ" на стр. 342) на основе информации, зафиксированной в журнале выполнения задачи.

Вы можете настроить задачу Контроль запуска программ по одному из следующих сценариев:

- дополнительная настройка и применение правил контроля запуска программ (см. раздел "О правилах контроля запуска программ" на стр. 295).
- базовая настройка правил и использование KSN для Контроля запуска программ (см. раздел "Настройка использования KSN" на стр. 335).

Если файлы операционной системы попадают под действие задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что новые правила разрешают запуск таких программ. В противном случае операционная система может не запуститься.

Kaspersky Embedded Systems Security также перехватывает процессы, запущенные в рамках подсистемы Windows для Linux (за исключением скриптов, запущенных из оболочки UNIX™, или командных интерпретаторов). Для данных целей задача Контроль запуска программ применяет действия, указанные в текущих настройках. Задача Формирование правил контроля запуска программ фиксирует запуск программы и создает соответствующие правила для программ, работающих в рамках Windows Subsystem для Linux.

О правилах контроля запуска программ

Как работают правила контроля запуска программ

Работа правил контроля запуска программ основана на следующих составляющих:

- Тип правила.

  Правила контроля запуска программ могут разрешить или запретить запуск программы. Соответственно, они называются *разрешающими* или *запрещающими*. Для создания списка разрешающих правил контроля запуска программ можно использовать задачу формирования разрешающих правил или задачу Контроль запуска программ в режиме **Только статистика**. Можно также добавлять разрешающие правила вручную.

- Пользователь и / или группа пользователей.

  Правила контроля запуска программ контролируют запуск указанных программ пользователем или группой пользователей.

- Область применения правила.

  Правила контроля запуска программ могут применяться к *исполняемым файлам*, *скриптам* и *пакетам MSI*.

- Критерий срабатывания правила.

  Правила контроля запуска программ регулируют запуск файлов, удовлетворяющих одному из указанных в параметрах правила критериев: подписаны указанным *цифровым сертификатом*, обладают указанным *хешем SHA256* или расположены по указанному *пути*.

  Если в качестве критерия срабатывания правила выбран **Цифровой сертификат**, созданное правило контролирует запуск всех доверенных программ в операционной системе. Вы можете задать более строгие условия для этого критерия, установив следующие флажки:

  - **Использовать заголовок**

    Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

    Если флажок установлен, заголовок указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

    Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

    Заголовок цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над разделом **Критерий срабатывания правила**.

    По умолчанию флажок снят.

  - **Использовать отпечаток**

    Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

    Если флажок установлен, отпечаток указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

    Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над разделом **Критерий срабатывания правила**.

По умолчанию флажок снят.

Использование отпечатка наиболее строго ограничивает срабатывание правил запуска программ на основе цифрового сертификата, поскольку отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан, в отличие от заголовка цифрового сертификата.

Вы можете задать исключения для правила контроля запуска программ. Исключения из правила контроля запуска программ основываются на тех же критериях, по которым срабатывают правила: цифровой сертификат, хеш SHA256 или путь к файлу. Исключения из правил контроля запуска программ могут понадобиться для определенных разрешающих правил: например, если требуется разрешить пользователям запуск программ по пути C:\Windows, но при этом запретить запуск файла Regedit.exe.

Если файлы операционной системы попадают под действие задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что новые правила разрешают запуск таких программ. В противном случае операционная система может не запуститься.

Управление правилами контроля запуска программ

Вы можете выполнять следующие действия с правилами контроля запуска программ:

- Добавлять правила вручную.
- Формировать и добавлять правила автоматически.
- Удалять правила.
- Экспортировать правила в файл.
- Проверять выбранные файлы на наличие правил, разрешающих запуск этих файлов.
- Фильтровать список правил по заданному критерию.

О Контроле пакетов установки

Формирование правил контроля запуска программ может усложниться, если вы хотите контролировать распространение программного обеспечения на защищаемых компьютерах, например, на компьютерах, где происходит регулярное автоматическое обновление установленного программного обеспечения. В этом случае требуется обновлять списки разрешающих правил после каждого обновления программного обеспечения, чтобы в параметрах задачи Контроль запуска программ учитывались новые файлы, созданные в процессе обновления. Для упрощения контроля запуска файлов в сценариях распространения программного обеспечения можно использовать подсистему Контроль пакетов установки.

Пакет установки (далее также "пакет") представляет собой программу, устанавливаемую на компьютер. В каждом пакете содержится как минимум одна программа, а также могут содержаться отдельные файлы, обновления и отдельные команды, в частности, когда выполняется установка программы или обновления.

Модуль Контроль пакетов установки реализован в виде дополнительного списка исключений. При добавлении пакета установки в список он становится доверенным. Для доверенных пакетов разрешается распаковка, а для программ, установленных или обновленных из доверенных пакетов, разрешается автоматический запуск. Извлеченные файлы могут наследовать признак доверенности от основного пакета установки. *Основной пакет установки* – это пакет, добавленный в список исключений контроля пакетов установки и ставший доверенным пакетом.

Kaspersky Embedded Systems Security контролирует только полный цикл распространения программного обеспечения. Программа не может корректно обработать запуск файлов, измененных доверенным пакетом, если при первом запуске пакета был выключен компонент Контроль пакетов установки или не был установлен компонент Контроль запуска программ.

Контроль пакетов установки невозможен, если в параметрах задачи Контроль запуска программ не установлен флажок **Использовать правила для исполняемых файлов**.

Кеш распространения программного обеспечения

Kaspersky Embedded Systems Security использует динамически формируемый кеш распространения программного обеспечения (далее "кеш распространения") для связи между доверенными пакетами и файлами, созданными во время распространения программного обеспечения. При первом запуске пакета Kaspersky Embedded Systems Security обнаруживает все файлы, созданные этим пакетом во время распространения программного обеспечения, и сохраняет контрольные суммы и пути файлов в кеше распространения. Затем, по умолчанию, разрешается запуск всех файлов в кеше распространения.

Кеш распространения нельзя просматривать, очищать и изменять вручную через пользовательский интерфейс. Kaspersky Embedded Systems Security самостоятельно наполняет его, а также контролирует его актуальность.

Кеш распространения можно экспортировать в конфигурационный файл (в формате XML) и очищать с помощью команд командной строки.

► *Чтобы экспортировать кеш распространения в конфигурационный файл, выполните команду:*

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

► *Чтобы полностью очистить кеш распространения, выполните команду:*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security обновляет кеш распространения раз в сутки. При изменении контрольной суммы разрешенного ранее файла программа удаляет запись для этого файла из кеша распространения. При активном режиме работы задачи Контроль запуска программ дальнейшие попытки запуска этого файла будут заблокированы. При изменении полного пути к разрешенному ранее файлу последующие попытки запустить этот файл не блокируются, поскольку контрольная сумма хранится в кеше распространения.

Обработка извлеченных файлов

Все извлеченные из доверенного пакета файлы наследуют атрибут доверенности при первом запуске пакета. При снятии флажка после первого запуска все извлеченные из пакета файлы сохраняют атрибут наследования. Чтобы отменить признак наследования для всех извлеченных файлов, необходимо очистить кеш распространения и снять флажок **Разрешать исполнение всей цепочке файлов, извлеченных из этого пакета установки** перед следующим запуском доверенного пакета установки.

Извлеченные файлы и пакеты, созданные основным доверенным пакетом установки, наследуют признак доверенности, поскольку их контрольные суммы добавляются в кеш распространения, когда пакет установки из списка исключений открывается в первый раз. Таким образом, сам пакет установки и все извлеченные из него файлы являются доверенными. По умолчанию количество уровней наследования признака доверенности не ограничено.

Извлеченные файлы сохраняют признак доверенности при перезагрузке операционной системы.

Обработка файлов настраивается в параметрах Контроля пакетов установки (см. раздел "Настройка Контроля пакетов установки" на стр. 312) с помощью флажка **Разрешать исполнение всей цепочке файлов, извлеченных из этого пакета установки**.

Например, если пакет test.msi, содержащий несколько пакетов и программ, добавлен в список исключений и установлен флажок, то все пакеты и программы, содержащиеся в пакете test.msi, можно распаковать и запустить, даже если они содержат другие вложенные файлы. Это соблюдается для всех уровней вложенности.

Если пакет test.msi добавлен в список исключений, а флажок **Разрешать исполнение всей цепочке файлов, извлеченных из этого пакета установки** не установлен, программа присваивает признак доверенности только пакетам и исполняемым файлам, извлеченным непосредственно из основного доверенного пакета (только первого уровня вложенности). Контрольные суммы этих файлов хранятся в кеше распространения. Все файлы второго и следующих уровней вложенности блокируются согласно принципу запрета по умолчанию.

Работа со списком правил контроля запуска программ

Список доверенных пакетов подсистемы Контроля пакетов установки – это список исключений, который дополняет, но не заменяет основной список правил контроля запуска программ.

Запрещающие правила контроля запуска программ имеют абсолютный приоритет: распаковка доверенного пакета или запуск созданных и измененных им файлов будут заблокированы, если такие пакеты и файлы подпадают под запрещающие правила контроля запуска программ.

Исключения Контроля пакетов установки учитываются и для доверенных пакетов, и для созданных и измененных ими файлов, если к таким пакетам и файлам не применяются запрещающие правила из списка правил контроля запуска программ.

Использование заключений KSN

Заключения KSN о том, что файл является недоверенным, имеют более высокий приоритет, чем исключения Контроля пакетов установки. Распаковка доверенных пакетов и запуск файлов, созданных или измененных доверенными пакетами, будет заблокирован, если для таких файлов получено заключение KSN о том, что файл является недоверенным.

При распаковке из доверенного пакета, запуск всех вложенных файлов будет разрешен, независимо от использования KSN в задаче Контроль запуска программ. При этом значение флажков **Запрещать запуск программ, недоверенных в KSN** и **Разрешать запуск программ, доверенных в KSN** не влияет на флажок **Разрешать исполнение всей цепочке файлов, извлеченных из этого пакета установки**.

Об использовании KSN в задаче Контроль запуска программ

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

Если данные KSN о репутации программы используются в задаче Контроль запуска программ, репутация программы по данным KSN считается основным критерием для разрешения или запрета запуска этой программы. Если KSN передает Kaspersky Embedded Systems Security данные о том, что программа не является доверенной, то попытка пользователя запустить программу блокируется. Если KSN передает Kaspersky Embedded Systems Security данные о том, что программа является доверенной, то разрешается запуск программы пользователем. KSN можно применять совместно с правилами контроля запуска программ или в качестве самостоятельного критерия блокировки запуска программ.

Применение заключений KSN в качестве самостоятельного критерия блокировки запуска программ

Этот сценарий позволяет безопасно контролировать запуски программ на защищаемом компьютере без расширенной настройки списка правил.

Вы можете применить заключения KSN к Kaspersky Embedded Systems Security вместе с единственным указанным правилом. Будет разрешен запуск только тех программ, которые имеют статус доверенных в KSN, или запускать которые разрешает указанное правило.

При использовании этого сценария рекомендуется задать правило, разрешающее запуск программ по цифровому сертификату.

Все остальные программы будут блокироваться в соответствии с принципом запрета по умолчанию. Применение KSN, при отсутствии правил, позволяет защитить компьютер от программ, которые по данным KSN представляют угрозу.

Применение заключений KSN совместно с правилами контроля запуска программ

При использовании заключений KSN совместно с правилами контроля запуска программ применяются следующие условия:

- Kaspersky Embedded Systems Security всегда блокирует запуск программы, если она подпадает под действие хотя бы одного запрещающего правила. Если такая программа признана доверенной службами KSN, это заключение имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволит вам расширить список нежелательных программ.
- Kaspersky Embedded Systems Security всегда блокирует запуск программы, если установлен запрет запуска программ, недоверенных в KSN, и данная программа признана недоверенной службами KSN. Если для этой программы задано разрешающее правило, оно имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволяет защитить компьютер от программ, которые по данным KSN представляют угрозу, но не были учтены при первоначальной настройке правил.

Формирование правил контроля запуска программ

Вы можете создать списки правил контроля запуска программ с помощью задач и политик Kaspersky Security Center одновременно для всех компьютеров и групп компьютеров в сети организации. Этот вариант рекомендуется, если в сети организации нет эталонной машины и вы не можете сформировать список разрешающих правил на основе программ, установленных на эталонной машине. Также можно запустить задачу Формирование правил контроля запуска программ локально через Консоль программы, чтобы создать список правил на основе программ, запущенных на отдельном компьютере.

По умолчанию компонент Контроль запуска программ устанавливается с двумя разрешающими правилами:

- Разрешающее правило для скриптов и MSI-файлов с сертификатом, доверенным в операционной системе.
- Разрешающее правило для исполняемых файлов с сертификатом, доверенным в операционной системе.

Вы можете создавать списки правил контроля запуска программ на стороне Kaspersky Security Center двумя способами:

- С помощью групповой задачи Формирование правил контроля запуска программ.

  В рамках этого сценария групповая задача формирует собственный список правил контроля запуска программ для каждого компьютера в сети и сохраняет эти списки в XML-файл в указанной папке общего доступа. XML-файл, созданный задачей Формирование правил контроля запуска программ, содержит разрешающие правила, указанные при настройке параметров задачи, до ее запуска. Для программ, запуск которых не разрешен в параметрах указанной задачи, не будет создано ни одного правила. Запуск таких программ будет заблокирован по умолчанию. Затем вы можете вручную импортировать сформированные списки правил в задачу Контроль запуска программ для политики Kaspersky Security Center. В политике Kaspersky Security Center также можно настроить автоматическое добавление созданных правил в список правил контроля запуска программ по завершении групповой задачи формирования правил контроля запуска программ.

  Вы можете настроить автоматический импорт сформированных правил в список правил задачи Контроль запуска программ.

  Рекомендуется использовать этот сценарий, если требуется быстро сформировать списки правил контроля запуска программ. Запуск задачи Формирование правил контроля запуска программ по расписанию рекомендуется настраивать, только если область применения разрешающих правил включает папки, содержащие заведомо безопасные файлы.

  > Перед запуском задачи Контроль запуска программ в сети убедитесь, что для всех защищаемых компьютеров настроен доступ к папке общего доступа. Если применение папки общего доступа не предусмотрено политикой организации, рекомендуется запустить задачу Формирование правил контроля запуска программ на компьютере в тестовой группе компьютеров или на эталонной машине.

- На основе отчета о событиях в работе задачи Контроль запуска программ в режиме **Только статистика**, сформированного в Kaspersky Security Center.

  В рамках этого сценария Kaspersky Embedded Systems Security не блокирует запуск программ. Задача Контроль запуска программ работает в режиме **Только статистика** и регистрирует все разрешенные и запрещенные запуски программ на всех компьютерах сети на закладке **События** в рабочей области узла Сервера администрирования в Kaspersky Security Center. Kaspersky Security Center использует журнал выполнения задачи для формирования единого списка событий, включающего заблокированные запуски программ.

Нужно настроить период выполнения задачи так, чтобы за указанный промежуток времени выполнились все возможные сценарии работы защищаемых компьютеров и групп компьютеров и хотя бы одна перезагрузка. После добавления правил в задачу контроля запуска программ можно импортировать данные о запусках программ из сохраненного отчета о событиях Kaspersky Security Center (файла в формате TXT) и сформировать на основе этих данных разрешающие правила контроля запуска таких программ.

Рекомендуется использовать этот сценарий, если в сети организации имеется большое количество компьютеров разных типов с различным набором установленных программ.

- На основе событий блокировки запуска программ, полученных через Kaspersky Security Center, без создания и импорта конфигурационного файла.

  Чтобы воспользоваться данной возможностью, задача Контроль запуска программ на локальном компьютере должна находиться под управлением активной политики Kaspersky Security Center. Все события на локальном компьютере при этом передаются на Сервер администрирования.

Рекомендуется обновить список правил при изменении состава программ, установленных на компьютерах сети (например, при установке обновлений или переустановке операционной системы). Рекомендуется сформировать обновленный список правил, запустив задачу Формирование правил контроля запуска программ или задачу Контроль запуска программ в режиме **Только статистика** на компьютерах тестовой группы администрирования. Тестовая группа администрирования включает компьютеры, необходимые для тестового запуска новых программ перед их установкой на остальные компьютеры сети.

XML-файлы, содержащие списки разрешающих правил, создаются на основе анализа запускаемых задач на защищаемом компьютере. Чтобы при формировании списка правил учесть все используемые в сети программы, рекомендуется запускать задачи Формирование правил контроля запуска программ и Контроль запуска программ в режиме **Только статистика** на эталонной машине организации.

Перед формированием разрешающих правил на основе программ, запущенных на эталонной машине организации, убедитесь, что эталонная машина защищена и на ней нет вредоносных программ.

Перед добавлением разрешающих правил выберите один из доступных режимов применения правил. В списке правил политики Kaspersky Security Center отображаются только правила, заданные в этой политике, вне зависимости от режима применения правил. Список локальных правил включает все применимые правила: локальные и добавленные через политику.

Параметры по умолчанию для задачи Контроль запуска программ

По умолчанию задача Контроль запуска программ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 47. Параметры по умолчанию для задачи Контроль запуска программ

Параметр	Значение по умолчанию	Описание
Режим работы	**Только статистика**. Задача регистрирует события, соответствующие попыткам запуска программ, запрещенным или разрешенным на основе набора правил. Фактическая блокировка запуска программ не выполняется.	Вы можете выбрать режим **Активный** после того, как будет сформирован окончательный список правил.
Повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках	Применяется.	Можно повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках.
Запрещать запуск командных интерпретаторов без команды к исполнению	Не применяется.	Вы можете запрещать запуск командных интерпретаторов без исполняемых команд.
Правила	**Заменить правилами политики локальные правила**	Вы можете выбрать режим совместного применения правил, заданных в политике, и правил на локальном компьютере.
Область применения правил	Задача контролирует запуск исполняемых файлов, скриптов и MSI-пакетов. Кроме того, она контролирует загрузку DLL-модулей.	Вы можете указывать типы файлов, запуск которых будет контролироваться правилами.

Параметр	Значение по умолчанию	Описание
Использование KSN	Данные KSN о репутации программы не используются.	Вы можете использовать данные о репутации программ в KSN при работе задачи Контроль запуска программ.
Автоматически разрешать распространение с помощью указанных программ и пакетов установки	Не применяется.	Вы можете разрешать распространение программного обеспечения с помощью указанных в настройках пакетов установки и программ. По умолчанию распространение программ разрешено только с помощью служб установщика Windows.
Всегда разрешать распространение программ с помощью Windows Installer	Применяется. Можно изменить, только если включен параметр **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.	Вы можете разрешить установку или обновление любого программного обеспечения, если операции выполняются с помощью установщика Windows.
Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи	Не применяется. Можно изменить, только если включен параметр **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.	Можно включить или выключить автоматическое распространение программного обеспечения с помощью решения System Center Configuration Manager.
Параметры запуска задачи	Первый запуск не определен.	Задача Контроль запуска программ не запускается автоматически сразу после Kaspersky Embedded Systems Security. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

Таблица 48. Заданные по умолчанию параметры задачи Формирование правил контроля запуска программ

Параметр	Значение по умолчанию	Описание
Префикс для названий разрешающих правил	Совпадает с именем компьютера, на котором установлена программа Kaspersky Embedded Systems Security.	Вы можете изменить префикс для названий разрешающих правил.
Область применения разрешающих правил	Под область применения разрешающих правил по умолчанию подпадают следующие категории файлов: • файлы с расширением EXE, расположенные в папках C:\Windows, C:\Program Files (x86) и C:\Program Files; • пакеты MSI, расположенные в папке C:\Windows; • скрипты, расположенные в папке C:\Windows. Также задача создает правила для всех уже запущенных программ независимо от их расположения и формата.	Вы можете изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых будет разрешен автоматически сформированными правилами. Также при создании разрешающих правил вы можете не учитывать запущенные программы.
Критерии формирования разрешающих правил	Используется заголовок и отпечаток цифрового сертификата; правила формируются для всех пользователей и групп пользователей.	Вы можете использовать хеш SHA256 при формировании разрешающих правил. Вы можете выбрать пользователя и группу пользователей, для которых необходимо автоматически формировать разрешающие правила.
Действия по завершении задачи	Разрешающие правила добавляются в список правил контроля запуска программ; новые правила объединяются с существующими правилами; дублирующиеся правила удаляются.	Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующихся правил или заменять существующие правила новыми разрешающими правилами, а также настраивать параметры экспорта разрешающих правил в файл.

Параметр	Значение по умолчанию	Описание
Параметры запуска задачи с правами	Задача запускается с правами системной учетной записи.	Вы можете разрешить запуск задачи Формирование правил контроля запуска программ с правами системной учетной записи или с правами указанного пользователя.
Расписание запуска задачи	Первый запуск не определен.	Задача Формирование правил контроля запуска программ не запускается автоматически при запуске Kaspersky Embedded Systems Security. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

Управление контролем запуска программ с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для одного или всех компьютеров сети.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

В этом разделе

Переход к параметрам политики для задачи Контроль запуска программ

► *Чтобы перейти к параметрам задачи Контроль запуска программ в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую требуется настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.

   Откроется окно **Контроль запуска программ**.

Настройте политику в соответствии с вашими требованиями.

Переход к списку правил контроля запуска программ

► *Чтобы перейти к списку правил контроля запуска программ в Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую требуется настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.

   Откроется окно **Контроль запуска программ**.
7. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля запуска программ**.

Настройте список правил в соответствии с вашими требованиями.

Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам

► *Чтобы создать задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**.

   Откроется окно **Мастер создания задачи**.
5. Выберите задачу **Формирование правил контроля запуска программ**.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Настройка**.

► *Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Задачи**.
4. Выберите название задачи в списке задач Kaspersky Security Center двойным щелчком мыши.

   Откроется окно **Свойства: Формирование правил контроля запуска программ**.

Дополнительную информацию о настройке задачи см. в разделе Настройка задачи Формирование правил контроля запуска программ.

Настройка параметров задачи Контроль запуска программ

► *Чтобы настроить общие параметры задачи Контроль запуска программ, выполните следующие действия:*

1. Откройте окно **Контроль запуска программ** (см. раздел "**Переход к параметрам политики для задачи Контроль запуска программ**" на стр. 307).
2. На закладке **Общие** в блоке **Режим работы** настройте следующие параметры:
   - В раскрывающемся списке **Режим работы** выберите режим работы задачи.

     В раскрывающемся списке вы можете выбрать один из следующих режимов работы задачи Контроль запуска программ:

     - **Активный**. Kaspersky Embedded Systems Security использует определенные правила контроля запуска всех программ.
     - **Только статистика**. Kaspersky Embedded Systems Security не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы

можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о заблокированных запусках программ, зарегистрированной в журнале выполнения задачи.

По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.

- Снимите или установите флажок **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска**.

  Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше.

  Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки.

  Если флажок снят, Kaspersky Embedded Systems Security проверяет программу при каждой попытке ее запуска.

  По умолчанию флажок установлен.

- Снимите или установите флажок **Запрещать запуск командных интерпретаторов без команды к исполнению**.

  Если флажок установлен, Kaspersky Embedded Systems Security запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий:

  - Запуск командного интерпретатора разрешен.
  - Исполняемая команда разрешена.

  Если флажок снят, Kaspersky Embedded Systems Security учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее.

  Kaspersky Embedded Systems Security работает со следующими командными интерпретаторами:

  - cmd.exe;
  - powershell.exe;
  - python.exe;
  - perl.exe.

  По умолчанию флажок снят.

3. В блоке **Правила** настройте параметры применения правил:

   a. Нажмите на кнопку **Список правил**, чтобы добавить разрешающие правила в задачу Контроль запуска программ.

   > Kaspersky Embedded Systems Security не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.

b. Выберите режим применения правил:

- **Заменить правилами политики локальные правила**

  Программа применяет список правил, заданных в политике, для централизованного контроля запуска программ на группе компьютеров. Формирование, редактирование и применение локальных списков правил недоступно.

- **Добавить правила политики к локальным правилам**

  Программа применяет список правил, заданный в политике, совместно с локальными списками правил. Вы можете редактировать локальные списки правил с помощью задач автоматического формирования правил контроля запуска программ.

По умолчанию Kaspersky Embedded Systems Security применяет два стандартных правила, которые разрешают запуск скриптов, MSI-пакетов и исполняемых файлов, если эти объекты подписаны доверенной цифровой подписью.

4. В блоке **Область применения правил** укажите следующие параметры:

- **Использовать правила для исполняемых файлов**

  Флажок включает или выключает контроль запуска исполняемых файлов.

  Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

  Если флажок снят, Kaspersky Embedded Systems Security не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен.

  По умолчанию флажок установлен.

- **Контролировать загрузку DLL-модулей**

  Флажок включает или выключает контроль загрузки DLL-модулей.

  Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

  Если флажок снят, Kaspersky Embedded Systems Security не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена.

  Флажок доступен, если установлен флажок **Использовать правила для исполняемых файлов**.

  По умолчанию флажок снят.

Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Использовать правила для скриптов и пакетов MSI**

  Флажок включает или выключает запуск скриптов и пакетов MSI.

  Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает запуск скриптов и пакетов MSI с помощью заданных правил, в

параметрах которых указана область применения Скрипты и пакеты MSI.

Если флажок снят, Kaspersky Embedded Systems Security не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

По умолчанию флажок установлен.

5. В блоке параметров **Использование KSN** настройте следующие параметры запуска программ:

   - **Запрещать запуск программ, недоверенных в KSN**

     Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

     Если флажок установлен, Kaspersky Embedded Systems Security запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

     Если флажок снят, Kaspersky Embedded Systems Security не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

     По умолчанию флажок снят.

   - **Разрешать запуск программ, доверенных в KSN**

     Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

     Если флажок установлен, Kaspersky Embedded Systems Security разрешает запуск программ, доверенных в KSN. Запрещающие правила контроля запуска программ, под которые подпадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.

     Если флажок снят, Kaspersky Embedded Systems Security не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

     По умолчанию флажок снят.

   - Пользователи и / или группы пользователей, которым разрешен запуск доверенных в KSN программ.

6. На закладке **Контроль пакетов установки** настройте параметры контроля пакетов установки (см. раздел "Настройка контроля пакетов установки" на стр. 312).
7. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 130).
8. В окне **Параметры задачи** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

Настройка Контроля пакетов установки

► *Чтобы добавить доверенный пакет установки, выполните следующие действия:*

1. Откройте окно **Контроль запуска программ** (см. Раздел "Переход к параметрам политики для задачи Контроль запуска программ" на стр. 307).
2. На закладке **Контроль пакетов установки** установите флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью указанных в списке программ и пакетов установки.

   Если флажок установлен, программа автоматически разрешает запуск файлов с помощью доверенных пакетов установки. Список программ и пакетов установки, разрешенных к запуску, доступен для редактирования.

   Если флажок снят, программа не применяет указанные в списке исключения.

   По умолчанию флажок снят.

   Вы можете установить флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**, если на закладке **Общие** в параметрах задачи **Контроль запуска программ** установлен флажок **Использовать правила для исполняемых файлов**.

3. Если требуется, снимите флажок **Всегда разрешать распространение программ с помощью Windows Installer**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью установщика Windows.

   Если флажок установлен, всегда будет разрешен запуск файлов, установленных с помощью установщика Windows.

   Если флажок не установлен, файл нельзя будет запустить без выполнения условий контроля запуска программ, даже если файл запускается с помощью установщика Windows.

   По умолчанию флажок установлен.

   Флажок недоступен для редактирования, если снят флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

   Флажок **Всегда разрешать распространение программ с помощью Windows Installer** рекомендуется снимать только в случае крайней необходимости. Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

4. Если требуется, установите флажок **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи**.

   Флажок включает или выключает автоматическое разрешение распространения программного обеспечения с помощью решения System Center Configuration Manager.

   Если флажок установлен, Kaspersky Embedded Systems Security автоматически разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Программа разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service).

   Программа контролирует запуск объектов со следующими расширениями:

   - exe;
   - msi.

   По умолчанию флажок снят.

   Программа контролирует цикл распространения программного обеспечения на компьютере: от доставки пакета до установки или обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки программы на компьютер.

5. Чтобы отредактировать список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в открывшемся окне выберите один из следующих способов:

   - **Добавить один вручную**.

     a. Нажмите на кнопку **Обзор** и выберите исполняемый файл или пакет установки.

        Блок **Критерий доверенности** автоматически заполнится данными о выбранном файле.

     b. Снимите или установите флажок **Разрешать исполнение всей цепочке файлов, извлеченных из этого пакета установки**.

     c. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

        - **Использовать цифровой сертификат**
        - Использовать хеш SHA256

   - **Добавить несколько по хешу**

     Вы можете выбрать неограниченное число исполняемых файлов и пакетов установки и добавить их в список одновременно. Kaspersky Embedded Systems Security учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

   - **Изменить выбранный**

     Используйте этот вариант, чтобы выбрать другой исполняемый файл или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла**

  Вы можете импортировать список доверенных пакетов установки из конфигурационного файла. Для распознавания в Kaspersky Embedded Systems Security такой файл должен удовлетворять следующим параметрам:

  - иметь расширение TXT;
  - содержать информацию в виде списка строк, каждая из которых – данные для одного доверенного файла;
  - содержать список, соответствующий одному из двух форматов:
    - <имя файла>:<хеш SHA256>.
    - <хеш SHA256>*<имя файла>.

  В окне **Открыть** укажите конфигурационный файл со списком доверенных пакетов установки.

6. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск распакованных файлов будет разрешен.

   Чтобы запретить запуск извлеченных файлов, удалите программу с защищаемого компьютера или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Настройка задачи Формирование правил контроля запуска программ

► *Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам**" на стр. 308).
2. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*

3. В разделе **Настройка** вы можете настроить следующие параметры:
   - Укажите префикс для названий правил.
   - Настройте область применения разрешающих правил:
     - Создавать разрешающие правила на основе запущенных программ.
     - Создавать разрешающие правила для программ из определенных папок.
4. В разделе **Параметры** вы можете указать действия при формировании разрешающих правил контроля запуска программ:
   - **Использовать цифровой сертификат**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

Данный вариант выбран по умолчанию.

- **Использовать заголовок и отпечаток цифрового сертификата**

  Флажок включает или выключает использование заголовка и отпечатка цифрового сертификата файла в качестве критерия срабатывания разрешающих правил контроля запуска программ. Включение этого флажка позволяет задать более строгие условия проверки цифрового сертификата.

  Если флажок установлен, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливаются значения заголовка и отпечатка цифрового сертификата файлов, для которых формируются правила. Kaspersky Embedded Systems Security разрешит запуск программ, которые запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

  Использование этого флажка строго ограничивает срабатывание разрешающих правил запуска программ по цифровому сертификату, так как отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан.

  Если флажок снят, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

  Флажок доступен, если выбран вариант **Использовать цифровой сертификат**.

  По умолчанию флажок установлен.

- **Если сертификат отсутствует, использовать**

  Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

  - **хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.
  - **путь к файлу** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице **Создавать разрешающие правила для программ из папок** в разделе **Настройка**.

- **Использовать хеш SHA256**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

По умолчанию этот вариант не выбран.

- **Формировать правила для пользователя или группы пользователей**

  Поле, в котором отображается пользователь или группа пользователей. Программа будет контролировать запуски программ указанным пользователем или группой.

  По умолчанию выбрана группа **Все**.

Вы можете настроить параметры для конфигурационных файлов со списком сформированных разрешающих правил контроля устройств и контроля запуска программ, которые Kaspersky Embedded Systems Security создает по завершении задач.

1. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз программы).
2. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.
3. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*

4. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

Настройка правил контроля запуска программ в Kaspersky Security Center

В этом разделе описано формирование списка правил на основе различных критериев, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль запуска программ.

В этом разделе

Добавление правила контроля запуска программ

► *Чтобы добавить правило контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "Переход к списку правил контроля запуска программ" на стр. 307).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
4. Укажите следующие параметры:
   a. В поле **Название** введите название правила.
   b. В раскрывающемся списке **Тип** выберите тип правила:
      - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск программ в соответствии с критериями, указанными в параметрах правила.
      - **Запрещающее**, если вы хотите, чтобы правило блокировало запуск программ в соответствии с критериями, указанными в параметрах правила.
   c. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
      - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов.
      - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
   d. В поле **Пользователь или группа пользователей** укажите пользователей, которым будет разрешено или запрещено запускать программы в соответствии с типом правила. Для этого выполните следующие действия:
      i. Нажмите на кнопку **Выбрать**.
      ii. Откроется стандартное окно Microsoft Windows **Выбор пользователя или групп**.
      iii. Задайте список пользователей и / или групп пользователей.
      iv. Нажмите на кнопку **OK**.
   e. Чтобы использовать значения критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла, выполните следующие действия:
      i. Нажмите на кнопку **Задать критерий срабатывания правила из свойств файла**.

         Откроется стандартное окно Microsoft Windows **Открыть**.
      ii. Выберите файл.
      iii. Нажмите на кнопку **Открыть**.

         Значения критериев из файла отобразятся в полях блока **Критерий срабатывания правила**. По умолчанию будет выбран первый в списке критерий, данные для которого присутствуют в свойствах файла.
   f. В блоке **Критерий срабатывания правила** выберите один из следующих вариантов:
      - **Цифровой сертификат**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, подписанных цифровым сертификатом:

- Установите флажок **Использовать заголовок**, если вы хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
- Установите флажок **Использовать отпечаток**, если вы хотите, чтобы правило контролировало только запуск файлов, подписанных цифровым сертификатом с указанным отпечатком.

- **Хеш SHA256**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, контрольная сумма которых соответствует указанной.
- **Путь к файлу**, если требуется, чтобы правило контролировало запуск программ, запускаемых с помощью файлов, расположенных по указанному пути.

  Kaspersky Embedded Systems Security не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.

g. Если вы хотите добавить исключения из правила, выполните следующие действия:

   i. В блоке **Исключения из правила** нажмите на кнопку **Добавить**.

      Откроется окно **Исключение из правила**.

   ii. В поле **Название** введите название исключения.

   iii. Укажите параметры исключения файлов программ из правила контроля запуска программ. Вы можете заполнить поля параметров из свойств файла по кнопке **Задать исключение на основе свойств файла**.

      - **Цифровой сертификат**

        Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

        Данный вариант выбран по умолчанию.

      - **Использовать заголовок**

        Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

        Если флажок установлен, заголовок указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

        Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

        Заголовок цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над разделом **Критерий срабатывания правила**.

По умолчанию флажок снят.

- **Использовать отпечаток**

  Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, отпечаток указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

  Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

  Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над разделом **Критерий срабатывания правила**.

  По умолчанию флажок снят.

- **Хеш SHA256**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

  Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

  По умолчанию этот вариант не выбран.

- **Путь к файлу**

  Если флажок установлен, Kaspersky Embedded Systems Security использует полный путь к файлу для определения, является ли процесс доверенным.

  Если флажок не установлен, путь к файлу не будет учитываться при определении доверенности процесса.

  По умолчанию флажок снят.

iv. Нажмите на кнопку **OK**.

v. Повторите пункты (i)-(iv) для добавления дополнительных исключений.

5. В окне **Параметры правила** нажмите на кнопку **OK**.

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

Включение режима разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и

не являются недоверенными согласно заключению KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить разрешение по умолчанию только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило разрешения по умолчанию, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 307).
2. Нажмите на кнопку **Добавить** и в открывшемся контекстном меню выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
3. В поле **Название** введите название правила.
4. В раскрывающемся списке **Тип** выберите элемент **Разрешающее**.
5. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов;
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
6. В блоке **Критерий срабатывания правила** выберите вариант **Путь к файлу**.
7. Введите следующую маску: `?:\`
8. В окне **Параметры правила** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security применяет режим разрешения по умолчанию.

Создание разрешающих правил на основе событий Kaspersky Security Center

► *Чтобы сформировать разрешающие правила контроля запуска программ для программ из событий Kaspersky Security Center, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "**Переход к списку правил контроля запуска программ**" на стр. 307).
2. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Создать разрешающие правила программ из событий Kaspersky Security Center**.
3. Выберите принцип добавления правил к списку уже созданных правил контроля запуска программ:
   - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется окно **Создать правила контроля запуска программ**.

4. Настройте следующие параметры запроса:
   - **Адрес Сервера администрирования**
   - **Порт**
   - **Пользователь**
   - **Пароль**
5. Выберите типы событий, которые должны стать основой для задачи формирования правил:
   - **Только статистика: запуск программы запрещен**.
   - **Запуск программы запрещен**.
6. Выберите период из раскрывающегося списка **Учитывать события, сформированные в течение периода**.
7. Нажмите на кнопку **Создать правила**.
8. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

   Список правил в задаче Контроль запуска программ будет дополнен новыми правилами, сформированными на основе системных данных компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

   Если список правил контроля запуска программ уже задан в политике, Kaspersky Embedded Systems Security добавит выбранные правила из событий блокирования к уже заданным правилам. Правила с повторяющимся хешем не добавляются, поскольку все правила в списке должны быть уникальными.

Импорт правил из отчета Kaspersky Security Center о заблокированных программах

Вы можете импортировать данные о заблокированных запусках программ из отчета, сформированного в Kaspersky Security Center по результатам выполнения задачи Контроль запуска программ в режиме **Только статистика**, и применить эти данные для формирования списка разрешающих правил запуска программ в настраиваемой политике.

При формировании отчета о событиях, возникающих в ходе выполнения задачи Контроль запуска программ, вы можете отслеживать программы, запуск которых был заблокирован.

При импорте из отчета данных о заблокированных программах в свойства политики убедитесь, что применяемый список содержит только те программы, запуск которых вы хотите разрешить.

► *Чтобы задать разрешающие правила контроля запуска программ для группы компьютеров на основе отчета о заблокированных программах из Kaspersky Security Center, выполните следующие действия:*

1. Откройте окно **Контроль запуска программ** (см. раздел "Переход к параметрам политики для задачи Контроль запуска программ" на стр. 307).
2. В блоке **Режим работы** выберите режим **Только статистика**.

3. В свойствах политики в разделе **Уведомления о событиях** убедитесь, что:

   - Для событий с уровнем важности **Критический** срок хранения событий **Запуск программы запрещен** в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).
   - Для событий с уровнем важности **Предупреждение** срок хранения событий **Только статистика: запуск программы запрещен** в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

   По истечении срока хранения событий информация о зарегистрированных событиях будет удалена и не попадет в файл отчета. Перед запуском задачи Контроль запуска программ в режиме **Только статистика** убедитесь, что время выполнения задачи не превышает установленный срок хранения указанных событий.

4. По завершении задачи выполните экспорт зарегистрированных событий в файл формата TXT:

   a. В Kaspersky Security Center в рабочей области узла **Сервер администрирования** выберите закладку **События**.

   b. Нажмите на кнопку **Создать выборку**, чтобы создать выборку событий по критерию *Запрещен* и просмотреть, запуск каких программ будет заблокирован задачей Контроль запуска программ.

   c. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных запусках программ в файл формата TXT.

   Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех программах, запуск которых требуется разрешить.

5. Импортируйте данные о заблокированных запусках программ в задачу контроля запуска программ. Для этого в свойствах политики в параметрах задачи Контроль запуска программ выполните следующие действия:

   a. На закладке **Общие** нажмите на кнопку **Список правил**.

      Откроется окно **Правила контроля запуска программ**.

   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать данные о заблокированных программах из отчета Kaspersky Security Center**.

   c. Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку настроенных ранее правил контроля запуска программ:

      - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
      - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
      - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

d. В открывшемся стандартном окне Microsoft Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных запусках программ.

e. Нажмите на кнопку **ОК** в окне Правила контроля запуска программ и в окне **Параметры задачи**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных программах, будут добавлены к списку правил контроля запуска программ.

Импорт правил контроля запуска программ из XML-файла

Вы можете импортировать отчеты, сформированные по результатам выполнения групповой задачи Формирование правил контроля запуска программ, и применить их в качестве списка разрешающих правил в настраиваемой политике.

По завершении групповой задачи формирования правил контроля запуска программ выполняется экспорт созданных разрешающих правил в XML-файлы в указанную папку общего доступа. Каждый файл со списком правил создается на основе анализа исполняемых файлов и запущенных программ на каждом отдельном компьютере в сети организации. Списки содержат разрешающие правила для файлов и программ, тип которых соответствует параметрам, указанным в групповой задаче формирования правил контроля запуска программ.

► *Чтобы задать разрешающие правила контроля запуска программ для группы компьютеров на основе автоматически сформированного списка разрешающих правил, выполните следующие действия:*

1. На закладке **Задачи** панели результатов настраиваемой группы компьютеров создайте групповую задачу Формирование правил контроля запуска программ или выберите существующую задачу (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. 308).
2. В свойствах созданной групповой задачи Формирование правил контроля запуска программ или в мастере создания задачи настройте следующие параметры:
   - В разделе **Уведомление** настройте параметры сохранения отчета выполнения задачи.

     Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*

   - В разделе **Настройка** укажите типы программ, запуск которых будет разрешен созданными правилами. Можно изменить набор папок, содержащих разрешенные для запуска программы: исключать из области действия задачи папки, указанные по умолчанию, и добавлять новые папки вручную.
   - В блоке **Параметры** укажите действия, выполняемые задачей во время работы и после завершения. Укажите критерий формирования правил и имя файла, в который будут экспортированы эти правила.
   - В блоке **Расписание** настройте параметры запуска задачи по расписанию.
   - В разделе **Учетная запись** укажите учетную запись пользователя, с правами которой будет выполняться задача.
   - В блоке **Исключения из области действия задачи** укажите группы компьютеров, которые требуется исключить из области действия задачи.

Kaspersky Embedded Systems Security не создает разрешающие правила для программ, запускаемых на исключенных компьютерах.

3. На закладке **Задачи** панели управления настраиваемой группы компьютеров в списке групповых задач выберите созданную задачу Формирование правил контроля запуска программ и нажмите на кнопку **Запустить** для запуска задачи.

   После завершения задачи, автоматически сформированные списки разрешающих правил будут сохранены в XML-файлы в папке общего доступа.

   Перед запуском задачи Контроль запуска программ в сети убедитесь, что для всех защищаемых компьютеров настроен доступ к папке общего доступа. Если применение папки общего доступа не предусмотрено политикой организации, рекомендуется запустить задачу Формирование правил контроля запуска программ на компьютере в тестовой группе компьютеров или на эталонной машине.

4. Чтобы добавить сформированные списки разрешающих правил в задачу Контроль запуска программ, выполните следующие действия:

   a. Откройте окно **Правила контроля запуска программ** (см. раздел "Переход к списку правил контроля запуска программ" на стр. 307).

   b. Нажмите на кнопку **Добавить** и в открывшемся списке выберите пункт **Импортировать правила из файла формата XML**.

   c. Выберите принцип добавления автоматически сформированных разрешающих правил к списку уже заданных правил контроля запуска программ:

      - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
      - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
      - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   d. В открывшемся стандартном окне Microsoft Windows выберите XML-файлы, созданные по завершении групповой задачи Формирование правил контроля запуска программ.

   e. Нажмите на кнопку **ОК** в окне **Правила контроля запуска программ** и в окне **Параметры задачи**.

5. Если вы хотите применять созданные правила для контроля запуска программ, в политике в свойствах задачи Контроль запуска программ выберите режим **Активный**.

Разрешающие правила, автоматически сформированные на основе запусков задач на каждом отдельном компьютере, будут применены для всех компьютеров в сети под управлением настраиваемой политики. Для этих компьютеров программа разрешит запуск только тех программ, для которых созданы разрешающие правила.

Проверка запуска программ

Перед применением заданных правил контроля запуска программ вы можете проверить любую программу, чтобы определить, какие правила контроля запуска программ срабатывают для выбранной программы.

По умолчанию Kaspersky Embedded Systems Security блокирует программы, запуск которых не разрешен хотя бы одним правилом. Чтобы избежать блокировки запуска важных программ, необходимо создать для них разрешающие правила.

Если запуск программы контролируется несколькими правилами разных типов, запрещающие правила имеют больший приоритет: запуск программы блокируется, если она подпадает под действие хотя бы одного запрещающего правила.

► *Чтобы проверить правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ** (см. раздел "Переход к списку правил контроля запуска программ" на стр. 307).
2. В открывшемся окне нажмите на кнопку **Показать правила для файла**.

   Откроется стандартное окно Microsoft Windows.
3. Выберите файл, контроль запуска которого хотите протестировать.

В строке поиска отобразится путь к указанному файлу. В списке правил отобразятся все правила, которые сработают при запуске указанного файла.

Создание задачи Формирование правил контроля запуска программ

► *Чтобы создать задачу Формирование правил контроля запуска программ и настроить ее параметры, выполните следующие действия:*

1. Откройте окно **Параметры** в мастере создания задачи (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. 308).
2. Настройте следующие параметры:
   - Укажите **Префикс для названий правил**.

     Это первая часть названия правила. Вторая часть названия правила формируется из названия объекта, запуск которого разрешен.

     По умолчанию в качестве префикса указано имя компьютера, на котором установлена программа Kaspersky Embedded Systems Security. Вы можете изменить префикс для названий разрешающих правил.
   - Настройте область применения разрешающих правил (см. раздел "Ограничение области действия задачи" на стр. 345).
3. Нажмите на кнопку **Далее**.

4. Укажите действия, которые должна выполнять программа Kaspersky Embedded Systems Security:
   - при формировании разрешающих правил (см. раздел "Действия при автоматическом формировании правил" на стр. 346);
   - по завершении задачи (см. раздел "Действия по завершении автоматического формирования правил" на стр. 348).
5. В окне **Расписание** укажите параметры запуска задачи по расписанию.
6. Нажмите на кнопку **Далее**.
7. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
8. Нажмите на кнопку **Далее**.
9. Укажите название задачи.
10. Нажмите на кнопку **Далее**.

    Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы:
    " * < > & \ : |

    Откроется окно **Завершение создания задачи**.
11. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
12. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.

► *Чтобы настроить существующее правило в Kaspersky Security Center,*

откройте окно **Свойства: Формирование правил контроля запуска программ** и настройте параметры, как описано выше.

Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

В этом разделе

Ограничение области действия задачи

► *Чтобы ограничить область действия задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. 308).
2. Настройте следующие параметры задачи:
   - **Создавать разрешающие правила на основе запущенных программ**

     Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на компьютере имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.

     Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

     Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

     По умолчанию флажок установлен.

     Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.
   - **Создавать разрешающие правила для программ из папок**

     В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.
3. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Действия при автоматическом формировании правил

► *Чтобы настроить действия Kaspersky Embedded Systems Security во время выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам**" на стр. 308).
2. Выберите закладку **Параметры**.
3. В блоке **При формировании разрешающих правил** настройте следующие параметры:
   - **Использовать цифровой сертификат**

     Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у

которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

Данный вариант выбран по умолчанию.

- **Использовать заголовок и отпечаток цифрового сертификата**

  Флажок включает или выключает использование заголовка и отпечатка цифрового сертификата файла в качестве критерия срабатывания разрешающих правил контроля запуска программ. Включение этого флажка позволяет задать более строгие условия проверки цифрового сертификата.

  Если флажок установлен, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливаются значения заголовка и отпечатка цифрового сертификата файлов, для которых формируются правила. Kaspersky Embedded Systems Security разрешит запуск программ, которые запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

  Использование этого флажка строго ограничивает срабатывание разрешающих правил запуска программ по цифровому сертификату, так как отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан.

  Если флажок снят, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

  Флажок доступен, если выбран вариант **Использовать цифровой сертификат**.

  По умолчанию флажок установлен.

- **Если сертификат отсутствует, использовать**

  Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

  - **хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.
  - **путь к файлу** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице **Создавать разрешающие правила для программ из папок** в разделе **Настройка**.

- **Использовать хеш SHA256**

Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

По умолчанию этот вариант не выбран.

- **Формировать правила для пользователя или группы пользователей**

  Поле, в котором отображается пользователь или группа пользователей. Программа будет контролировать запуски программ указанным пользователем или группой.

  По умолчанию выбрана группа **Все**.

1. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Действия по завершении автоматического формирования правил

► *Чтобы настроить действия Kaspersky Embedded Systems Security по завершении выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля запуска программ** (см. раздел "Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам" на стр. 308).
2. Выберите закладку **Параметры**.
3. В блоке **По завершении задачи** настройте следующие параметры:

   - **Добавлять разрешающие правила в список правил контроля запуска программ**

     Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля запуска программ. Список правил контроля запуска программ отображается при переходе по ссылке **Правила контроля запуска программ** в панели результатов узла Контроль запуска программ.

     Если флажок установлен, Kaspersky Embedded Systems Security добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля запуска программ, в список правил контроля запуска программ согласно выбранному принципу добавления правил.

     Если флажок снят, Kaspersky Embedded Systems Security не добавляет новые сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

     По умолчанию флажок установлен.

- **Принцип добавления**

  Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

  - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Заменять существующие правила**. Правила добавляются в список вместо существующих правил.
  - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

  По умолчанию выбран способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**
- **Добавлять информацию о компьютере в имя файла**

  Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются разрешающие правила.

  Если флажок установлен, программа добавляет имя защищаемого компьютера, а также дату и время формирования файла в имя файла экспорта.

  Если флажок снят, программа не добавляет информацию о защищаемом компьютере в имя файла экспорта.

  По умолчанию флажок установлен.

4. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Управление контролем запуска программ с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи для локального компьютера.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

В этом разделе

Переход к параметрам задачи Контроль запуска программ

► *Чтобы перейти к общим параметрам задачи Контроль запуска программ в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

Переход к окну с правилами контроля запуска программ

► *Чтобы перейти к списку правил контроля запуска программ в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Настройте список правил в соответствии с вашими требованиями.

Переход к параметрам задачи Формирование правил контроля запуска программ

► *Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Настройте задачу в соответствии с вашими требованиями.

Настройка параметров задачи Контроль запуска программ

► *Чтобы настроить общие параметры задачи Контроль запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. Раздел "Переход к параметрам задачи Контроль запуска программ" на стр. 331).
2. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - Режим работы задачи Контроль запуска программ (см. раздел "Выбор режима работы задачи Контроль запуска программ" на стр. 332).
     - Область применения правил в задаче (см. раздел "Настройка области применения задачи Контроль запуска программ" на стр. 334).
     - Использование KSN (см. раздел "Настройка использования KSN" на стр. 335).
   - Параметры контроля пакетов установки (см. раздел "Контроль пакетов установки" на стр. 336) на закладке **Контроль пакетов установки**.
   - Расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. 151) на закладках **Расписание** и **Дополнительно**.
3. В окне **Параметры задачи** нажмите на кнопку **OK**.

   Изменения параметров задачи будут сохранены.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

В этом разделе

Выбор режима работы задачи Контроль запуска программ

► *Чтобы настроить режим работы задачи Контроль запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. Раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 331).

2. На закладке **Общие** в раскрывающемся списке **Режим работы** выберите режим работы задачи.

   В раскрывающемся списке можно выбрать режим работы задачи Контроль запуска программ:

   - **Активный**. Kaspersky Embedded Systems Security контролирует все запускаемые программы с помощью заданных правил.
   - **Только статистика**. Kaspersky Embedded Systems Security не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о блокировках, зарегистрированной в журнале выполнения задачи.

   По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.

3. Снимите или установите флажок **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска**.

   Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше.

   Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки.

   Если флажок снят, Kaspersky Embedded Systems Security проверяет программу при каждой попытке ее запуска.

   По умолчанию флажок установлен.

   Kaspersky Embedded Systems Security заводит новый список событий в кеше при каждом изменении параметров задачи Контроль запуска программ. Таким образом, контроль запуска программ осуществляется в соответствии с актуальными параметрами безопасности.

4. Снимите или установите флажок **Запрещать запуск командных интерпретаторов без команды к исполнению**.

   Если флажок установлен, Kaspersky Embedded Systems Security запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий:

   - Запуск командного интерпретатора разрешен.
   - Исполняемая команда разрешена.

   Если флажок снят, Kaspersky Embedded Systems Security учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее.

Kaspersky Embedded Systems Security работает со следующими командными интерпретаторами:

- cmd.exe;
- powershell.exe;
- python.exe;
- perl.exe.

По умолчанию флажок снят.

5. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Все попытки запуска программ фиксируются в журнале выполнения задач.

Настройка области действия задачи Контроль запуска программ

► *Чтобы задать область действия задачи Контроль запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. Раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 331).
2. На закладке **Общие** в блоке **Область применения правил** задайте следующие параметры:
   - **Использовать правила для исполняемых файлов**

     Флажок включает или выключает контроль запуска исполняемых файлов.

     Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

     Если флажок снят, Kaspersky Embedded Systems Security не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен.

     По умолчанию флажок установлен.

   - **Контролировать загрузку DLL-модулей**

     Флажок включает или выключает контроль загрузки DLL-модулей.

     Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**.

     Если флажок снят, Kaspersky Embedded Systems Security не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена.

     Флажок доступен, если установлен флажок **Использовать правила для исполняемых файлов**.

     По умолчанию флажок снят.

Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Использовать правила для скриптов и пакетов MSI**

  Флажок включает или выключает запуск скриптов и пакетов MSI.

  Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает запуск скриптов и пакетов MSI с помощью заданных правил, в параметрах которых указана область применения Скрипты и пакеты MSI.

  Если флажок снят, Kaspersky Embedded Systems Security не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

  По умолчанию флажок установлен.

3. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Настройка использования KSN

► *Чтобы настроить использование служб KSN в задаче Контроль запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. Раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 331).
2. На закладке **Общие** в блоке **Использование KSN** укажите параметры использования служб KSN:
   - Если требуется, установите флажок **Запрещать запуск программ, недоверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

     Если флажок установлен, Kaspersky Embedded Systems Security запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

     Если флажок снят, Kaspersky Embedded Systems Security не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

     По умолчанию флажок снят.

   - Если требуется, установите флажок **Разрешать запуск программ, доверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

     Если флажок установлен, Kaspersky Embedded Systems Security разрешает запуск программ, доверенных в KSN. Запрещающие правила контроля запуска программ, под которые подпадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.

Если флажок снят, Kaspersky Embedded Systems Security не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам.

По умолчанию флажок снят.

- Если установлен флажок **Разрешать запуск программ, доверенных в KSN**, укажите пользователей и группы пользователей, которым разрешен запуск доверенных в KSN программ. Для этого выполните следующие действия:

  a. Нажмите на кнопку **Изменить**.

  Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

  b. Задайте список пользователей и / или групп пользователей.

  c. Нажмите на кнопку **OK**.

3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Формирование списка доверенных пакетов установки

► *Чтобы добавить доверенный пакет установки, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. Раздел "**Переход к параметрам задачи Контроль запуска программ**" на стр. 331).
2. На закладке **Контроль пакетов установки** установите флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью указанных в списке программ и пакетов установки.

   Если флажок установлен, программа автоматически разрешает запуск файлов с помощью доверенных пакетов установки. Список программ и пакетов установки, разрешенных к запуску, доступен для редактирования.

   Если флажок снят, программа не применяет указанные в списке исключения.

   По умолчанию флажок снят.

   Вы можете установить флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**, если на закладке **Общие** в параметрах задачи **Контроль запуска программ** установлен флажок **Использовать правила для исполняемых файлов**.

3. Если требуется, снимите флажок **Всегда разрешать распространение программ с помощью Windows Installer**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью установщика Windows.

   Если флажок установлен, всегда будет разрешен запуск файлов, установленных с помощью установщика Windows.

Если флажок не установлен, файл нельзя будет запустить без выполнения условий контроля запуска программ, даже если файл запускается с помощью установщика Windows.

По умолчанию флажок установлен.

Флажок недоступен для редактирования, если снят флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

Флажок **Всегда разрешать распространение программ с помощью Windows Installer** рекомендуется снимать только в случае крайней необходимости. Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

4. Если требуется, установите флажок **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи**.

   Флажок включает или выключает автоматическое разрешение распространения программного обеспечения с помощью решения System Center Configuration Manager.

   Если флажок установлен, Kaspersky Embedded Systems Security автоматически разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Программа разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service).

   Программа контролирует запуск объектов со следующими расширениями:

   - exe;
   - msi.

   По умолчанию флажок снят.

   Программа контролирует цикл распространения программного обеспечения на компьютере: от доставки пакета до установки или обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки программы на компьютер.

5. Чтобы отредактировать список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в открывшемся окне выберите один из следующих способов:

   - **Добавить один вручную**.

     a. Нажмите на кнопку **Обзор** и выберите исполняемый файл или пакет установки.

        Блок **Критерий доверенности** автоматически заполнится данными о выбранном файле.

     b. Снимите или установите флажок **Разрешать исполнение всей цепочке файлов, извлеченных из этого пакета установки**.

     c. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

        - **Использовать цифровой сертификат**
        - Использовать хеш SHA256

- **Добавить несколько по хешу**

  Вы можете выбрать неограниченное число исполняемых файлов и пакетов установки и добавить их в список одновременно. Kaspersky Embedded Systems Security учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

- **Изменить выбранный**

  Используйте этот вариант, чтобы выбрать другой исполняемый файл или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла**

  Вы можете импортировать список доверенных пакетов установки из конфигурационного файла. Для распознавания в Kaspersky Embedded Systems Security такой файл должен удовлетворять следующим параметрам:

  - иметь расширение TXT;
  - содержать информацию в виде списка строк, каждая из которых – данные для одного доверенного файла;
  - содержать список, соответствующий одному из двух форматов:
    - <имя файла>:<хеш SHA256>.
    - <хеш SHA256>*<имя файла>.

  В окне **Открыть** укажите конфигурационный файл со списком доверенных пакетов установки.

6. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск распакованных файлов будет разрешен.

   Чтобы запретить запуск извлеченных файлов, удалите программу с защищаемого компьютера или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Настройка правил контроля запуска программ

В этом разделе описано формирование, импорт и экспорт списка правил, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль запуска программ.

В этом разделе

Добавление правила контроля запуска программ

► *Чтобы добавить правило контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
4. Укажите следующие параметры:
   a. В поле **Название** введите название правила.
   b. В раскрывающемся списке **Тип** выберите тип правила:
      - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск программ в соответствии с критериями, указанными в параметрах правила.
      - **Запрещающее**, если вы хотите, чтобы правило блокировало запуск программ в соответствии с критериями, указанными в параметрах правила.
   c. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
      - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов.
      - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
   d. В поле **Пользователь или группа пользователей** укажите пользователей, которым будет разрешено или запрещено запускать программы в соответствии с типом правила. Для этого выполните следующие действия:
      i. Нажмите на кнопку **Выбрать**.
      ii. Откроется стандартное окно Microsoft Windows **Выбор пользователя или групп**.
      iii. Задайте список пользователей и / или групп пользователей.
      iv. Нажмите на кнопку **OK**.
   e. Чтобы использовать значения критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла, выполните следующие действия:

i. Нажмите на кнопку **Задать критерий срабатывания правила из свойств файла**.

Откроется стандартное окно Microsoft Windows **Открыть**.

ii. Выберите файл.

iii. Нажмите на кнопку **Открыть**.

Значения критериев из файла отобразятся в полях блока **Критерий срабатывания правила**. По умолчанию будет выбран первый в списке критерий, данные для которого присутствуют в свойствах файла.

f. В блоке **Критерий срабатывания правила** выберите один из следующих вариантов:

- **Цифровой сертификат**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, подписанных цифровым сертификатом:
  - Установите флажок **Использовать заголовок**, если вы хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
  - Установите флажок **Использовать отпечаток**, если вы хотите, чтобы правило контролировало только запуск файлов, подписанных цифровым сертификатом с указанным отпечатком.
- **Хеш SHA256**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, контрольная сумма которых соответствует указанной.
- **Путь к файлу**, если требуется, чтобы правило контролировало запуск программ, запускаемых с помощью файлов, расположенных по указанному пути.

> Kaspersky Embedded Systems Security не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.

g. Если вы хотите добавить исключения из правила, выполните следующие действия:

i. В блоке **Исключения из правила** нажмите на кнопку **Добавить**.

Откроется окно **Исключение из правила**.

ii. В поле **Название** введите название исключения.

iii. Укажите параметры исключения файлов программ из правила контроля запуска программ. Вы можете заполнить поля параметров из свойств файла по кнопке **Задать исключение на основе свойств файла**.

- **Цифровой сертификат**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

  Данный вариант выбран по умолчанию.

- **Использовать заголовок**

  Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

Если флажок установлен, заголовок указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

Заголовок цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над разделом **Критерий срабатывания правила**.

По умолчанию флажок снят.

- **Использовать отпечаток**

  Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, отпечаток указанного цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

  Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, программа будет контролировать запуск программ, подписанных цифровым сертификатом с любым отпечатком.

  Отпечаток цифрового сертификата, которым подписан файл, можно указать только в свойствах выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над разделом **Критерий срабатывания правила**.

  По умолчанию флажок снят.

- **Хеш SHA256**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

  Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

  По умолчанию этот вариант не выбран.

- **Путь к файлу**

  Если флажок установлен, Kaspersky Embedded Systems Security использует полный путь к файлу для определения, является ли процесс доверенным.

Если флажок не установлен, путь к файлу не будет учитываться при определении доверенности процесса.

По умолчанию флажок снят.

iv. Нажмите на кнопку **OK**.

v. Повторите пункты (i)-(iv) для добавления дополнительных исключений.

5. В окне **Параметры правила** нажмите на кнопку **OK**.

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

Включение режима разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и не являются недоверенными согласно заключению KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить разрешение по умолчанию только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило разрешения по умолчанию, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
4. В поле **Название** введите название правила.
5. В раскрывающемся списке **Тип** выберите элемент **Разрешающее**.
6. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов;
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
7. В блоке **Критерий срабатывания правила** выберите вариант **Путь к файлу**.
8. Введите следующую маску: `?:\`
9. В окне **Параметры правила** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security применяет режим разрешения по умолчанию.

Формирование разрешающих правил по событиям задачи Контроль запуска программ

► *Чтобы создать конфигурационный файл с разрешающими правилами, сформированный по событиям задачи Контроль запуска программ, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме **Только статистика** (см. раздел "Выбор режима работы задачи Контроль запуска программ" на стр. 332), чтобы регистрировать в журнале выполнения задачи информацию обо всех запусках программ на защищаемом компьютере.

2. По завершении выполнения задачи в режиме **Только статистика** откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в блоке **Управление** панели результатов узла **Контроль запуска программ**.
3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Embedded Systems Security создаст конфигурационный файл в формате XML со списком правил, сформированных на основе событий задачи Контроль запуска программ, отработавшей в режиме **Только статистика**. Вы можете применить этот список правил (см. раздел "Импорт правил контроля запуска программ из XML-файла" на стр. 343) в задаче Контроль запуска программ.

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть и обработать вручную список правил, чтобы убедиться, что запуск важных файлов (например, файлов операционной системы) разрешен заданными правилами.

Все события задачи фиксируются в журнале выполнения задачи, независимо от режима работы задачи. Вы можете создать конфигурационный файл со списком правил на основе журнала, сформированного во время выполнения задачи в режиме **Активный**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, поскольку финальный список правил должен быть сформирован перед запуском задачи в режиме **Активный**, чтобы правила работали эффективно.

Экспорт правил контроля запуска программ

► *Чтобы экспортировать правила контроля запуска программ в конфигурационный файл, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.
3. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, при экспорте правил его содержимое будет перезаписано.
4. Нажмите на кнопку **Сохранить**.

Параметры правил будут экспортированы в указанный файл.

Импорт правил контроля запуска программ из XML-файла

► *Чтобы импортировать правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Импортировать правила из файла формата XML**.

4. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла формата XML**:
   - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется стандартное окно Microsoft Windows **Открыть**.
5. В окне **Открыть** выберите XML-файл, содержащий правила контроля запуска программ.
6. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля запуска программ**.

Удаление правил контроля запуска программ

► *Чтобы удалить правила контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Правила контроля запуска программ**.
2. В списке выберите правила, которые требуется удалить.
3. Нажмите на кнопку **Удалить выбранные**.
4. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля запуска программ будут удалены.

Настройка задачи Формирование правил контроля запуска программ

► *Чтобы настроить параметры задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 331) для задачи Формирование правил контроля запуска программ.
2. Настройте следующие параметры:
   - На закладке **Общие**:
     - Укажите **Префикс для названий правил**.

       Это первая часть названия правила. Вторая часть названия правила формируется из названия объекта, запуск которого разрешен.

       По умолчанию в качестве префикса указано имя компьютера, на котором установлена программа Kaspersky Embedded Systems Security. Вы можете изменить префикс для названий разрешающих правил.

- Настройте область применения разрешающих правил (см. раздел "Ограничение области действия задачи" на стр. 345).

- На закладке **Действия** укажите действия, которые должна выполнять программа Kaspersky Embedded Systems Security:
  - при формировании разрешающих правил (см. раздел "Действия при автоматическом формировании правил" на стр. 346);
  - по завершении задачи (см. раздел "Действия по завершении автоматического формирования правил" на стр. 348).
- На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. 151).
- На закладке **Запуск с правами** настройте запуск задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 154).

3. Нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после их изменения.

В этом разделе

Ограничение области действия задачи

► *Чтобы ограничить область действия задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 331) для задачи Формирование правил контроля запуска программ.
2. Настройте следующие параметры задачи:
   - **Создавать разрешающие правила на основе запущенных программ**

     Флажок включает или выключает формирование правил контроля запуска программ для уже запущенных программ. Рекомендуется использовать этот вариант, если на компьютере имеется эталонный набор программ, на основе которого вы хотите сформировать разрешающие правила.

     Если флажок установлен, разрешающие правила контроля запуска программ формируются на основе запущенных программ.

     Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

     По умолчанию флажок установлен.

Флажок нельзя снять, если в таблице **Создавать разрешающие правила для программ из папок** не выбрана ни одна папка.

- **Создавать разрешающие правила для программ из папок**

  В таблице вы можете выбрать или указать для задачи папки и типы исполняемых файлов, которые будут учитываться при формировании правил контроля запуска программ. Задача сформирует разрешающие правила для файлов выбранных типов, расположенных в указанных папках.

3. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Действия при автоматическом формировании правил

► *Чтобы настроить действия Kaspersky Embedded Systems Security во время выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 331) для задачи Формирование правил контроля запуска программ.
2. Выберите закладку **Параметры**.
3. В блоке **При формировании разрешающих правил** настройте следующие параметры:

   - **Использовать цифровой сертификат**

     Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

     Данный вариант выбран по умолчанию.

   - **Использовать заголовок и отпечаток цифрового сертификата**

     Флажок включает или выключает использование заголовка и отпечатка цифрового сертификата файла в качестве критерия срабатывания разрешающих правил контроля запуска программ. Включение этого флажка позволяет задать более строгие условия проверки цифрового сертификата.

     Если флажок установлен, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливаются значения заголовка и отпечатка цифрового сертификата файлов, для которых формируются правила. Kaspersky Embedded Systems Security разрешит запуск программ, которые запускаются с помощью файлов с указанным заголовком и отпечатком цифрового сертификата.

     Использование этого флажка строго ограничивает срабатывание разрешающих правил запуска программ по цифровому сертификату, так как отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан.

Если флажок снят, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

Флажок доступен, если выбран вариант **Использовать цифровой сертификат**.

По умолчанию флажок установлен.

- **Если сертификат отсутствует, использовать**

  Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

  - **хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.
  - **путь к файлу** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице **Создавать разрешающие правила для программ из папок** в разделе **Настройка**.

- **Использовать хеш SHA256**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

  Использование этого параметра рекомендуется в случаях, когда сформированные правила должны обеспечить самый высокий уровень безопасности: контрольная сумма SHA256 должны быть уникальным идентификатором файла. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.

  По умолчанию этот вариант не выбран.

- **Формировать правила для пользователя или группы пользователей**

  Поле, в котором отображается пользователь или группа пользователей. Программа будет контролировать запуски программ указанным пользователем или группой.

  По умолчанию выбрана группа **Все**.

4. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Действия по завершении автоматического формирования правил

► *Чтобы настроить действия Kaspersky Embedded Systems Security по завершении выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "**Переход к параметрам задачи Формирование правил контроля запуска программ**" на стр. 331) для задачи **Формирование правил контроля запуска программ**.
2. Выберите закладку **Параметры**.
3. В блоке **По завершении задачи** настройте следующие параметры:
   - **Добавлять разрешающие правила в список правил контроля запуска программ**

     Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля запуска программ. Список правил контроля запуска программ отображается при переходе по ссылке **Правила контроля запуска программ** в панели результатов узла Контроль запуска программ.

     Если флажок установлен, Kaspersky Embedded Systems Security добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля запуска программ, в список правил контроля запуска программ согласно выбранному принципу добавления правил.

     Если флажок снят, Kaspersky Embedded Systems Security не добавляет новые сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

     По умолчанию флажок установлен.

   - **Принцип добавления**

     Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

     - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
     - **Заменять существующие правила**. Правила добавляются в список вместо существующих правил.
     - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

     По умолчанию выбран способ **Объединять с существующими правилами**.

   - **Экспортировать разрешающие правила в файл**
   - **Добавлять информацию о компьютере в имя файла**

     Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются разрешающие правила.

     Если флажок установлен, программа добавляет имя защищаемого компьютера, а также дату и время формирования файла в имя файла экспорта.

Если флажок снят, программа не добавляет информацию о защищаемом компьютере в имя файла экспорта.

По умолчанию флажок установлен.

4. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Контроль устройств

Этот раздел содержит информацию о задаче Контроль устройств и инструкции по настройке ее параметров.

В этом разделе

О задаче Контроль устройств

Kaspersky Embedded Systems Security контролирует регистрацию и использование запоминающих устройств и устройств чтения CD/DVD-дисков в целях защиты компьютера от угроз безопасности, которые могут возникнуть во время файлового обмена с USB-подключаемым флеш-накопителем или внешним устройством другого типа. Запоминающее устройство – это подключаемое к компьютеру внешнее устройство, предназначенное для записи и хранения данных.

Kaspersky Embedded Systems Security контролирует подключение следующих типов внешних устройств:

- USB-подключаемые флеш-накопители;
- устройства чтения CD/DVD-дисков;
- USB-подключаемые устройства чтения гибких дисков;
- USB-подключаемые мобильные устройства MTP.

Kaspersky Embedded Systems Security сообщает обо всех устройствах, подключенных по USB, с помощью соответствующего события в журнале событий и в журнале выполнения задачи. Описание события включает тип устройства и путь подключения При запуске задачи Контроль устройств Kaspersky Embedded Systems Security проверяет и перечисляет все устройства, подключенные по USB. Уведомления можно настроить в блоке параметров уведомлений Kaspersky Security Center.

Задача Контроль устройств отслеживает попытки подключения внешних устройств по USB к защищаемому компьютеру и блокирует их подключение, если не находит разрешающих правил для этих устройств. После блокировки соединения устройство становится недоступно.

Программа присваивает каждому подключаемому запоминающему устройству один из следующих статусов:

- *Доверенное*. Устройство, обмен данными с которым разрешен. При формировании правила значение *Путь к экземпляру устройства* подпадает под область применения хотя бы одного правила.
- *Недоверенное*. Устройство, обмен данными с которым запрещен. Путь к экземпляру такого устройства не подпадает под область применения разрешающих правил.

Вы можете создать разрешающие правила для внешних устройств, обмен данными с которыми вы хотите разрешить, с помощью задачи Формирование правил контроля устройств. Вы также можете расширять область применения уже созданных разрешающих правил. Вы не можете создавать разрешающие правила вручную.

Kaspersky Embedded Systems Security идентифицирует регистрируемое в системе запоминающее устройство по значению пути к экземпляру устройства. Путь к экземпляру устройства является уникальным признаком для каждого устройства. Информация о пути к экземпляру устройства содержится в свойствах внешнего устройства в операционной системе Windows и определяется Kaspersky Embedded Systems Security в момент создания разрешающих правил автоматически.

Задача Контроль устройств может выполняться в одном из двух режимов:

- **Активный**. Kaspersky Embedded Systems Security контролирует с помощью правил подключение флеш-накопителей и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

  Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому компьютеру до того, как была запущена задача Контроль устройств в режиме **Активный**, то это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить компьютер. В противном случае принцип запрета по умолчанию не будет применен к устройству.

- **Только статистика**. Kaspersky Embedded Systems Security не контролирует подключение флеш-накопителей и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключении и регистрации внешних устройств на защищаемом компьютере, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.

  Этот режим можно использовать для формирования правил на основе информации о блокировании устройств, зарегистрированной во время выполнения задачи (см. раздел "Формирование списка правил по событиям задачи Контроль устройств" на стр. 373).

О правилах контроля устройств

Правила создаются индивидуально для каждого устройства, подключенного в данный момент или подключавшегося ранее к защищаемому компьютеру, если данные об этом устройстве сохранились в системе.

Вы можете создавать разрешающие правила контроля устройств следующими способами:

- использовать задачу Формирование правил контроля устройств (см. раздел "О задаче Формирование правил контроля устройств" на стр. 355).
- запустить задачу Контроль устройств в режиме Только статистика (см. раздел "Формирование списка правил по событиям задачи Контроль устройств" на стр. 373).
- использовать данные системы о подключавшихся устройствах (см. раздел "Добавление разрешающего правила для одного или нескольких внешних устройств" на стр. 373).
- расширить область применения уже созданных правил (см. раздел "Расширение области применения правил контроля устройств" на стр. 375).

Максимальное количество правил контроля устройств, которое поддерживает Kaspersky Embedded Systems Security, составляет 3072.

Правила контроля устройств описаны ниже.

Тип правила

Тип правила - всегда *разрешающее*. Задача Контроль устройств по умолчанию блокирует подключение всех флеш-накопителей и других внешних устройств, если они не подпадают под область действия ни одного разрешающего правила.

Критерий срабатывания и область применения правила

Правила контроля устройств идентифицируют подключаемые флеш-накопители и другие внешние устройства по значению *пути к экземпляру устройства*. Путь к экземпляру устройства является уникальным идентификатором, который система присваивает устройству в момент его подключения и регистрации в качестве запоминающего устройства или устройства чтения CD/DVD-дисков (например, IDE или SCSI).

Kaspersky Embedded Systems Security контролирует подключение внешних устройств чтения CD/DVD дисков вне зависимости от шины подключения. При монтировании таких устройств по USB, операционная система регистрирует два значения пути к экземпляру устройства: для запоминающего устройства и для устройства чтения CD/DVD-дисков (например, IDE или SCSI). Для корректного подключения таких устройств требуется наличие разрешающих правил для каждого значения пути к экземпляру устройства.

Kaspersky Embedded Systems Security автоматически определяет путь к экземпляру устройства и разбивает найденное значение на следующие составляющие:

- производитель устройства (VID);
- тип контроллера устройства (PID);
- серийный номер устройства.

Вы не можете задавать путь к экземпляру устройства вручную. Заданные в свойствах разрешающего правила критерии срабатывания правила определяют область применения этого правила. По умолчанию в область применения только что созданного разрешающего правила включено одно устройство, на основе свойств которого Kaspersky Embedded Systems Security сформировал разрешающее правило. Вы можете

изменять значения параметров созданного правила с помощью маски, чтобы расширить область применения правила (см. раздел "Расширение области применения правил контроля устройств" на стр. 375).

Данные исходного устройства

Данные устройства, на основе которых программа Kaspersky Embedded Systems Security сформировала разрешающее правило, отображаются в свойствах каждого правила.

Данные исходного устройства содержат следующую информацию:

- **Путь к экземпляру устройства**. На основании этого свойства Kaspersky Embedded Systems Security определяет критерий срабатывания правила и заполняет следующие поля: **Производитель (VID)**, **Тип контроллера (PID)**, **Серийный номер** в блоке **Область применения правила** окна **Параметры правила**.
- **Адаптированное имя**. Имя, которое задается в свойствах устройства производителем.

При создании правила Kaspersky Embedded Systems Security автоматически определяет исходные значения для устройства. В дальнейшем вы можете использовать эти значения, чтобы определить, на основе данных какого устройства было создано правило. Данные исходного устройства недоступны для редактирования.

Описание

Вы можете добавить дополнительную информацию для каждого созданного правила контроля устройств в поле **Комментарий**, например, название подключаемого флеш-накопителя или имя его владельца. Комментарий отображается в соответствующем поле в окне **Правила контроля устройств**.

Комментарий и данные исходного устройства не учитываются при работе правила и служат только для упрощения идентификации устройств и правил пользователем.

О формировании списка правил контроля устройств

Вы можете импортировать списки разрешающих правил контроля устройств из XML-файлов, сформированных автоматически в ходе выполнения задачи Контроль устройств или задачи Формирование правил контроля устройств.

По умолчанию Kaspersky Embedded Systems Security запрещает подключение любых флеш-накопителей и других внешних устройств, которые не подпадают под действие заданных правил контроля устройств.

Таблица 49. Цели и сценарии формирования списка правил контроля устройств

Сценарий формирования списка правил	Решаемая задача
Задача Формирование правил контроля устройств	• Создать разрешающие правила для уже использовавшихся доверенных устройств перед первым запуском задачи Контроль устройств. • Сформировать список правил для доверенных устройств в сети защищаемых компьютеров.
Создание правил на основе данных системы	Добавить разрешающие правила для одного или нескольких новых подключенных устройств.

Режим **Только статистика** задачи Контроль устройств	Добавить разрешающие правила для большого количества доверенных устройств.

Использование задачи Формирование правил контроля устройств

XML-файл, сформированный по завершении задачи Формирование правил контроля устройств, содержит разрешающие правила для флеш-накопителей и других внешних устройств, данные о подключении которых сохранились в системе.

В ходе выполнения задачи Kaspersky Embedded Systems Security получает данные системы обо всех запоминающих устройствах, подключавшихся ранее и подключенных в данный момент к защищаемому компьютеру, и формирует на основе этих данных список разрешающих правил для обнаруженных устройств. По завершении задачи программа формирует XML-файл в папке по пути, указанному в параметрах задачи. Вы можете настроить автоматический импорт сформированных правил в список правил задачи Контроль устройств.

Рекомендуется использовать этот сценарий для формирования списка разрешающих правил перед первым запуском задачи Контроль устройств, чтобы созданные разрешающие правила учитывали все доверенные внешние устройства, используемые на защищаемом компьютере.

Использование данных системы обо всех подключаемых устройствах

В ходе выполнения задачи Kaspersky Embedded Systems Security получает данные системы обо всех внешних устройствах, подключавшихся ранее и подключенных в данный момент к защищаемому компьютеру, и отображает обнаруженные устройства в списке в окне **Сформировать правила на основе данных системы**.

Для каждого обнаруженного устройства Kaspersky Embedded Systems Security определяет производителя (VID), тип контроллера (PID), адаптированное имя, серийный номер и путь к экземпляру устройства. Можно сформировать разрешающие правила для любого запоминающего устройства, данные о котором хранятся в системе, и сразу добавить новые правила в список правил контроля устройств.

Рекомендуется использовать этот сценарий для обновления списка существующих правил, если нужно разрешить использование небольшого количества новых запоминающих устройств.

Kaspersky Embedded Systems Security не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать разрешающие правила для MTP-подключаемых мобильных устройств.

Использование задачи Контроль устройств в режиме Только статистика

XML-файл, полученный по завершении задачи Контроль устройств в режиме **Только статистика**, формируется на основе журнала выполнения задачи.

В ходе выполнения задачи Kaspersky Embedded Systems Security фиксирует информацию обо всех подключениях флеш-накопителей и других запоминающих устройств к защищаемому компьютеру в журнале выполнения задачи. Вы можете сформировать разрешающие правила по событиям задачи и экспортировать их в XML-файл. Перед запуском задачи в режиме **Только статистика** рекомендуется настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнились все возможные подключения внешних устройств к защищаемому компьютеру.

Рекомендуется использовать этот сценарий для обновления существующего списка правил, если нужно разрешить использование большого количества новых внешних устройств.

Если формирование списка правил по этому сценарию выполняется на эталонной машине, вы можете применить сформированный список разрешающих правил при настройке задачи Контроль устройств в Kaspersky Security Center. Таким образом вы сможете разрешать использование внешних устройств, подключенных к эталонной машине, на всех компьютерах защищаемой сети.

О задаче Формирование правил контроля устройств

Задача Формирование правил контроля устройств позволяет автоматически формировать список разрешающих правил для подключения флеш-накопителей и других запоминающих устройств на основе данных операционной системы обо всех внешних устройствах, которые ранее подключались к защищаемому компьютеру.

Kaspersky Embedded Systems Security не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать разрешающие правила для MTP-подключаемых мобильных устройств.

По завершении выполнения задачи Kaspersky Embedded Systems Security создает конфигурационный файл в формате XML со списком разрешающих правил для обнаруженных внешних устройств или сразу добавляет сформированные правила в задачу Контроль устройств в зависимости от параметров задачи Формирование правил контроля устройств. В дальнейшем программа будет разрешать подключение устройств, для которых были автоматически сформированы разрешающие правила.

Сформированные и добавленные в задачу правила отображаются в окне **Правила контроля устройств**.

Сценарии формирования правил контроля устройств

Вы можете создавать правила (см. раздел "Формирование правил контроля устройств для всей сети в Kaspersky Security Center" на стр. 361) на основании данных Windows обо всех запоминающих устройствах, подключаемых ранее или подключенных сейчас, с помощью следующих сценариев:

- С помощью групповой задачи Формирование правил контроля устройств. Используйте этот способ, чтобы учесть при формировании правил данные обо всех когда-либо подключавшихся запоминающих устройствах, сохранившиеся в системах на всех компьютерах сети.
- С помощью параметра **Сформировать правила на основе данных системы**. Используйте этот способ, чтобы учесть при формировании правил данные обо всех когда-либо подключавшихся запоминающих устройствах, сохранившиеся в системе на компьютере, на котором установлена Консоль администрирования Kaspersky Security Center.
- С помощью параметра **Сформировать правила для устройств, подключенных в текущий момент** в окне **Правила контроля устройств** и в параметрах задачи Формирование правил контроля устройств. Используйте этот способ, если требуется, чтобы при формировании разрешающих правил учитывались данные только об устройствах, подключенных к защищаемому компьютеру в настоящее время.

Kaspersky Embedded Systems Security не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать разрешающие правила для доверенных MTP-подключаемых мобильных устройств с помощью сценариев наполнения списка правил, основанных на применении данных системы обо всех устройствах.

Параметры по умолчанию для задачи Контроль устройств

По умолчанию задача Контроль устройств имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 50. Параметры по умолчанию для задачи Контроль устройств

Параметр	Значение по умолчанию	Описание
Режим работы	**Только статистика**	Задача фиксирует в журнале выполнения события запрета и разрешения подключения внешних устройств в соответствии с заданными правилами. Фактическая блокировка использования внешних устройств не выполняется. Вы можете выбрать режим **Активный** для защиты компьютера, чтобы применять фактическую блокировку использования внешних устройств.
Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется	Не применяется	Kaspersky Embedded Systems Security запрещает использование внешних устройств вне зависимости от статуса выполнения задачи Контроль устройств. Это обеспечивает максимальную защиту от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами. Вы можете настраивать параметр таким образом, чтобы Kaspersky Embedded Systems Security разрешал использование всех внешних устройств, если задача Контроль устройств не выполняется.
Расписание запуска задачи	Первый запуск не определен.	Задача Контроль устройств запускается автоматически сразу после Kaspersky Embedded Systems Security. Вы можете настроить запуск задачи по расписанию.

Таблица 51. Параметры задачи Формирование правил контроля устройств по умолчанию

Параметр	Значение по умолчанию	Описание
Режим генерации	**Учитывать данные системы обо всех когда-либо подключавшихся устройствах**	Режим работы задачи. Можно выбрать режим **Учитывать только подключенные в настоящий момент запоминающие устройства**.
Действия по завершении задачи	Разрешающие правила добавляются в список правил задачи Контроль устройств; новые правила объединяются с существующими правилами; дублирующие правила удаляются.	Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующих правил или заменять существующие правила новыми разрешающими правилами, а также настроить параметры экспорта разрешающих правил в файл.
Расписание запуска задачи	Первый запуск не определен.	Задача Формирование правил контроля устройств не запускается автоматически сразу после Kaspersky Embedded Systems Security. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

Управление контролем устройств с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и управление подключением запоминающих устройств ко всем компьютерам в сети с помощью списков правил в Kaspersky Security Center для групп компьютеров.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

В этом разделе

Переход к параметрам политики для задачи Контроль устройств

► *Чтобы перейти к параметрам задачи Контроль устройств в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую требуется настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль устройств**.

   Откроется окно **Контроль устройств**.
7. Настройте политику в соответствии с вашими требованиями.

Переход к списку правил контроля устройств

► *Чтобы перейти к списку правил контроля устройств в Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую требуется настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на компьютерах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль устройств**.

   Откроется окно **Контроль устройств**.

7. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля устройств**.

8. Настройте политику в соответствии с вашими требованиями.

Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам

► *Чтобы создать задачу Формирование правил контроля устройств, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**.

   Откроется окно **Мастер создания задачи**.

5. Выберите задачу **Формирование правил контроля устройств**.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Настройка**.

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Задачи**.
4. Выберите название задачи в списке задач Kaspersky Security Center двойным щелчком мыши.

   Откроется окно **Свойства: Формирование правил контроля устройств**.

Дополнительную информацию о настройке задачи см. в разделе Настройка задачи Формирование правил контроля устройств.

Настройка задачи Контроль устройств

► *Чтобы настроить параметры задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Контроль устройств** (см. раздел "Переход к параметрам политики для задачи Контроль устройств" на стр. 358).

2. На закладке **Общие** настройте следующие параметры задачи:
   - В блоке **Режим работы** выберите один из следующих режимов работы задачи:
     - **Активный**.

       Kaspersky Embedded Systems Security контролирует с помощью правил подключение флеш-накопителей и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

       Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому компьютеру до того, как была запущена задача Контроль устройств в активном режиме, то это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить компьютер. В противном случае принцип запрета по умолчанию не будет применен к устройству.

     - **Только статистика**.

       Kaspersky Embedded Systems Security не контролирует подключение флеш-накопителей и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключении и регистрации внешних устройств на защищаемом компьютере, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.
   - Снимите или установите флажок **Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется**.

     Флажок разрешает или запрещает использование запоминающих устройств, если задача Контроль устройств не выполняется.

     Если флажок установлен и задача Контроль устройств не выполняется, Kaspersky Embedded Systems Security разрешает использовать любые запоминающие устройства на защищаемом компьютере.

     Если флажок снят, Kaspersky Embedded Systems Security запрещает использовать недоверенные запоминающие устройства на защищаемом компьютере в следующих случаях: если не выполняется задача Контроль устройств или если отключена служба Kaspersky Security. Рекомендуется использовать этот вариант для обеспечения максимальной защиты от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами.

     По умолчанию флажок снят.
3. Нажмите на кнопку **Список правил**, чтобы изменить список правил контроля устройств (см. раздел "Настройка правил контроля устройств в Kaspersky Security Center" на стр. 363).
4. Если требуется, настройте расписание запуска задачи на закладке **Управление задачей**.
5. Нажмите на кнопку **ОК**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров до и после их изменения будут сохранены в журнале выполнения задачи.

Формирование правил контроля устройств для всей сети в Kaspersky Security Center

Вы можете создавать списки правил контроля устройств с помощью задач Kaspersky Security Center сразу для всех компьютеров и групп компьютеров в сети организации.

Вы можете создавать списки правил контроля устройств на стороне Kaspersky Security Center следующими способами:

- С помощью групповой задачи Формирование правил контроля устройств.

  При использовании этого сценария групповая задача формирует списки правил на основе системных данных каждого компьютера обо всех когда-либо подключавшихся к нему запоминающих устройствах. Задача также учитывает все запоминающие устройства, подключенные в момент выполнения групповой задачи. По завершении выполнения групповой задачи, Kaspersky Embedded Systems Security формирует списки разрешающих правил для всех зарегистрированных запоминающих устройств сети и сохраняет эти списки в XML-файл в указанной общей папке. Далее вы можете вручную импортировать сформированные правила в свойства задачи Контроль устройств. В отличие от задачи на локальном компьютере, в политике невозможно настроить автоматическое добавление созданных правил в список правил контроля устройств по завершении групповой задачи Формирование правил контроля устройств.

  Рекомендуется использовать этот сценарий для формирования списка разрешающих правил перед первым запуском задачи Контроль устройств в **Активном** режиме применения правил.

  > При применении политики контроля устройств в сети убедитесь, что для всех защищаемых компьютеров настроен доступ к папке общего доступа. Если применение сетевой папки общего доступа не предусмотрено политикой организации, рекомендуется запускать задачу Формирование правил контроля устройств в тестовой группе компьютеров или на эталонной машине организации.

- На основе отчета о событиях в работе задачи Контроль устройств в режиме **Только статистика**, сформированного в Kaspersky Security Center.

  При использовании этого сценария Kaspersky Embedded Systems Security не блокирует подключения запоминающих устройств, но фиксирует все попытки подключения и регистрации запоминающих устройств на всех компьютерах сети за период работы задачи Контроль устройств в режиме **Только статистика**. Эта информация содержится на закладке **События** рабочей области узла **Сервер администрирования** в Kaspersky Security Center. Затем Kaspersky Security Center создает на основе журнала выполнения задачи единый список событий блокировки и подключения запоминающих устройств.

  Вам нужно настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнились все подключения запоминающих устройств. Далее при добавлении правил в задачу контроля устройств вы можете импортировать данные о подключениях устройств из сохраненного файла отчета о событиях Kaspersky Security Center (в формате TXT) и сформировать на основе этих данных разрешающие правила контроля таких устройств. При импорте созданного отчета на основе событий любого типа формируются разрешающие правила.

  Рекомендуется использовать этот сценарий для добавления разрешающих правил для большого количества новых запоминающих устройств, а также для создания правил для доверенных мобильных устройств, подключаемых по протоколу MTP.

- На основе системных данных о подключавшихся запоминающих устройствах, с помощью параметра **Сформировать правила на основе данных системы** в параметрах задачи Контроль устройств.

  При использовании этого сценария Kaspersky Embedded Systems Security формирует разрешающие правила для запоминающих устройств, подключавшихся ранее или подключенных в текущий момент к компьютеру, на котором установлен Kaspersky Security Center.

  Рекомендуется использовать этот сценарий, если требуется сформировать правила для небольшого количества новых запоминающих устройств, использование которых вы хотите разрешить на всех компьютерах сети.

- На основе данных об устройствах, подключенных в текущий момент (с помощью параметра **Сформировать правила для устройств, подключенных в текущий момент**).

  При использовании этого сценария Kaspersky Embedded Systems Security формирует разрешающие правила только для устройств, подключенных в текущий момент. Вы можете выбрать одно или несколько устройств, для которых вы хотите сформировать разрешающие правила.

  > Kaspersky Embedded Systems Security не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать разрешающие правила для доверенных MTP-подключаемых мобильных устройств с помощью сценариев наполнения списка правил, основанных на применении данных системы обо всех устройствах.

Настройка задачи Формирование правил контроля устройств

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. Откройте окно **Свойства: Формирование правил контроля устройств** (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам**" на стр. 359).
2. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   > Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*

3. В разделе **Настройка** вы можете настроить следующие параметры:
   - Выбор режима работы: учитывать данные системы обо всех когда-либо подключавшихся запоминающих устройствах или только о подключенных в настоящий момент запоминающих устройствах.
   - Настройте параметры для конфигурационных файлов со списком разрешающих правил, которые Kaspersky Embedded Systems Security создает по завершении задачи.
4. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз программы).
5. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.
6. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*

7. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

Настройка правил контроля устройств в Kaspersky Security Center

В этом разделе описано формирование списка правил на основе различных критериев, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль устройств.

В этом разделе

Формирование разрешающих правил на основе данных системы в политике Kaspersky Security Center

► *Чтобы задать разрешающие правила с помощью параметра **Сформировать правила на основе данных системы** задачи Контроль устройств, выполните следующие действия:*

1. Если требуется, подключите к компьютеру с установленной Консолью администрирования Kaspersky Security Center новое запоминающее устройство, использование которого вы хотите разрешить.
2. Откройте окно **Правила контроля устройств** (см. раздел "Переход к списку правил контроля устройств" на стр. 358).
3. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила на основе данных системы**.
4. Выберите принцип добавления разрешающих правил к списку созданных ранее правил контроля устройств:
   - Выберите устройство в списке устройств в окне **Сформировать правила на основе данных системы**.
   - Нажмите на кнопку **Добавить правила для выбранных устройств**.
5. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в задаче Контроль устройств будет дополнен новыми правилами, сформированными на основе системных данных компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

Формирование правил для подключенных устройств

► *Чтобы задать разрешающие правила с помощью параметра **Сформировать правила для устройств, подключенных в текущий момент** задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к списку правил контроля устройств**" на стр. 358).
2. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила для устройств, подключенных в текущий момент**.

   Откроется окно **Сформировать правила на основе данных системы**.
3. В списке обнаруженных устройств, подключенных к защищаемому компьютеру, выберите устройства, для которых требуется сформировать разрешающие правила.
4. Нажмите на кнопку **Добавить правила для выбранных устройств**.
5. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в задаче Контроль устройств будет дополнен новыми правилами, сформированными на основе системных данных компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

Импорт правил из отчета Kaspersky Security Center о заблокированных устройствах

Можно импортировать данные о заблокированных попытках подключения запоминающих устройств из отчета, сформированного в Kaspersky Security Center по результатам выполнения задачи Контроль устройств в режиме **Только статистика** (см. раздел "Настройка задачи Контроль устройств" на стр. 359), и применить эти данные для формирования списка разрешающих правил контроля устройств в настраиваемой политике.

При формировании отчета о событиях, возникающих в ходе выполнения задачи Контроль устройств, вы можете отследить, подключение каких устройств будет блокироваться.

► *Чтобы задать разрешающие правила подключения устройств для группы компьютеров на основе отчета Kaspersky Security Center о заблокированных устройствах, выполните следующие действия:*

1. В свойствах политики в разделе **Уведомления о событиях** убедитесь, что выполняются следующие условия:
   - Для событий с уровнем важности **Критическое событие** срок хранения событий *Запоминающее устройство запрещено* в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).
   - Для событий с уровнем важности **Предупреждение** срок хранения событий *Только статистика: обнаружено недоверенное запоминающее устройство* в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

По завершении периода хранения событий, информация о зарегистрированных событиях будет удалена и не попадет в файл отчета. Перед запуском задачи Контроль устройств в режиме **Только статистика** убедитесь, что время выполнения задачи не превышает установленное время хранения указанных событий.

2. Запустите задачу Контроль устройств в режиме **Только статистика**. В Kaspersky Security Center в рабочей области узла **Сервер администрирования** выберите закладку **События**. Нажмите на кнопку **Создать выборку** и создайте выборку событий по критерию *Обнаружено недоверенное запоминающее устройство*. Просмотрите, подключения каких устройств заблокированы задачей Контроль устройств. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных подключениях в файл формата TXT.

   Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех устройствах, подключение которых вы хотите разрешить.

3. Импортируйте данные о заблокированных попытках подключения устройств в задачу Контроль устройств.

   a. Откройте окно **Правила контроля устройств** (см. раздел "Переход к списку правил контроля устройств" на стр. 358).

   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать правила из файла отчета KSC о заблокированных устройствах**.

   c. Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку уже заданных правил контроля устройств:

      - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
      - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
      - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   d. В открывшемся стандартном окне Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных устройствах.

   e. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

4. Нажмите на кнопку **ОК** в окне **Контроль устройств**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных устройствах, будут добавлены к списку правил в политике контроля устройств.

Создание правил с помощью задачи Формирование правил контроля устройств

► *Чтобы задать разрешающие правила контроля устройств для группы компьютеров с помощью задачи Формирование правил контроля устройств, выполните следующие действия:*

1. Откройте окно **Настройка** в мастере создания задачи (см. раздел "**Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам**" на стр. 359).
2. Настройте следующие параметры:
   - В блоке **Режим**:
     - **Учитывать данные системы обо всех когда-либо подключавшихся устройствах**
     - **Учитывать данные только об устройствах, подключенных в текущий момент**
   - В блоке **После завершения задачи**:
     - **Добавлять разрешающие правила в список правил контроля устройств**

       Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля устройств. Список правил контроля устройств отображается по ссылке **Правила контроля устройств** в панели результатов узла **Контроль устройств**.

       Если флажок установлен, Kaspersky Embedded Systems Security добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля устройств, в список правил контроля устройств согласно выбранному принципу добавления правил.

       Если флажок снят, Kaspersky Embedded Systems Security не добавляет новые сформированные разрешающие правила в список правил контроля устройств. Сформированные правила только экспортируются в файл.

       По умолчанию флажок установлен.

       Флажок не может быть установлен, если не установлен флажок **Экспортировать разрешающие правила в файл**.

     - **Принцип добавления**

       Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

       - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
       - **Заменять существующие правила**. Правила добавляются в список вместо существующих правил.
       - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

       По умолчанию выбран способ **Объединять с существующими правилами**.

     - **Экспортировать разрешающие правила в файл**

       Флажок включает или выключает экспорт разрешающих правил контроля устройств в файл.

Если флажок установлен, по завершении задачи Формирование правил контроля устройств Kaspersky Embedded Systems Security экспортирует разрешающие правила в файл, указанный в поле ниже.

Если флажок снят, по завершении задачи Формирование правил контроля устройств экспорт сформированных разрешающих правил в файл не выполняется. Правила только добавляются в список правил контроля устройств.

По умолчанию флажок снят.

Флажок не может быть установлен, если не установлен флажок **Добавлять разрешающие правила в список правил контроля устройств**.

- **Добавлять информацию о компьютере в имя файла**

  Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются разрешающие правила.

  Если флажок установлен, программа добавляет имя защищаемого компьютера, а также дату и время формирования файла в имя файла экспорта.

  Если флажок снят, программа не добавляет информацию о защищаемом компьютере в имя файла экспорта.

  По умолчанию флажок установлен.

3. Нажмите на кнопку **Далее**.
4. В окне **Расписание** укажите параметры запуска задачи по расписанию.
5. Нажмите на кнопку **Далее**.
6. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
7. Нажмите на кнопку **Далее**.
8. Укажите название задачи.
9. Нажмите на кнопку **Далее**.

   Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы:
   " * < > & \ : |

   Откроется окно **Завершение создания задачи**.
10. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
11. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.
12. На закладке **Задачи** в рабочей области настраиваемой группы компьютеров в списке групповых задач выберите созданную задачу Формирование правил контроля устройств.
13. Нажмите на кнопку **Запустить** для запуска задачи.

    По завершении задачи автоматически сформированные списки разрешающих правил будут сохранены в папке общего доступа в файлах формата XML.

При применении политики контроля устройств в сети убедитесь, что для всех защищаемых компьютеров настроен доступ к папке общего доступа. Если применение сетевой папки общего доступа не предусмотрено политикой организации, рекомендуется запускать задачу Формирование правил контроля устройств в тестовой группе компьютеров или на эталонной машине организации.

Добавление сформированных правил в список правил контроля устройств

► *Чтобы добавить сформированные списки разрешающих правил в задачу Контроль устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "Переход к списку правил контроля устройств" на стр. 358).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки **Добавить** выберите пункт **Импортировать правила из файла XML**.
4. Выберите принцип добавления автоматически сформированных разрешающих правил к списку уже заданных правил контроля устройств:
   - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.
5. В открывшемся стандартном окне Windows выберите файлы формата XML, созданные по завершении групповой задачи Формирование правил контроля устройств.
6. Нажмите на кнопку **Открыть**.

   Все сформированные правила из XML-файла добавляются в список в соответствии с выбранным принципом.
7. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.
8. Если вы хотите применять созданные правила контроля устройств, в свойствах политики для Контроля устройств выберите режим выполнения задачи **Активный**.

Разрешающие правила, автоматически сформированные на основе данных системы на каждом отдельном компьютере, будут применены ко всем компьютеров в сети под управлением настраиваемой политики. Для этих компьютеров программа разрешит подключение только тех устройств, для которых созданы разрешающие правила.

Управление Контролем устройств с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи для локального компьютера.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

В этом разделе

Переход к параметрам задачи Контроль устройств

► *Чтобы перейти к параметрам задачи Контроль устройств в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В панели результатов узла **Контроль устройств** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Настройте задачу в соответствии с вашими требованиями.

Переход к окну с правилами контроля устройств

► *Чтобы перейти к списку правил контроля устройств в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.

3. В панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.

4. Настройте список правил в соответствии с вашими требованиями.

Переход к параметрам задачи Формирование правил контроля устройств

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
2. Выберите вложенный узел **Формирование правил контроля устройств**.
3. В панели результатов узла **Формирование правил контроля устройств** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. Настройте задачу в соответствии с вашими требованиями.

Настройка параметров задачи Контроль устройств

► *Чтобы настроить параметры задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Параметры задачи** (см. раздел "Переход к параметрам задачи Контроль устройств" на стр. 369).
2. На закладке **Общие** настройте следующие параметры задачи:
   - В блоке **Режим работы** выберите один из следующих режимов работы задачи:
     - **Активный**.

       Kaspersky Embedded Systems Security контролирует с помощью правил подключение флеш-накопителей и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

       Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому компьютеру до того, как была запущена задача Контроль устройств в активном режиме, то это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить компьютер. В противном случае принцип запрета по умолчанию не будет применен к устройству.

- **Только статистика**.

  Kaspersky Embedded Systems Security не контролирует подключение флеш-накопителей и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключении и регистрации внешних устройств на защищаемом компьютере, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.

- Снимите или установите флажок **Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется**.

  Флажок разрешает или запрещает использование запоминающих устройств, если задача Контроль устройств не выполняется.

  Если флажок установлен и задача Контроль устройств не выполняется, Kaspersky Embedded Systems Security разрешает использовать любые запоминающие устройства на защищаемом компьютере.

  Если флажок снят, Kaspersky Embedded Systems Security запрещает использовать недоверенные запоминающие устройства на защищаемом компьютере в следующих случаях: если не выполняется задача Контроль устройств или если отключена служба Kaspersky Security. Рекомендуется использовать этот вариант для обеспечения максимальной защиты от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами.

  По умолчанию флажок снят.

3. Если требуется, на закладках **Расписание** и **Дополнительно** настройте параметры запуска задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 151).
4. Чтобы отредактировать список правил контроля устройств (см. раздел "О формировании списка правил контроля устройств" на стр. 353), перейдите по ссылке **Правила контроля устройств** в нижней части панели результатов узла **Контроль устройств**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

Настройка правил контроля устройств

В этом разделе описано формирование, импорт и экспорт списка правил, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль устройств.

В этом разделе

Импорт правил контроля устройств из файла формата XML

► *Чтобы импортировать правила контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 369).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Импортировать правила из файла XML**.
4. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла XML**:
   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется стандартное окно Microsoft Windows **Открыть**.
5. В окне **Открыть** выберите XML-файл, который содержит параметры правил контроля устройств.
6. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля устройств**.

Формирование списка правил по событиям задачи Контроль устройств

► *Чтобы создать конфигурационный файл со списком правил контроля устройств, сформированным по событиям задачи Контроль устройств, выполните следующие действия:*

1. Запустите задачу Контроль устройств в режиме **Только статистика** (см. раздел "**Настройка параметров задачи Контроль устройств**" на стр. 370), чтобы зафиксировать в журнале выполнения задачи все события подключения флеш-накопителей и других внешних устройств к защищаемому компьютеру.
2. По завершении выполнения задачи в режиме **Только статистика** откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в блоке **Управление** в панели результатов узла **Контроль устройств**.
3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Embedded Systems Security создаст конфигурационный файл в формате XML со списком правил на основе событий, зарегистрированных при работе задачи Контроль устройств в режиме **Только статистика**. Можно применить этот список правил в задаче Контроль устройств (см. раздел "Импорт правил контроля устройств из XML-файла" на стр. 372).

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть, а затем вручную обработать список правил, чтобы убедиться, что подключение недоверенных устройств не разрешено заданными правилами.

При конвертации XML-файла с событиями выполнения задачи в список правил контроля устройств, программа создает разрешающие правила для всех зафиксированных событий, в том числе для событий блокирования устройств.

Все события, возникшие в ходе выполнения задачи, фиксируются в журнале выполнения задачи, независимо от режима. Вы можете создать конфигурационный файл со списком правил по результатам выполнения задачи в режиме **Активный**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, так как для эффективного выполнения задачи требуется сформировать финальную версию списка правил до запуска задачи в активном режиме.

Добавление разрешающего правила для внешних устройств

В задаче контроля устройств не предусмотрена функция добавления одного правила вручную. Однако в случае, если вам необходимо добавить разрешающие правила для одного или нескольких новых внешних устройств, вы можете использовать опцию **Сформировать правила на основе данных системы**. При использовании этого сценария наполнения списка разрешающих правил программа использует данные Windows обо всех подключениях внешних устройств, когда-либо регистрировавшихся в системе, а также учитывает подключенные в текущий момент устройства.

Kaspersky Embedded Systems Security не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать разрешающие правила для MTP-подключаемых мобильных устройств.

► *Чтобы добавить разрешающее правило для внешних устройств, подключенных в данный момент, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "Переход к окну с правилами контроля устройств" на стр. 369).
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Сформировать правила на основе данных системы**.
4. В открывшемся окне в списке обнаруженных устройств выберите одно или несколько устройств, использование которых вы хотите разрешить на защищаемом компьютере.
5. Нажмите на кнопку **Добавить правила для выбранных устройств**.

Новые правила будут добавлены в список правил контроля устройств.

Удаление правил контроля устройств

► *Чтобы удалить правила контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 369).
2. В списке правил выберите одно или несколько правил, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить выбранные**.
4. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля устройств будут удалены.

Экспорт правил контроля устройств

► *Чтобы экспортировать правила контроля устройств в конфигурационный файл, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 369).
2. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.
3. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, его содержимое будет перезаписано после окончания экспорта правил.
4. Нажмите на кнопку **Сохранить**.

Правила и их параметры будут экспортированы в указанный файл.

Включение и выключение правила контроля устройств

Вы можете включать и выключать применение созданных разрешающих правил контроля устройств, не удаляя их.

► *Чтобы включить или выключить созданное правило контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 369).
2. В списке заданных правил откройте окно **Параметры правила** двойным щелчком мыши на правиле, параметры которого хотите настроить.
3. В открывшемся окне снимите или установите флажок **Применять правило**.

   Флажок включает или выключает применение конкретного правила контроля устройств.

   Если флажок установлен в параметрах правила, такое правило будет применяться. Подключение внешних устройств, подпадающих под область применения этого правила, будет разрешено.

   Если флажок снят в параметрах правила, такое правило не будет применяться. Подключение внешних устройств, подпадающих под область применения этого правила, будет запрещено.

   По умолчанию флажок установлен в параметрах каждого созданного правила.
4. Нажмите на кнопку **ОК**.

Статус применения правила будет сохранен и отобразится для указанного правила.

Расширение области применения правил контроля устройств

Каждое автоматически созданное правило контроля устройств разрешает подключение только одного внешнего устройства. Вы можете вручную расширить область применения правила, применив маску пути к экземпляру устройства в свойствах любого заданного правила контроля устройств.

Применение маски пути к экземпляру устройства уменьшает количество разрешающих правил контроля устройств и упрощает процесс их обработки вручную. Однако расширение области применения правил может снижать эффективность контроля запоминающих устройств.

► *Чтобы применить маску пути к экземпляру устройства в свойствах правила контроля устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств** (см. раздел "**Переход к окну с правилами контроля устройств**" на стр. 369).
2. В открывшемся окне выберите правило, на основе свойств которого вы хотите применить маску пути к экземпляру устройства.
3. Откройте окно **Параметры правила** двойным щелчком мыши на выбранном правиле контроля устройств.

4. В открывшемся окне выполните следующие действия:

   - Установите флажок **Использовать маску** рядом с полем **Тип контроллера (PID)**, если вы хотите, чтобы выбранное правило разрешало подключение всех запоминающих устройств с указанными данными о производителе и типе устройства.
   - Установите флажок **Использовать маску** рядом с полем **Серийный номер**, если вы хотите, чтобы выбранное правило разрешало подключение всех запоминающих устройств с указанными данными о производителе и серийном номере устройства.
   - Установите флажки **Использовать маску** рядом с полями **Тип контроллера (PID)** и **Серийный номер**, если вы хотите, чтобы выбранное правило разрешало подключение всех запоминающих устройств с указанными данными о производителе устройства.

   Если хотя бы в одном поле установлен флажок **Использовать маску**, данные в полях, в которых установлен этот флажок, заменяются символом * и не учитываются при применении правила.
5. Если требуется, введите дополнительную информацию о правиле в поле **Комментарий**. Например, уточните, на какие устройства должно распространяться правило.
6. Нажмите на кнопку **ОК**.

Настроенные параметры правила будут сохранены. Область применения правила будет расширена в соответствии с указанной маской пути к экземпляру устройства.

Настройка задачи Формирование правил контроля устройств

► *Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
2. Выберите вложенный узел **Формирование правил контроля устройств**.
3. В панели результатов узла **Формирование правил контроля устройств** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие** в блоке **Режим генерации** выберите режим работы задачи:

   - **Учитывать данные системы обо всех когда-либо подключавшихся устройствах**
   - **Учитывать данные только об устройствах, подключенных в текущий момент**
5. В блоке **По завершении задачи** укажите действия, которые программа Kaspersky Embedded Systems Security должна выполнять по завершении задачи:

   - **Добавлять разрешающие правила в список правил контроля устройств**

     Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля устройств. Список правил контроля устройств отображается по ссылке **Правила контроля устройств** в панели результатов узла **Контроль устройств**.

     Если флажок установлен, Kaspersky Embedded Systems Security добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля устройств, в список правил контроля устройств согласно выбранному принципу добавления правил.

Если флажок снят, Kaspersky Embedded Systems Security не добавляет новые сформированные разрешающие правила в список правил контроля устройств. Сформированные правила только экспортируются в файл.

По умолчанию флажок установлен.

Флажок не может быть установлен, если не установлен флажок **Экспортировать разрешающие правила в файл**.

- **Принцип добавления**

  Раскрывающийся список позволяет указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

  - **Добавлять к существующим правилам**. Правила добавляются в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Заменять существующие правила**. Правила добавляются в список вместо существующих правил.
  - **Объединять с существующими правилами**. Правила добавляются в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

  По умолчанию выбран способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**

  Флажок включает или выключает экспорт разрешающих правил контроля устройств в файл.

  Если флажок установлен, по завершении задачи Формирование правил контроля устройств Kaspersky Embedded Systems Security экспортирует разрешающие правила в файл, указанный в поле ниже.

  Если флажок снят, по завершении задачи Формирование правил контроля устройств экспорт сформированных разрешающих правил в файл не выполняется. Правила только добавляются в список правил контроля устройств.

  По умолчанию флажок снят.

  Флажок не может быть установлен, если не установлен флажок **Добавлять разрешающие правила в список правил контроля устройств**.

- **Добавлять информацию о компьютере в имя файла**

  Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются разрешающие правила.

  Если флажок установлен, программа добавляет имя защищаемого компьютера, а также дату и время формирования файла в имя файла экспорта.

  Если флажок снят, программа не добавляет информацию о защищаемом компьютере в имя файла экспорта.

  По умолчанию флажок установлен.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. 151).
7. Нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

Управление сетевым экраном

Этот раздел содержит информацию о задаче Управление сетевым экраном и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Управление сетевым экраном

Kaspersky Embedded Systems Security обеспечивает надежное и эргономичное решение для защиты сетевых подключений с помощью задачи Управление сетевым экраном.

Задача Управление сетевым экраном не выполняет самостоятельную фильтрацию сетевого трафика, но предоставляет возможность управления сетевым экраном Windows через графический интерфейс Kaspersky Embedded Systems Security. В ходе выполнения задачи Управление сетевым экраном Kaspersky Embedded Systems Security полностью принимает на себя управление параметрами и правилами сетевого экрана операционной системы и блокирует любую возможность настройки сетевого экрана другими способами.

В ходе установки программы компонент Управление сетевым экраном считывает и копирует состояние сетевого экрана Windows, а также все заданные правила. В дальнейшем изменение набора правил или их параметров, а также остановка или запуск сетевого экрана возможны только через Kaspersky Embedded Systems Security.

Если при установке Kaspersky Embedded Systems Security сетевой экран Windows отключен, задача Управление сетевым экраном не выполняется по завершении установки. Если при установке программы сетевой экран Windows включен, задача Управление сетевым экраном выполняется по завершении установки и блокирует все сетевые подключения, на разрешенные заданными правилами.

Компонент Управление сетевым экраном не входит в набор компонентов Рекомендуемой установки и не устанавливается по умолчанию.

Задача Управление сетевым экраном форсирует блокирование всех входящих и исходящих подключений, если они не разрешены заданными правилами задачи.

Задача регулярно опрашивает сетевой экран Windows и контролирует его состояние. По умолчанию интервал опроса составляет 1 минуту и не может быть изменен. Если при совершении опроса Kaspersky Embedded Systems Security обнаруживает несовпадение параметров брандмауэра Windows и параметров задачи Управление сетевым экраном, программа принудительно применяет параметры задачи в брандмауэре Windows.

При ежеминутном опросе брандмауэра Windows, Kaspersky Embedded Systems Security контролирует следующие статусы:

- статус работы брандмауэра Windows;
- статус правил, добавленных после установки Kaspersky Embedded Systems Security другими программами или инструментами (например, добавление нового правила программы для порта или программы с помощью wf.msc).

После передачи правил сетевому экрану Kaspersky Embedded Systems Security создает группу правил Kaspersky Security Group в оснастке **Брандмауэр Windows**. Эта группа объединяет все правила, созданные на стороне Kaspersky Embedded Systems Security с помощью задачи Управление сетевым экраном. Правила, входящие в группу Kaspersky Security Group, не контролируются программой при ежеминутном опросе и не синхронизируются автоматически со списком правил, заданным в параметрах задачи Управление сетевым экраном. При необходимости вы можете выполнить обновление правил Kaspersky Security Group вручную.

► *Чтобы обновить список правил Kaspersky Security Group вручную,*

перезапустите задачу Управление сетевым экраном Kaspersky Embedded Systems Security.

Вы также можете изменять правила Kaspersky Security Group вручную через оснастку **Брандмауэр Windows**.

Запуск задачи Управление сетевым экраном невозможен, если сетевой экран Windows находится под управлением групповой политики Kaspersky Security Center.

О правилах сетевого экрана

Задача Управление сетевым экраном контролирует фильтрацию входящего и исходящего трафика с помощью разрешающих правил, которые принудительно применяются в брандмауэре Windows при выполнении задачи.

При первом запуске задачи Kaspersky Embedded Systems Security считывает и копирует все разрешающие правила для входящего трафика, заданные в параметрах брандмауэра Windows, в параметры задачи Управление сетевым экраном. При дальнейшей работе программа действует в соответствии со следующими алгоритмами:

- Если в параметрах брандмауэра Windows создается новое правило (вручную или автоматически при установке новой программы), Kaspersky Embedded Systems Security удаляет такое правило.
- Если в параметрах брандмауэра Windows удаляется существующее правило, Kaspersky Embedded Systems Security восстанавливает это правило при повторном запуске задачи.
- Если в параметрах брандмауэра Windows изменяются параметры существующего правила, Kaspersky Embedded Systems Security отменяет изменения.

- Если в параметрах задачи Управление сетевым экраном создается новое правило, Kaspersky Embedded Systems Security принудительно применяет это правило в брандмауэре Windows.
- Если в параметрах задачи Управление сетевым экраном удаляется существующее правило, Kaspersky Embedded Systems Security принудительно удаляет это правило из параметров брандмауэра Windows.

Kaspersky Embedded Systems Security не работает с запрещающими правилами, а также с правилами, контролирующими исходящий трафик. В момент запуска задачи Управление сетевым экраном Kaspersky Embedded Systems Security удаляет все правила этих типов в параметрах брандмауэра Windows.

Вы можете задавать, удалять и редактировать правила для фильтрации входящего трафика.

Вы не можете задать новое правило для контроля исходящего трафика через параметры задачи Управление сетевым экраном. Все правила сетевого экрана, заданные через Kaspersky Embedded Systems Security, контролируют только входящий трафик.

Вы можете работать с правилами сетевого экрана следующих типов:

- правила для приложений;
- правила для портов.

Правила для приложений

Правила этого типа выборочно разрешают сетевые подключения для указанных приложений. Критерием срабатывания таких правил является путь к исполняемому файлу.

Вы можете управлять правилами для приложений:

- добавлять новые правила;
- удалять существующие правила;
- активировать или деактивировать заданные правила.
- изменять параметры заданных правил: указывать имя правила, путь к исполняемому файлу и область применения правила.

Правила для портов

Правила этого типа разрешают сетевые подключения для указанных портов и протоколов (TCP / UDP). Критериями срабатывания таких правил являются номер порта и тип протокола.

Вы можете управлять правилами для портов:

- добавлять новые правила;
- удалять существующие правила;
- активировать или деактивировать заданные правила.
- изменять параметры заданных правил: указывать имя правила, номер порта, тип протокола и область применения правила.

Правила для портов предполагают более широкую область действия, чем правила для приложений. Разрешая подключения с помощью правил для портов, вы снижаете уровень безопасности защищаемого компьютера.

Параметры по умолчанию для задачи Управление сетевым экраном

По умолчанию в задаче Управление сетевым экраном используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 52. Параметры по умолчанию для задачи Управление сетевым экраном

Параметр	Значение по умолчанию	Описание
Правила сетевого экрана для программы	Включено два заданных по умолчанию правила для программы.	Можно выключить заданные по умолчанию правила и добавлять новые правила.
Правила сетевого экрана для портов	Включено шесть заданных по умолчанию правил для портов.	Можно выключить заданные по умолчанию правила и добавлять новые правила.
Расписание запуска задачи	Первый запуск не определен.	Задача Управление сетевым экраном не запускается автоматически при запуске Kaspersky Embedded Systems Security. Вы можете настроить запуск задачи по расписанию.

Управление правилами сетевого экрана с помощью Плагина управления

В этом разделе описано управление правилами сетевого экрана с помощью Консоли программы.

В этом разделе

Включение и выключение правил сетевого экрана

► *Чтобы включить или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.
5. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.
6. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.
7. В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:
   - Если вы хотите, чтобы неактивное правило применялось, установите флажок слева от имени правила.

     Выбранное правило будет активировано.
   - Если вы хотите, чтобы активное правило не применялось, снимите флажок слева от имени правила.

     Выбранное правило будет выключено.
8. В окне **Правила сетевого экрана** нажмите на кнопку **OK**.
9. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.
10. В окне **Свойства: <Имя политики>** нажмите на кнопку **OK**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Добавление правил сетевого экрана вручную

Вы можете добавлять и редактировать только правила для приложений и портов. Вы не можете добавлять новые или редактировать существующие правила для групп.

► *Чтобы добавить новое или изменить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.
5. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.
6. В зависимости от типа правила, которое вы хотите добавить, выберите закладку **Приложения** или закладку **Порты** и выполните одно из следующих действий:
   - Чтобы изменить существующее правило, в списке правил выберите правило, параметры которого вы хотите настроить и нажмите на кнопку **Изменить**.
   - Чтобы создать новое правило, нажмите на кнопку **Добавить**.

     В зависимости от типа настраиваемого правила, откроется окно **Настроить правило для приложения** или окно **Настроить правило для порта**.
7. В открывшемся окне выполните следующие действия:
   - Если вы работаете с правилом для приложения, выполните следующие действия:
     a. В поле **Имя правила** укажите имя редактируемого правила.
     b. В поле **Путь к приложению** укажите путь к исполняемому файлу программы, подключения для которого вы хотите разрешить с помощью редактируемого правила.

        Вы можете задать путь вручную или с помощью кнопки **Обзор**.
     c. В поле **Область применения правила** укажите сетевые адреса, в рамках которых будет

выполнятся настраиваемое правило.

Допускается указание IP-адресов только в формате IPv4.

- Если вы работаете с правилом для порта, выполните следующие действия:
  a. В поле **Имя правила** укажите имя редактируемого правила.
  b. В поле **Номер порта** укажите номер порта, для которого программа будет разрешать соединения.
  c. Выберите тип протокола (TCP / UDP), для которого программа будет разрешать соединения.
  d. В поле **Область применения правила** укажите сетевые адреса, в рамках которых будет выполнятся настраиваемое правило.

Допускается указание IP-адресов только в формате IPv4.

8. В окне **Настроить правило для приложения** или **Настроить правило для порта** нажмите на кнопку **ОК**.
9. В окне **Управление сетевым экраном** нажмите на кнопку **ОК**.
10. В окне **Свойства: <Имя политики>** нажмите на кнопку **ОК**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Удаление правил сетевого экрана

Вы можете удалять только правила для приложений и портов. Вы не можете удалять существующие правила для групп.

► *Чтобы удалить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.
5. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.
6. В зависимости от типа правила, которое вы хотите удалить, выберите закладку **Приложения** или закладку **Порты**.
7. В списке правил выберите правило, которое вы хотите удалить.
8. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.
9. В окне **Правила сетевого экрана** нажмите на кнопку **OK**.
10. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.
11. В окне **Свойства: <Имя политики>** нажмите на кнопку **OK**.

Настроенные изменения параметров задачи Управление сетевым экраном будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Управление правилами сетевого экрана с помощью Консоли программы

В этом разделе описано управление правилами сетевого экрана с помощью Консоли программы.

В этом разделе

Включение и выключение правил сетевого экрана

► *Чтобы включить или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Правила сетевого экрана**.

Откроется окно **Правила сетевого экрана**.

4. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.
5. В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:
   - Если вы хотите, чтобы неактивное правило применялось, установите флажок слева от имени правила.

     Выбранное правило будет активировано.
   - Если вы хотите, чтобы активное правило не применялось, снимите флажок слева от имени правила.

     Выбранное правило будет выключено.
6. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Добавление правил сетевого экрана вручную

► *Чтобы добавить новое или изменить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Правила сетевого экрана**.

   Откроется окно **Правила сетевого экрана**.
4. В зависимости от типа правила, которое вы хотите добавить, выберите закладку **Приложения** или закладку **Порты** и выполните одно из следующих действий:
   - Чтобы изменить существующее правило, в списке правил выберите правило, параметры которого вы хотите настроить и нажмите на кнопку **Изменить**.
   - Чтобы создать новое правило, нажмите на кнопку **Добавить**.

     В зависимости от типа настраиваемого правила, откроется окно **Настроить правило для приложения** или окно **Настроить правило для порта**.
5. В открывшемся окне выполните следующие действия:
   - Если вы работаете с правилом для приложения, выполните следующие действия:
     a. В поле **Имя правила** укажите имя редактируемого правила.
     b. В поле **Путь к приложению** укажите путь к исполняемому файлу программы, подключения для которого вы хотите разрешить с помощью редактируемого правила.

        Вы можете задать путь вручную или с помощью кнопки **Обзор**.
     c. В поле **Область применения правила** укажите сетевые адреса, в рамках которых будет выполнятся настраиваемое правило.

Допускается указание IP-адресов только в формате IPv4.

- Если вы работаете с правилом для порта, выполните следующие действия:
  a. В поле **Имя правила** укажите имя редактируемого правила.
  b. В поле **Номер порта** укажите номер порта, для которого программа будет разрешать соединения.
  c. Выберите тип протокола (TCP / UDP), для которого программа будет разрешать соединения.
  d. В поле **Область применения правила** укажите сетевые адреса, в рамках которых будет выполнятся настраиваемое правило.

  Допускается указание IP-адресов только в формате IPv4.

6. В окне **Настроить правило для приложения** или **Настроить правило для порта** нажмите на кнопку **ОК**.
7. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Удаление правил сетевого экрана

Вы можете удалять только правила для приложений и портов. Вы не можете удалять существующие правила для групп.

► *Чтобы удалить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Правила сетевого экрана**.

   Откроется окно **Правила сетевого экрана**.
4. В зависимости от типа правила, которое вы хотите удалить, выберите закладку **Приложения** или закладку **Порты**.
5. В списке правил выберите правило, которое вы хотите удалить.
6. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.
7. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Мониторинг файловых операций

Этот раздел содержит информацию о запуске и настройке задачи Мониторинг файловых операций.

В этом разделе

О задаче Мониторинг файловых операций

Задача Мониторинг файловых операций предназначена для отслеживания действий, выполненных с указанными файлами или папками, в областях мониторинга, заданных в параметрах задачи. Вы можете использовать задачу, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом компьютере. Вы также можете настроить отслеживание изменений файлов в периоды обрыва мониторинга.

Обрыв мониторинга – это период, когда область мониторинга временно выпадает из действия задачи, например из-за приостановки выполнения задачи или физического отсутствия запоминающего устройства на защищаемом компьютере. Kaspersky Embedded Systems Security сообщит об обнаружении файловых операций в области мониторинга, как только запоминающее устройство будет вновь подключено.

Приостановка выполнения задачи в заданной области мониторинга, вызванная переустановкой компонента Мониторинг файловых операций, не является обрывом мониторинга. В этом случае задача Мониторинг файловых операций не выполняется.

Требования к среде

Для запуска задачи Мониторинг файловых операций должны быть соблюдены следующие условия:

- На защищаемом компьютере установлено запоминающее устройство, поддерживающее файловые системы ReFS и NTFS.
- USN-журнал Windows должен быть включен. На основе опроса USN-журнала компонент получает данные о файловых операциях.

  Если вы включили USN-журнал после того, как было создано правило для тома и запущена задача Мониторинг файловых операций, вам нужно перезапустить задачу. В противном случае, данное правило не будет учитываться при мониторинге.

Исключения для области мониторинга

Вы можете создать исключения из области мониторинга (см. раздел "Настройка правил мониторинга" на стр. 394). Исключения задаются для каждого отдельного правила и работают только для указанной области мониторинга. Вы можете задать неограниченное количество исключений для каждого правила.

Исключения имеют более высокий приоритет, чем область мониторинга, и не контролируются задачей, даже если указанная папка или файл входят в область мониторинга. Если в параметрах одного из правил задана область мониторинга, которая является нижнеуровневой по отношению к папке, заданной в исключениях, такая область мониторинга не будет учитываться при выполнении задачи.

Для задания исключений вы можете использовать те же маски, что и для задания областей мониторинга.

О правилах мониторинга файловых операций

Задача Мониторинг файловых операций выполняется на основе правил мониторинга файловых операций. Вы можете настраивать условия срабатывания задачи и регулировать уровень важности событий для обнаруженных файловых операций, фиксируемых в журнале выполнения задачи, с помощью критериев срабатывания правила.

Правило мониторинга файловых операций задается для каждой указанной области мониторинга.

Вы можете настраивать следующие критерии срабатывания правил:

- доверенные пользователи;
- маркеры файловых операций.

Доверенные пользователи

По умолчанию действия всех пользователей расцениваются программой как потенциальные нарушения безопасности. Список доверенных пользователей пуст. Вы можете настраивать уровни важности события, формируя список доверенных пользователей в параметрах правила мониторинга файловых операций.

Недоверенный пользователь – любой пользователь, не указанный в списке доверенных в параметрах правила области мониторинга. Если Kaspersky Embedded Systems Security обнаруживает файловую операцию, выполненную недоверенным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности Критическое событие в журнале выполнения задачи.

Доверенный пользователь – пользователь или группа пользователей, которым разрешено выполнение файловых операций в указанной области мониторинга. Если Kaspersky Embedded Systems Security обнаруживает файловую операцию, выполненную доверенным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности Информационное событие в журнале выполнения задачи.

Kaspersky Embedded Systems Security не может определить пользователя, выполнившего операции в период обрыва мониторинга. В этом случае статус пользователя определяется как неизвестный.

Неизвестный пользователь – данный статус присваивается пользователю в случае, когда Kaspersky Embedded Systems Security не может получить данные о пользователе вследствие прерывания задачи или сбоя драйвера синхронизации данных или USN-журнала. Если Kaspersky Embedded Systems Security обнаруживает файловую операцию, выполненную неизвестным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности *Предупреждение* в журнале выполнения задачи.

Маркеры файловых операций

В ходе выполнения задачи Мониторинг файловых операций Kaspersky Embedded Systems Security определяет, что над файлом было произведено действие, с помощью маркеров файловых операций.

Маркер файловой операции – это единичный признак, которым может быть охарактеризована файловая операция.

Каждая файловая операция может представлять собой одно действие или цепочку действий с файлами. Каждое такое действие приравнивается к маркеру файловой операции. Если в цепочке файловой операции был обнаружен маркер, указанный вами в качестве критерия срабатывания правила мониторинга, программа зарегистрирует событие по факту совершения такой файловой операции.

Уровень важности фиксируемых событий не зависит от выбранных маркеров файловых операций или их количества.

По умолчанию Kaspersky Embedded Systems Security учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см. таблицу ниже).

Таблица 53. Маркеры файловых операций

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
BASIC_INFO_CHANGE	изменены атрибуты или метки времени файла или папки	NTFS, ReFS
COMPRESSION_CHANGE	изменено сжатие файла или папки	NTFS, ReFS
DATA_EXTEND	размер файла или папки увеличен	NTFS, ReFS
DATA_OVERWRITE	перезаписаны данные в файле или папке	NTFS, ReFS
DATA_TRUNCATION	файл или папка усечены	NTFS, ReFS
EA_CHANGE	изменены расширенные атрибуты файла или папки	только NTFS
ENCRYPTION_CHANGE	изменен статус шифрования файла или папки	NTFS, ReFS
FILE_CREATE	файл или папка созданы впервые	NTFS, ReFS
FILE_DELETE	Файл или папка удалены, минуя корзину, с помощью команды SHIFT+DEL	NTFS, ReFS
HARD_LINK_CHANGE	жесткая связь создана или удалена для файла или папки	только NTFS
INDEXABLE_CHANGE	изменен статус индексирования файла или папки	NTFS, ReFS

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
INTEGRITY_CHANGE	изменен атрибут целостности для именованного файлового потока	только ReFS
NAMED_DATA_EXTEND	размер именованного файлового потока увеличен	NTFS, ReFS
NAMED_DATA_OVERWRITE	именованный файловый поток перезаписан	NTFS, ReFS
NAMED_DATA_TRUNCATION	именованный файловый поток усечен	NTFS, ReFS
OBJECT_ID_CHANGE	изменен идентификатор файла или папки	NTFS, ReFS
RENAME_NEW_NAME	присвоено новое имя для файла или папки	NTFS, ReFS
REPARSE_POINT_CHANGE	создана новая или изменена существующая точка повторного анализа для файла или папки	NTFS, ReFS
SECURITY_CHANGE	изменены права доступа к файлу или папке	NTFS, ReFS
STREAM_CHANGE	создан новый или изменен существующий именованный файловый поток	NTFS, ReFS
TRANSACTED_CHANGE	именованный файловый поток изменен транзакцией TxF	только ReFS

Параметры по умолчанию для задачи Мониторинг файловых операций

По умолчанию в задаче Мониторинг файловых операций используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 54. Параметры по умолчанию для задачи Мониторинг файловых операций

Параметр	Значение по умолчанию	Описание
Область мониторинга	Не задано	Вы можете задать папки и файлы, действия над которыми будут отслеживаться. Для папок и файлов заданной области мониторинга будут формироваться события мониторинга.

Параметр	Значение по умолчанию	Описание
Список доверенных пользователей	Не задано	Вы можете задать пользователей и группы пользователей, действия которых в указанных папках будут расцениваться компонентом как безопасные.
Контролировать файловые операции во время простоя задачи	Применяется	Вы можете включать или выключать учет файловых операций, которые были выполнены в указанных областях мониторинга в период простоя задачи.
Исключить следующие папки из контроля	Не применяется	Вы можете контролировать применение исключений для папок, где не требуется выполнять контроль за файловыми операциями. При выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security будет пропускать области мониторинга, заданные в качестве исключений.
Расчет контрольной суммы	Не применяется	Вы можете настроить расчет контрольной суммы файла после произведенных в нем изменений.
Учитывать маркеры файловых операций	Учитываются все доступные маркеры файловых операций	Вы можете задать набор маркеров файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Embedded Systems Security формирует событие аудита.
Расписание запуска задачи	Время первого запуска не задано.	Вы можете настраивать параметры запуска задачи по расписанию.

Управление мониторингом файловых операций с помощью Плагина управления

В этом разделе описана настройка параметров задачи Мониторинг файловых операций.

В этом разделе

Настройка параметров задачи Мониторинг файловых операций

Чтобы настроить параметры задачи Мониторинг файловых операций, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Диагностика системы** в подразделе **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг файловых операций**.
5. В открывшемся окне на закладке **Параметры мониторинга файловых операций** настройте параметры области мониторинга:
   a. Снимите или установите флажок **Фиксировать информацию о файловых операциях за период обрыва мониторинга**.

      Флажок включает или выключает контроль над файловыми операциями, выбранными в параметрах задачи Мониторинг файловых операций, во время простоя задачи по любой причине (извлечение жесткого диска, остановка задачи пользователем, сбой программного обеспечения).

      Если флажок установлен, Kaspersky Embedded Systems Security будет фиксировать события во всех областях мониторинга при прерывании задачи Мониторинг файловых операций.

      Если флажок снят, при прерывании задачи файловые операции в областях мониторинга не будут фиксироваться программой.

      По умолчанию флажок установлен.

   b. Добавьте области мониторинга (см. раздел "Настройка правил мониторинга" на стр. 394), которые будет контролировать задача.
6. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Работа с расписанием задач" на стр. 130).
7. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Настройка правил мониторинга

Вы можете изменять параметры задачи Мониторинг файловых операций, заданные по умолчанию (см. таблицу ниже).

Таблица 55. Параметры по умолчанию для задачи Мониторинг файловых операций

Параметр	Значение по умолчанию	Описание
Область мониторинга	Не задано	Вы можете задать папки и файлы, действия над которыми будут отслеживаться. Для папок и файлов заданной области мониторинга будут формироваться события мониторинга.
Список доверенных пользователей	Не задано	Вы можете задать пользователей и группы пользователей, действия которых в указанных папках будут расцениваться компонентом как безопасные.
Контролировать файловые операции во время простоя задачи	Применяется	Вы можете включать или выключать учет файловых операций, которые были выполнены в указанных областях мониторинга в период простоя задачи.
Исключить следующие папки из контроля	Не применяется	Вы можете контролировать применение исключений для папок, где не требуется выполнять контроль за файловыми операциями. При выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security будет пропускать области мониторинга, заданные в качестве исключений.
Расчет контрольной суммы	Не применяется	Вы можете настроить расчет контрольной суммы файла после произведенных в нем изменений.
Учитывать маркеры файловых операций	Учитываются все доступные маркеры файловых операций	Вы можете задать набор маркеров файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Embedded Systems Security формирует событие аудита.
Расписание запуска задачи	Время первого запуска не задано.	Вы можете настраивать параметры запуска задачи по расписанию.

► *Чтобы добавить область мониторинга, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

   > Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Диагностика системы** в подразделе **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

   Откроется окно **Свойства: Мониторинг файловых операций**.

5. В блоке **Область мониторинга** нажмите на кнопку **Добавить**.

   Откроется окно **Область мониторинга**.

6. Добавьте область мониторинга одним из следующих способов:

   - Если вы хотите выбрать папки через стандартный диалог Microsoft Windows:

     a. Нажмите на кнопку **Обзор**.

        Откроется стандартное окно Microsoft Windows Обзор папок.

     b. В открывшемся окне выберите папку, файловые операции в которой вы хотите контролировать, и нажмите кнопку **ОК**.

   - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:

     - <*.ext> - все файлы с расширением <ext>, независимо от их расположения;
     - <*\name.ext> - все файлы с именем <name> и расширением <ext>, независимо от их расположения;
     - <\dir*> - все файлы в папке <\dir>;
     - <\dir*\name.ext> - все файлы с именем <name> и расширением <ext> в папке <\dir> и всех ее подпапках.

   > При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Embedded Systems Security не добавит указанную область мониторинга.

7. На закладке **Доверенные пользователи** нажмите на кнопку **Добавить**.

   Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

8. Выберите пользователей или группы пользователей, которым будут разрешены операции с файлами для выбранной области мониторинга, и нажмите кнопку **ОК**.

По умолчанию Kaspersky Embedded Systems Security считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 389), и формирует для них события с уровнем важности Критический.

9. Выберите закладку **Маркеры файловых операций**.
10. Если требуется, выберите несколько маркеров файловых операций, выполнив следующие действия:
    a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
    b. В списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 389) установите флажки напротив тех операций, которые вы хотите контролировать.

По умолчанию Kaspersky Embedded Systems Security обнаруживает все маркеры файловых операций, выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

11. Если вы хотите, чтобы программа Kaspersky Embedded Systems Security рассчитывала контрольную сумму файлов после изменений, выполните следующие действия:
    a. Установите флажок **По возможности рассчитывать контрольную сумму файла. Контрольная сумма отображается в отчете о выполнении задачи**.

       Если флажок установлен, Kaspersky Embedded Systems Security рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

       Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только финальная контрольная сумма файла после всех изменений.

       Если флажок снят, Kaspersky Embedded Systems Security не рассчитывает контрольную сумму измененных файлов.

       Расчет контрольной суммы не выполняется в следующих случаях:

       - если файл стал недоступен (например, в результате изменения прав доступа к файлу);
       - если файловая операция фиксируется для файла, который впоследствии был удален.

       По умолчанию флажок снят.

    b. В раскрывающемся списке **Рассчитывать контрольную сумму по алгоритму** выберите один из следующих элементов:

       - **Хеш MD5**
       - **Хеш SHA256**

12. Если требуется контролировать не все файловые операции, в списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 389) установите флажки напротив тех операций, которые требуется контролировать.

13. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:
    a. Выберите закладку **Исключения**.
    b. Установите флажок **Исключить следующие папки из контроля**.

       Флажок выключает применение исключений для папок, в которых не требуется мониторинг файловых операций.

       Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security пропускает области мониторинга, заданные в списке исключений.

       Если флажок снят, Kaspersky Embedded Systems Security фиксирует события для всех заданных областей мониторинга.

       По умолчанию флажок снят, список исключений пуст.
    c. Нажмите на кнопку **Добавить**.

       Откроется окно **Выберите папку для добавления**.
    d. В открывшемся окне выберите папку, которую вы хотите исключить из области мониторинга.
    e. Нажмите на кнопку **ОК**.

       Указанная папка добавится в список исключенных областей.
14. В окне **Правила мониторинга файловых операций** нажмите на кнопку **ОК**.

    Указанные параметры правил будут применяться к выбранной области мониторинга задачи Мониторинг файловых операций.

Управление мониторингом файловых операций с помощью Консоли программы

В этом разделе описана настройка параметров задачи Мониторинг файловых операций с помощью Консоли программы.

В этом разделе

Настройка параметров задачи Мониторинг файловых операций

► *Чтобы настроить параметры задачи Мониторинг файловых операций, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.

3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** снимите или установите флажок **Фиксировать информацию о файловых операциях за период обрыва мониторинга**.

   Флажок включает или выключает контроль над файловыми операциями, выбранными в параметрах задачи Мониторинг файловых операций, во время простоя задачи по любой причине (извлечение жесткого диска, остановка задачи пользователем, сбой программного обеспечения).

   Если флажок установлен, Kaspersky Embedded Systems Security будет фиксировать события во всех областях мониторинга при прерывании задачи Мониторинг файловых операций.

   Если флажок снят, при прерывании задачи файловые операции в областях мониторинга не будут фиксироваться программой.

   По умолчанию флажок установлен.

5. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 130).

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Настройка правил мониторинга

Вы можете изменять параметры задачи Мониторинг файловых операций, заданные по умолчанию (см. таблицу ниже).

Таблица 56. Параметры по умолчанию для задачи Мониторинг файловых операций

Параметр	Значение по умолчанию	Описание
Область мониторинга	Не задано	Вы можете задать папки и файлы, действия над которыми будут отслеживаться. Для папок и файлов заданной области мониторинга будут формироваться события мониторинга.
Список доверенных пользователей	Не задано	Вы можете задать пользователей и группы пользователей, действия которых в указанных папках будут расцениваться компонентом как безопасные.
Контролировать файловые операции во время простоя задачи	Применяется	Вы можете включать или выключать учет файловых операций, которые были выполнены в указанных областях мониторинга в период простоя задачи.

Параметр	Значение по умолчанию	Описание
Исключить следующие папки из контроля	Не применяется	Вы можете контролировать применение исключений для папок, где не требуется выполнять контроль за файловыми операциями. При выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security будет пропускать области мониторинга, заданные в качестве исключений.
Расчет контрольной суммы	Не применяется	Вы можете настроить расчет контрольной суммы файла после произведенных в нем изменений.
Учитывать маркеры файловых операций	Учитываются все доступные маркеры файловых операций	Вы можете задать набор маркеров файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Embedded Systems Security формирует событие аудита.
Расписание запуска задачи	Время первого запуска не задано.	Вы можете настраивать параметры запуска задачи по расписанию.

► *Чтобы добавить область мониторинга, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Правила мониторинга файловых операций**.

   Откроется окно **Мониторинг файловых операций**.
4. Добавьте область мониторинга одним из следующих способов:
   - Если вы хотите выбрать папки через стандартный диалог Microsoft Windows:
     a. В левой части окна нажмите на кнопку **Обзор**.

        Откроется стандартное окно Microsoft Windows **Обзор папок**.
     b. В открывшемся окне выберите папку, операции в которой вы хотите контролировать, и нажмите кнопку **ОК**.
     c. Нажмите кнопку **Добавить**, чтобы программа Kaspersky Embedded Systems Security начала контролировать файловые операции в указанной области мониторинга.
   - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:
     - <*.ext> - все файлы с расширением <ext>, независимо от их расположения;
     - <*\name.ext> - все файлы с именем <name> и расширением <ext>, независимо от их расположения;
     - <\dir*> - все файлы в папке <\dir>;

- <\dir*\name.ext> - все файлы с именем <name> и расширением <ext> в папке <\dir> и всех ее подпапках.

При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Embedded Systems Security не добавит указанную область мониторинга.

В правой части окна на закладке **Описание правила** отобразятся доверенные пользователи и маркеры файловых операций, выбранные для этой области мониторинга.

5. В списке добавленных областей мониторинга выберите область, для которой хотите настроить другие параметры.
6. Выберите закладку **Доверенные пользователи**.
7. Нажмите на кнопку **Добавить**.

   Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.
8. Выберите пользователей или группы пользователей, которые Kaspersky Embedded Systems Security будет считать доверенными для выбранной области мониторинга.
9. Нажмите на кнопку **OK**.

По умолчанию Kaspersky Embedded Systems Security считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 389), и формирует для них события с уровнем важности Критическое событие.

10. Выберите закладку **Маркеры файловых операций**.
11. Если требуется, выберите несколько маркеров файловых операций, выполнив следующие действия:
    a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
    b. В списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 389) установите флажки напротив тех операций, которые вы хотите контролировать.

По умолчанию Kaspersky Embedded Systems Security обнаруживает все маркеры файловых операций, выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

12. Если вы хотите, чтобы программа Kaspersky Embedded Systems Security рассчитывала контрольную сумму файлов после изменений, выполните следующие действия:
    a. В блоке **Контрольная сумма** установите флажок **Рассчитывать контрольную сумму измененного файла, если это возможно**.

       Если флажок установлен, Kaspersky Embedded Systems Security рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только финальная контрольная сумма файла после всех изменений.

Если флажок снят, Kaspersky Embedded Systems Security не рассчитывает контрольную сумму измененных файлов.

Расчет контрольной суммы не выполняется в следующих случаях:

- если файл стал недоступен (например, в результате изменения прав доступа к файлу);
- если файловая операция фиксируется для файла, который впоследствии был удален.

По умолчанию флажок снят.

b. В раскрывающемся списке **Рассчитывать контрольную сумму по алгоритму** выберите один из следующих элементов:

- **Хеш MD5**
- **Хеш SHA256**

13. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:

a. Выберите закладку **Задать исключения**.

b. Установите флажок **Учитывать исключенные области мониторинга**.

Флажок выключает применение исключений для папок, в которых не требуется мониторинг файловых операций.

Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security пропускает области мониторинга, заданные в списке исключений.

Если флажок снят, Kaspersky Embedded Systems Security фиксирует события для всех заданных областей мониторинга.

По умолчанию флажок снят, список исключений пуст.

c. Нажмите на кнопку **Обзор**.

Откроется стандартное окно Microsoft Windows **Обзор папок**.

d. В открывшемся окне выберите папку, которую вы хотите исключить из области мониторинга.

e. Нажмите на кнопку **OK**.

f. Нажмите на кнопку **Добавить**.

Указанная папка добавится в список исключенных областей.

> Вы также можете добавить исключения для области мониторинга вручную используя те же маски, что и для задания областей мониторинга.

14. Нажмите на кнопку **Сохранить**, чтобы применить новые параметры правил.

Анализ журналов

Этот раздел содержит информацию о задаче Анализ журналов и параметрах задачи.

В этом разделе

О задаче Анализ журналов

В ходе выполнения задачи Анализ журналов Kaspersky Embedded Systems Security контролирует целостность защищаемой среды на основе результатов анализа журналов событий Windows. Программа информирует администратора при обнаружении признаков нетипичного поведения в системе, которые могут свидетельствовать о попытках кибератак.

Kaspersky Embedded Systems Security считывает данные журналов событий Windows и определяет нарушения в соответствии с правилами, заданными пользователем или параметрами эвристического анализатора, который применяется задачей для анализа журналов.

Стандартные правила и эвристический анализ

Вы можете использовать задачу Анализ журналов для контроля состояния защищаемой системы с помощью стандартных правил, осуществляющих анализ на основе встроенных эвристик. Эвристический анализатор определяет наличие аномальной активности на защищаемом компьютере, что может свидетельствовать о попытке атаки. Шаблоны определения аномальной активности заложены в доступных правилах в параметрах задачи.

Для задачи Анализ журналов доступно семь стандартных правил. Вы можете включать и выключать применение любого правила. Вы не можете удалять существующие или создавать новые правила.

Вы можете настроить критерии срабатывания правил, которые контролируют события для следующих операций:

- обработка подбора пароля;
- обработка сетевого входа.

В параметрах задачи вы также можете настроить исключения. Эвристический анализатор не срабатывает, если вход в систему выполнен доверенным пользователем или с доверенного IP-адреса.

Kaspersky Embedded Systems Security не применяет эвристики для анализа журналов Windows, если эвристический анализатор не используется задачей. По умолчанию эвристический анализатор включен.

При срабатывании правила, программа фиксирует событие с уровнем важности *Критическое* в журнале выполнения задачи Анализ журналов.

Пользовательские правила задачи Анализ журналов

С помощью параметров правил задачи вы можете задавать и изменять критерии срабатывания правила при обнаружении выбранных событий в указанном журнале Windows. По умолчанию список правил задачи Анализ журналов содержит четыре правила. Вы можете включать и выключать применение данных правил, удалять правила и редактировать их параметры.

Вы можете настроить следующие критерии срабатывания каждого правила:

- Список идентификаторов записей в журнале событий Windows.

  Правило срабатывает при появлении новой записи в журнале событий Windows, если в параметрах события обнаружен идентификатор события, указанный для правила. Вы также можете добавлять и удалять идентификаторы для каждого заданного правила.

- Источник событий.

  Для каждого правила вы можете задать поджурнал журнала событий Windows. Программа будет выполнять поиск записей с указанными идентификаторами событий только в этом поджурнале. Вы можете выбрать один из стандартных поджурналов (Программа, Безопасность или Система), а также указать пользовательский поджурнал, указав его имя в поле выбора источника.

  > Программа не выполняет проверок на фактическое наличие заданного поджурнала в журнале событий Windows.

При срабатывании правила Kaspersky Embedded Systems Security фиксирует событие с уровнем важности Критическое событие в журнале выполнения задачи Анализ журналов.

По умолчанию в задаче Анализ журналов учитываются пользовательские правила.

> Перед запуском задачи Анализ журналов убедитесь, что политика аудита системы настроена верно. Более подробную информацию можно найти в статье Microsoft https://technet.microsoft.com/ru-ru/library/cc952128.aspx.

Параметры по умолчанию для задачи Анализ журналов

По умолчанию в задаче Анализ журналов используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 57. Параметры по умолчанию для задачи Мониторинг файловых операций

Параметр	Значение по умолчанию	Описание
Применять пользовательские правила для анализа журналов	Применяется.	Пользовательские правила можно включать, отключать, добавлять или изменять.

Параметр	Значение по умолчанию	Описание
Использовать стандартные правила для анализа журналов	Применяется.	Можно включить или отключить эвристический анализатор, отвечающий за обнаружение аномальной активности на защищаемом сервере.
Обработка перебора пароля	10 неудачных попыток входа в течение 300 секунд.	Можно указать количество попыток и промежуток времени, в течение которого выполнялись попытки, которые будут являться критериями срабатывания эвристического анализатора.
Обработка сетевого входа	00:00:00.	Можно указать начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Embedded Systems Security расценивает данное действие как аномальную активность.
Исключения	Не применяется.	Можно указать пользователей и IP-адреса, которые не будут являться критериями срабатывания эвристического анализатора.
Расписание запуска задачи	Первый запуск не определен.	Вы можете настраивать параметры запуска задачи по расписанию.

Управление правилами анализа журналов с помощью Плагина управления

В этом разделе описано добавление и настройка правил анализа журналов с помощью Плагина управления.

В этом разделе

Управление стандартными правилами задачи с помощью Плагина управления

► *Чтобы настроить параметры стандартных правил для задачи Анализ журналов, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
   - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

   Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Мониторинг целостности системы** в блоке **Анализ журналов** нажмите на кнопку **Настройка**.

   Откроется окно **Анализ журналов**.
5. Выберите закладку **Стандартные правила**.
6. Снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security применяет эвристический анализатор для обнаружения аномальной активности на защищаемом компьютере.

   Если этот флажок не установлен, то эвристический анализатор выключен, и Kaspersky Embedded Systems Security использует стандартные или пользовательские правила для обнаружения аномальной активности.

   По умолчанию флажок установлен.

   Для выполнения задачи должно быть выбрано хотя бы одно правило анализа журналов.
7. Из списка стандартных правил, выберите правила, которые вы хотите применять для анализа журналов:
   - Обнаружена возможная попытка взлома пароля с помощью подбора.
   - Обнаружены признаки компрометации журналов Windows.
   - Обнаружена подозрительная активность со стороны новой установленной службы.
   - Обнаружена подозрительная аутентификация с явным указанием учетных данных.
   - Обнаружены признаки атаки Kerberos forged PAC (MS14-068).
   - Обнаружены подозрительные изменения привилегированной группы Администраторы.
   - Обнаружена подозрительная активность во время сетевого сеанса входа.
8. Чтобы настроить параметры выбранных правил, нажмите на кнопку **Дополнительные параметры**.

   Откроется окно **Анализ журналов**.

9. В блоке **Обработка перебора пароля** укажите количество попыток и промежуток времени, в который выполнялись попытки, которые будут являться критериями срабатывания эвристического анализатора.
10. В блоке **Обработка атипичной аутентификации** укажите начало и конец временного интервала, при выполнении попытки входа в который Kaspersky Embedded Systems Security расценивает данное действие как аномальную активность.
11. Выберите закладку **Исключения**.
12. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
    a. Нажмите на кнопку **Обзор**.
    b. Выберите пользователя.
    c. Нажмите на кнопку **ОК**.

    Указанный пользователь добавится в список доверенных.
13. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:
    a. Введите IP-адрес.
    b. Нажмите на кнопку **Добавить**.
14. Указанный IP-адрес добавится в список доверенных.
15. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Настройка расписания запуска задач" на стр. 130).
16. Нажмите на кнопку **ОК**.

Параметры задачи Анализ журналов будут сохранены.

Добавление правил анализа журналов с помощью Плагина управления

► *Чтобы добавить и настроить новое пользовательское правило анализа журналов, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
    - Чтобы настроить параметры программы для группы компьютеров, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** (см. раздел "Настройка политики" на стр. 115).
    - Чтобы настроить параметры программы для отдельного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. 119).

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Мониторинг целостности системы** в блоке **Анализ журналов** нажмите на кнопку **Настройка**.

   Откроется окно **Анализ журналов**.

5. На закладке **Пользовательские правила** снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security применяет пользовательские правила для анализа журналов в соответствии с настроенными параметрами каждого правила. Вы можете добавлять, удалять или изменять правила анализа журналов.

   Если флажок снят, нельзя добавлять или изменять пользовательские правила. Kaspersky Embedded Systems Security применяет параметры правил по умолчанию.

   По умолчанию флажок установлен. Активно только правило Обнаружено всплывающее окно приложения.

Вы можете контролировать применение стандартных правил для анализа журналов. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

6. Чтобы добавить новое пользовательское правило, нажмите на кнопку **Добавить**.

   Откроется окно **Правила анализа журналов**.

7. В блоке **Общие** введите следующие данные нового правила:

   - **Имя правила**
   - **Источник**

     Выберите журнал, события которого будут использоваться для анализа. Доступны следующие виды журналов событий Windows:

     - журнал приложений;
     - журнал безопасности;
     - системный журнал.

     Вы можете добавить новый пользовательский журнал, указав имя журнала в поле **Источник**.

8. В блоке **Параметры срабатывания** укажите идентификаторы записей, при обнаружении которых будет срабатывать правило:

   a. Введите числовое значение идентификатора.

   b. Нажмите на кнопку **Добавить**.

      Указанный идентификатор правила добавится в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.

   c. Нажмите на кнопку **OK**.

   Правило анализа журналов добавится в общий список правил.

Управление правилами анализа журналов с помощью Консоли программы

В этом разделе описано добавление и настройка правил анализа журналов с помощью Консоли программы.

В этом разделе

Управление стандартными правилами задачи с помощью Консоли программы

► *Чтобы настроить параметры работы эвристического анализатора для задачи Анализ журналов, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Выберите закладку **Стандартные правила**.
5. Снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security применяет эвристический анализатор для обнаружения аномальной активности на защищаемом компьютере.

   Если этот флажок не установлен, то эвристический анализатор выключен, и Kaspersky Embedded Systems Security использует стандартные или пользовательские правила для обнаружения аномальной активности.

   По умолчанию флажок установлен.

   Для выполнения задачи должно быть выбрано хотя бы одно правило анализа журналов.
6. Из списка стандартных правил, выберите правила, которые вы хотите применять для анализа журналов:
   - Обнаружена возможная попытка взлома пароля с помощью подбора.
   - Обнаружены признаки компрометации журналов Windows.
   - Обнаружена подозрительная активность со стороны новой установленной службы.
   - Обнаружена подозрительная аутентификация с явным указанием учетных данных.
   - Обнаружены признаки атаки Kerberos forged PAC (MS14-068).
   - Обнаружены подозрительные изменения привилегированной группы Администраторы.

- Обнаружена подозрительная активность во время сетевого сеанса входа.

7. Чтобы настроить параметры выбранных правил, выберите закладку **Расширенные**.
8. В блоке **Обработка перебора пароля** укажите количество попыток и промежуток времени, в который выполнялись попытки, которые будут являться критериями срабатывания эвристического анализатора.
9. В блоке **Обработка сетевого входа** укажите начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Embedded Systems Security расценивает данное действие как аномальную активность.
10. Выберите закладку **Исключения**.
11. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
    a. Нажмите на кнопку **Обзор**.
    b. Выберите пользователя.
    c. Нажмите на кнопку **OK**.

    Указанный пользователь добавится в список доверенных.
12. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:
    a. Введите IP-адрес.
    b. Нажмите на кнопку **Добавить**.

    Указанный IP-адрес добавится в список доверенных.
13. Выберите закладки **Расписание** и **Дополнительно**, чтобы настроить параметры расписания запуска задачи.
14. Нажмите на кнопку **OK**.

    Параметры задачи Анализ журналов будут сохранены.

Настройка правил анализа журналов

Чтобы добавить и настроить новое пользовательское правило анализа журналов, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Правила анализа журналов**.

   Откроется окно **Правила анализа журналов**.
4. Снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security применяет пользовательские правила для анализа журналов в соответствии с настроенными параметрами каждого правила. Вы можете добавлять, удалять или изменять правила анализа журналов.

   Если флажок снят, нельзя добавлять или изменять пользовательские правила.

Kaspersky Embedded Systems Security применяет параметры правил по умолчанию.

По умолчанию флажок установлен. Активно только правило Обнаружено всплывающее окно приложения.

Вы можете контролировать применение стандартных правил в задаче Анализ журналов. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

5. Чтобы создать новое пользовательское правило, выполните следующие действия:
   a. Введите имя нового правила.
   b. Нажмите на кнопку **Добавить**.

      Созданное правило добавится в общий список правил.
6. Чтобы настроить любое правило, выполните следующие действия:
   a. Выберите правило в списке нажатием левой кнопкой мыши.

      В правой области окна на закладке **Комментарий** отобразится общая информация о правиле.

      Комментарии для нового правила пусты.

   b. Выберите закладку **Параметры правила**.
   c. В блоке **Общие отредактируйте Имя** правила, если требуется.
   d. Выберите **Источник**.
7. В блоке **Идентификаторы событий** укажите идентификаторы записей, при обнаружении которых будет срабатывать правило:
   a. Введите числовое значение идентификатора.
   b. Нажмите на кнопку **Добавить**.

      Указанный идентификатор правила добавится в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.
   c. Нажмите на кнопку **Сохранить**.

      Настроенные параметры правил анализа журналов будут применены.

Проверка по требованию

Этот раздел содержит информацию о задачах проверки по требованию, а также инструкции по настройке параметров задач проверки по требованию и параметров безопасности защищаемого компьютера.

В этом разделе

О задачах проверки по требованию

Kaspersky Embedded Systems Security проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Kaspersky Embedded Systems Security проверяет файлы и оперативную память компьютера, а также объекты автозапуска.

В Kaspersky Embedded Systems Security предусмотрены следующие системные задачи проверки по требованию:

- Задача Проверка при старте операционной системы выполняется каждый раз при запуске Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security проверяет загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Каждый раз при запуске задачи Kaspersky Embedded Systems Security создает копию незараженных загрузочных секторов. Если при следующем запуске задачи в этих секторах обнаруживается угроза, программа заменяет возможно зараженный сектор резервной копией.
- По умолчанию задача Проверка важных областей выполняется еженедельно по расписанию. Kaspersky Embedded Systems Security проверяет объекты, расположенные в важных областях операционной системы: объекты автозапуска, загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Программа проверяет файлы, которые содержатся в системных папках, например, в папке %windir%\system32. Kaspersky Embedded Systems Security применяет параметры безопасности, значения которых соответствуют уровню Рекомендуемый (см. раздел "О стандартных уровнях безопасности в задачах проверки по требованию" на стр. 416). Вы можете изменять параметры задачи Проверка важных областей.

- Задача Проверка объектов на карантине по умолчанию выполняется по расписанию после каждого обновления баз программы. Область действия задачи Проверка объектов на карантине изменять нельзя.
- Задача Проверка целостности программы выполняется ежедневно. Она обеспечивает проверку модулей Kaspersky Embedded Systems Security на предмет наличия повреждений или изменений. Проверяется папка установки программы. Статистика выполнения задачи содержит сведения о количестве проверенных и поврежденных модулей. Значения параметров задачи устанавливаются по умолчанию и не доступны для изменения. Вы можете настраивать расписание запуска задачи.

Кроме того, вы можете создать пользовательские задачи проверки по требованию, например, задачу проверки папок общего доступа на компьютере.

Kaspersky Embedded Systems Security может одновременно выполнять несколько задач проверки по требованию.

Об области проверки

Вы можете настроить область проверки для задач Проверка при старте операционной системы и Проверка важных областей, а также для пользовательских задач проверки по требованию.

По умолчанию задачи проверки по требованию проверяют все объекты файловой системы компьютера. Если по требованиям к безопасности нет необходимости проверять все объекты файловой системы, вы можете ограничить область проверки.

В Консоли программы область проверки представляет собой дерево или список файловых ресурсов компьютера, которые может контролировать Kaspersky Embedded Systems Security. По умолчанию сетевые файловые ресурсы защищаемого компьютера отображаются в виде списка.

► *Чтобы включить отображение сетевых файловых ресурсов в виде дерева,*

в раскрывающемся списке, расположенном в левом верхнем углу окна **Настройка области проверки**, выберите элемент **Показывать в виде дерева**.

Узлы в дереве или списке файловых ресурсов компьютера отображаются следующим образом:

☑ Узел включен в область проверки.

☐ Узел исключен из области проверки.

☑ – по крайней мере один из узлов, вложенных в этот узел, исключен из области проверки, или параметры безопасности вложенных узлов отличаются от параметров безопасности этого узла (только для режима отображения в виде дерева).

Значок ☑ отображается, если выбраны все вложенные узлы, но не выбран родительский узел. В этом случае изменения состава файлов и папок родительского узла не учитываются автоматически при изменении области проверки для выбранного вложенного узла.

Имена виртуальных узлов области проверки отображаются шрифтом синего цвета.

Стандартные области проверки

Дерево или список файловых ресурсов компьютера для выбранной задачи проверки по требованию отображается на закладке **Настройка области проверки**.

Дерево или список файловых ресурсов отображает узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Embedded Systems Security предусмотрены следующие стандартные области проверки:

- **Мой компьютер**. Kaspersky Embedded Systems Security проверяет весь компьютер.
- **Локальные жесткие диски**. Kaspersky Embedded Systems Security проверяет объекты на жестких дисках компьютера. Вы можете включать в область проверки или исключать из нее все жесткие диски, а также отдельные диски, папки или файлы.
- **Съемные диски**. Kaspersky Embedded Systems Security проверяет файлы на внешних устройствах, например, на компакт-дисках или съемных дисках. Вы можете включать в область проверки или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.
- **Сетевое окружение**. Вы можете добавлять в область проверки сетевые папки или файлы, указывая пути к ним в формате UNC (Universal Naming Convention). Учетная запись, которую вы используете для запуска задачи, должна обладать правами доступа к добавленным сетевым папкам или файлам. По умолчанию задачи проверки по требованию выполняются под системной учетной записью.

  Подключенные сетевые диски также не отображаются в дереве файловых ресурсов компьютера. Чтобы включить в область проверки объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

- **Системная память**. Kaspersky Embedded Systems Security проверяет исполняемые файлы и модули процессов, которые выполняются в операционной системе на момент проверки.
- **Объекты автозапуска**. Kaspersky Embedded Systems Security проверяет объекты, на которые ссылаются ключи реестра и конфигурационные файлы, например, WIN.INI или SYSTEM.INI, INI, а также программные модули, которые автоматически запускаются при запуске компьютера.
- **Папки общего доступа**. Вы можете включать в область проверки папки общего доступа на защищаемом компьютере.
- **Виртуальные диски**. Вы можете включать в область проверки динамические папки и файлы, а также диски, которые подключены к компьютеру, например, общие диски кластера.

  Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов компьютера в Консоли программы. Чтобы проверить объекты на виртуальном диске, включите в область проверки папку на компьютере, с которой связан этот виртуальный диск.

Стандартные области проверки по умолчанию отображаются в дереве сетевых файловых ресурсов и доступны для добавления в список сетевых файловых ресурсов при его формировании в параметрах области проверки.

По умолчанию задачи проверки по требованию выполняются в следующих областях:

- Задача Проверка при старте операционной системы:
  - **Локальные жесткие диски**
  - **Съемные диски**
  - **Системная память**
- Задача Проверка важных областей:
  - **Локальные жесткие диски** (исключая папки Windows)
  - **Съемные диски**
  - **Системная память**
  - **Объекты автозапуска**
- Прочие задачи:
  - **Локальные жесткие диски** (исключая папки Windows)
  - **Съемные диски**
  - **Системная память**
  - **Объекты автозапуска**
  - **Папки общего доступа**

Проверка файлов в облачном хранилище

Об облачных файлах

Kaspersky Embedded Systems Security может взаимодействовать с облачными файлами Microsoft OneDrive. Программа поддерживает новую функцию "файлы OneDrive по запросу" (OneDrive Files On-Demand).

Kaspersky Embedded Systems Security не поддерживает другие облачные хранилища.

Функция "файлы OneDrive по запросу" помогает вам получить доступ к вашим файлам в OneDrive без необходимости загружать все файлы и занимать дисковое пространство на вашем устройстве. При необходимости можно загрузить файлы на жесткий диск вашего устройства.

Когда функция "файлы OneDrive по запросу" включена, рядом с каждым файлом в графе **Статус** в проводнике Windows отображается значок статуса. Файл может иметь один из следующих статусов:

– этот значок показывает, что файл *доступен только через интернет*. Файлы, доступные только через интернет, не хранятся физически на жестком диске. Если ваше устройство не подключено к интернету, вы не сможете открывать файлы, доступные только через интернет.

– этот значок показывает, что файл *доступен локально*. Он отображается, если вы открыли файл, доступный только через интернет, и он загрузился на ваше устройство. Доступные локально файлы можно открывать в любое время, даже без доступа в интернет. Чтобы освободить пространство, вы можете снова сделать файл доступным только через интернет ( ).

– этот значок показывает, что файл *хранится на жестком диске и всегда доступен*.

Проверка облачных файлов

Kaspersky Embedded Systems Security может выполнять проверку только облачных файлов, сохраненных локально на защищаемом компьютере. Такие файлы OneDrive имеют статус или . Проверка файлов со статусом не выполняется, поскольку физически они не хранятся на защищаемом компьютере.

> Во время проверки Kaspersky Embedded Systems Security не выполняет автоматическую загрузку файлов со статусом из облачного хранилища, даже если они включены в область проверки.

Обработка облачных файлов выполняется различными задачами Kaspersky Embedded Systems Security в различных сценариях, в зависимости от типа задачи:

- Постоянная проверка облачных файлов: вы можете добавить папки, содержащие облачные файлы, в область защиты задачи Постоянная защита файлов. Проверка файла выполняется, когда пользователь открывает его. Если пользователь открывает файл со статусом , этот файл загружается и становится доступным локально; его статус меняется на . Поэтому этот файл может быть обработан задачей Постоянная защита файлов.
- Проверка облачных файлов по требованию: вы можете добавить папки, содержащие облачные файлы, в область проверки задачи проверки по требованию. Задача выполняет проверку файлов со статусами и . Если в области проверки задачи обнаружены файлы со статусом , эти файлы будут пропущены при проверке, а в журнале выполнения задачи будет зарегистрировано информационное событие, показывающее, что проверяемый файл является временной заменой облачного файла и отсутствует на локальном диске.
- Формирование и использование правил контроля запуска программ: можно создавать разрешающие и запрещающие правила для файлов со статусами и с помощью задачи Формирование правил контроля запуска программ. Задача Контроль запуска программ обрабатывает и блокирует облачные файлы в соответствии с принципом запрета по умолчанию и созданными правилами.

  > Задача Контроль запуска программ блокирует запуск всех облачных файлов, независимо от статуса файла. Файлы со статусом не входят в область формирования правила, поскольку они не хранятся физически на жестком диске. Для таких файлов невозможно создать разрешающих правил, поэтому они подчиняются принципу запрета по умолчанию.

Если в облачном файле OneDrive обнаружена угроза, программа применяет действие, указанное в параметрах задачи, выполняющей проверку. Таким образом, файл может быть удален, вылечен, помещен на карантин или в резервное хранилище.

> При изменении локальные файлы синхронизируются с копиями в облачном хранилище OneDrive в соответствии с принципами, описанными в документации к Microsoft OneDrive.

Параметры безопасности выбранного узла в задачах проверки по требованию

В выбранной задаче проверки по требованию можно изменять заданные по умолчанию значения параметров безопасности, настроив их либо едиными для всей области защиты или проверки, либо различными для разных узлов или элементов в дереве или списке файловых ресурсов компьютера.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются ко всем вложенным узлам. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты или проверки одним из следующих способов:

- выбрать один из трех стандартных уровней безопасности (**Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**);
- вручную изменить параметры безопасности для выбранных узлов или элементов в дереве или списке файловых ресурсов компьютера (уровень безопасности примет значение **Другой**).

Вы можете сохранить набор параметров узла в шаблон, чтобы потом применять этот шаблон для других узлов.

О стандартных уровнях безопасности в задачах проверки по требованию

Параметры безопасности: **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов** – не входят в набор параметров стандартных уровней безопасности. Если вы измените состояние параметров **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов**, выбранный вами стандартный уровень безопасности не изменится.

Для выбранного узла в дереве файловых ресурсов можно задать один из трех стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**. Каждый из этих уровней имеет свой стандартный набор параметров безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, помимо использования Kaspersky Embedded Systems Security на компьютерах, применяются дополнительные меры компьютерной безопасности, например, сетевые экраны и политики безопасности.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых компьютеров. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты компьютеров в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если предъявляются повышенные требования к безопасности в сети организации.

Таблица 58. Стандартные уровни безопасности и соответствующие им значения параметров безопасности

Параметры	Уровень безопасности		
	Максимальное быстродействие	Рекомендуемый	Максимальная защита
Проверка объектов	По формату	Все объекты	Все объекты
Проверка только новых и измененных файлов	Включена	Выключено	Выключено
Действия над зараженными и другими обнаруженными объектами	Лечить. Удалить, если не удалось вылечить.	Выполнять рекомендованное действие (Лечить. Удалить, если не удалось вылечить.)	Лечить. Удалить, если не удалось вылечить.
Действия над возможно зараженными объектами	Карантин	Выполнять рекомендованное действие (Поместить на карантин)	Карантин
Исключать файлы	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.)	60 сек.	Нет	Нет
Не проверять составные объекты размером более (МБ)	8 МБ	Нет	Нет
Альтернативные потоки NTFS	Да	Да	Да
Загрузочные секторы дисков и MBR	Да	Да	Да

Параметры	Уровень безопасности		
Проверка составных объектов	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Только новые и измененные	• Архивы* • SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Все объекты	• Архивы* • SFX-архивы* • Почтовые базы* • Файлы почтовых форматов* • Упакованные объекты* • Вложенные OLE-объекты* * Все объекты

Проверка съемных дисков

Вы можете настроить проверку съемных дисков, подключаемых к защищаемому компьютеру по USB.

Kaspersky Embedded Systems Security выполняет проверку съемного диска с помощью задачи проверки по требованию. Программа автоматически создает новую задачу проверки по требованию в момент подключения съемного диска и удаляет созданную задачу по завершении проверки. Созданная задача выполняется со стандартным уровнем безопасности, указанным для проверки съемных дисков. Вы не можете настроить параметры временной задачи проверки по требованию.

Если программа Kaspersky Embedded Systems Security была установлена без антивирусных баз, проверка съемных дисков будет недоступна.

Kaspersky Embedded Systems Security выполняет проверку съемного диска с помощью задачи проверки по требованию. Программа автоматически создает новую задачу проверки по требованию в момент подключения съемного диска и удаляет созданную задачу по завершении проверки. Созданная задача выполняется со стандартным уровнем безопасности, указанным для проверки съемных дисков. Вы не можете настроить параметры временной задачи проверки по требованию.

Kaspersky Embedded Systems Security запускает проверку съёмных дисков, подключаемых по USB при их регистрации в операционной системе в качестве запоминающего устройства (USB Mass Storage Device). Программа не выполняет проверку съемного диска, если его подключение было заблокировано задачей Контроль устройств. Программа не выполняет проверку MTP-подключаемых мобильных устройств.

Kaspersky Embedded Systems Security не блокирует доступ к съёмному диску на время проверки.

Результаты проверки каждого съемного диска доступны в журнале выполнения задачи проверки по требованию, созданной при подключении этого съемного диска.

Вы можете изменять значения параметров компонента Проверка съемных дисков (см. таблицу ниже).

Таблица 59. Параметры проверки съемных дисков

Параметр	Значение по умолчанию	Описание
Проверять съемные диски при их подключении по USB	Флажок снят	Вы можете включать или выключать проверку съемных дисков при их подключении к защищаемому компьютеру.
Проверять, если объем содержащихся на диске данных не превышает порог (МБ)	1024 МБ	Вы можете уменьшить область срабатывания компонента, указав максимальный объем данных на съёмном диске. Kaspersky Embedded Systems Security не будет выполнять проверку съемного диска, если объем содержащихся на нем данных превышает указанное значение.
Запускать проверку с уровнем безопасности	Максимальная защита	Вы можете настраивать параметры создаваемых задач проверки по требованию, выбирая один из трех уровней безопасности: • **Максимальная защита** • **Рекомендуемый** • **Максимальное быстродействие** Алгоритм действий при обнаружении зараженных, возможно зараженных и других объектов, а также другие параметры проверки для каждого уровня безопасности соответствуют стандартным уровням безопасности в задачах проверки по требованию.

Заданные по умолчанию параметры задач проверки по требованию

По умолчанию задачи проверки по требованию имеют параметры, описанные в таблице ниже. Вы можете настраивать системные и пользовательские задачи проверки по требованию.

Таблица 60. Заданные по умолчанию параметры задач проверки по требованию

Параметр	Значение	Описание
Область проверки	Применяется в системных и пользовательских задачах: • **Проверка при старте операционной системы**: весь сервер, исключая папки общего доступа и объекты автозапуска. • **Проверка важных областей**: весь сервер, за исключением папок общего доступа и некоторых файлов операционной системы. • Пользовательские задачи проверки по требованию: весь сервер.	Вы можете изменить область проверки. Область проверки нельзя настроить для системных задач **Проверка объектов на карантине** и **Проверка целостности программы**.
Параметры безопасности	Единые для всей области проверки, соответствуют уровню безопасности **Рекомендуемый**.	Для выбранных узлов в дереве или списке файловых ресурсов компьютера вы можете выполнить следующие действия: • выбрать другой стандартный уровень безопасности; • вручную изменить параметры безопасности. Вы можете сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применить его для любого другого узла.
Использовать эвристический анализатор	Применяется с уровнем анализа **Средний** для задач Проверка важных областей и Проверка при старте операционной системы, а также для пользовательских задач. Применяется с уровнем анализа **Глубокий** для задачи Проверка объектов на карантине.	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа. Вы не можете настроить уровень анализа для задачи Проверка объектов на карантине. Применение эвристического анализатора в задаче Проверка целостности программы не предусматривается.
Применять доверенную зону	Применяется (не применяется для задачи Проверка объектов на карантине)	Единый список исключений, который вы можете применять в выбранных задачах.

Параметр	Значение	Описание
Использовать KSN для проверки	Применяется.	Вы можете увеличить эффективность защиты сервера с помощью использования инфраструктуры облачных служб Kaspersky Security Network.
Параметры запуска задачи с правами	Задача запускается с правами системной учетной записи.	Вы можете изменять параметры запуска с правами учетных записей для всех системных и пользовательских задач проверки по требованию, кроме задач Проверка объектов на карантине и Проверка целостности программы.
Выполнять задачу в фоновом режиме (низкий приоритет)	Не применяется	Вы можете настраивать приоритетность выполнения задач проверки по требованию.
Расписание запуска задачи	Применяется в системных задачах: • Проверка при старте операционной системы – **При запуске программы**; • Проверка важных областей – **Еженедельно**; • Проверка объектов на карантине – **После обновления баз программы**; • Проверка целостности программы – **Ежесуточно**. Не применяется во вновь созданных пользовательских задачах.	Вы можете настраивать параметры запуска задачи по расписанию.
Регистрация выполнения проверки и обновление статуса защиты сервера	Статус защиты сервера обновляется еженедельно после выполнения задачи Проверка важных областей.	Вы можете настраивать параметры регистрации выполнения проверки важных областей следующими способами: • изменяя параметры расписания запуска задачи Проверка важных областей; • изменяя область проверки задачи Проверка важных областей; • создавая пользовательские задачи проверки по требованию.

Управление задачами проверки по требованию с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для одного или всех компьютеров сети.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

В этом разделе

Переход к мастеру создания задачи проверки по требованию

► *Чтобы создать пользовательскую задачу проверки по требованию, выполните следующие действия:*

1. Для создания локальной задачи:
   a. Разверните узел **Управляемые устройства** в Консоли администрирования Kaspersky Security Center.
   b. Выберите группу администрирования, к которой принадлежит компьютер.
   c. В панели результатов на закладке **Устройства** откройте контекстное меню защищаемого сервера.
   d. Выберите пункт меню **Свойства**.
   e. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.

   Откроется окно **Мастер создания задачи**.
2. Для создания групповой задачи:
   a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

b. Выберите группу администрирования, для которой требуется создать задачу.

c. Выберите закладку **Задачи**.

d. Нажмите на кнопку **Создать задачу**.

Откроется окно **Мастер создания задачи**.

3. Чтобы создать задачу для произвольного набора компьютеров, выполните следующие действия:

a. В Консоли администрирования Kaspersky Security Center в панели результатов узла **Выборки устройств** нажмите на кнопку **Запустить выборку**, чтобы выбрать устройства.

b. Выберите закладку **Результаты выборки "имя выборки"**.

c. В раскрывающемся списке **Сделать выборку** выберите вариант **Создать задачу для результатов выборки**.

Откроется окно **Мастер создания задачи**.

4. Выберите задачу **Проверка по требованию** в списке доступных задач для Kaspersky Embedded Systems Security.

5. Нажмите на кнопку **Далее**.

Откроется окно **Настройка**.

Настройте параметры задачи в соответствии с вашими требованиями.

► *Чтобы настроить задачу проверки по требованию,*

откройте окно свойств задачи двойным щелчком мыши на названии задачи в списке задач Kaspersky Security Center.

Откроется окно **Свойства: Проверка по требованию**.

Переход к свойствам задачи проверки по требованию

► *Чтобы перейти к свойствам программы для задачи проверки по требованию на отдельном компьютере, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, к которой принадлежит защищаемый компьютер.
3. Выберите закладку **Устройства**.
4. Дважды щелкните мышью по имени компьютера, для которого требуется настроить область проверки.

Откроется окно **Свойства: <Имя компьютера>**.

5. Выберите раздел **Задачи**.
6. В списке задач, созданных для устройства, выберите созданную задачу проверки по требованию.
7. Нажмите на кнопку **Свойства**.

Откроется окно **Свойства: Проверка по требованию**.

Настройте параметры задачи в соответствии с вашими требованиями.

Создание задачи проверки по требованию

► *Чтобы создать пользовательскую задачу проверки по требованию, выполните следующие действия:*

1. Откройте окно **Настройка** (см. раздел "**Переход к мастеру создания задачи проверки по требованию**" на стр. 422) в мастере создания задачи.
2. Выберите требуемый **Способ создания задачи**.
3. Нажмите на кнопку **Далее**.
4. В окне **Область проверки** сформируйте область проверки.

   По умолчанию область проверки включает критические области компьютера. Проверяемые области помечены в таблице значком ☑. Области, являющиеся исключениями из проверки, помечены в таблице значком ☐.
   Вы можете изменять область проверки: включать в нее отдельные стандартные области, диски, папки, сетевые объекты и файлы и устанавливать особые параметры безопасности для каждой из добавленных областей.

   - Чтобы исключить из проверки все важные области, откройте контекстное меню на каждой из строк и выберите **Удалить область**.
   - Чтобы включить стандартную область проверки, диск, папку, сетевой объект или файл в область проверки, выполните следующие действия:
     a. Откройте контекстное меню таблицы **Область проверки** и выберите **Добавить область** или нажмите на кнопку **Добавить**.
     b. В окне **Добавление в область проверки** выберите стандартную область в списке **Предопределенная область**, укажите диск компьютера, папку, сетевой объект или файл на этом или другом компьютере в сети и нажмите на кнопку **ОК**.
   - Чтобы исключить вложенные папки или файлы из области проверки, выберите добавленную папку (диск) в окне мастера **Область проверки**:
     a. Откройте контекстное меню и выберите пункт **Настроить**.
     b. Нажмите на кнопку **Настройка** в окне **Уровень безопасности**.
     c. На закладке **Общие** в окне **Настройка проверки по требованию** снимите флажки **Вложенные папки** и **Вложенные файлы**.
   - Чтобы изменить параметры безопасности области проверки, выполните следующие действия:
     a. Откройте контекстное меню области проверки, параметры которой требуется изменить, и выберите пункт **Настроить**.
     b. В окне **Настройка проверки по требованию** выберите один из стандартных уровней безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры безопасности вручную.

     Параметры безопасности настраиваются таким же образом, как и для задачи Постоянная защита файлов (см. раздел "Настройка параметров безопасности вручную" на стр. 255).

- Чтобы пропускать вложенные объекты в добавленной области проверки, выполните следующие действия:

  a. Откройте контекстное меню таблицы **Область проверки** и выберите пункт **Добавить исключение**.

  b. Укажите объекты, которые вы хотите исключить: выберите стандартную область в списке **Предопределенная область**, укажите диск компьютера, папку, сетевой объект или файл на этом или другом компьютере сети.

  c. Нажмите на кнопку **ОК**.

5. В окне **Параметры** настройте эвристический анализатор и интеграцию с другими компонентами:

   - Настройте использование эвристического анализатора (см. раздел "Настройка эвристического анализатора и интеграции с другими компонентами программы" на стр. 251).
   - Установите флажок **Применять доверенную зону**, если вы хотите исключить из области проверки задачи объекты, входящие в доверенную зону.

     Флажок включает или выключает применение доверенной зоны в работе задачи.

     Если флажок установлен, Kaspersky Embedded Systems Security добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

     Если флажок снят, Kaspersky Embedded Systems Security не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

     По умолчанию флажок установлен.

   - Установите флажок **Использовать KSN для проверки**, если вы хотите использовать облачные службы Kaspersky Security Network для задачи.

     Этот флажок включает или выключает использование облачных служб Kaspersky Security Network (KSN) в задаче.

     Если флажок установлен, программа использует данные, полученные от служб KSN, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

     Если флажок снят, задача проверки по требованию не использует службы KSN.

     По умолчанию флажок установлен.

   - Чтобы присвоить рабочему процессу, в котором будет выполняться задача, базовый приоритет *Низкий*, в окне **Параметры** установите флажок **Выполнять задачу в фоновом режиме**.

     Флажок изменяет приоритет задачи.

     Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему компьютера со стороны других задач Kaspersky Embedded Systems Security и других программ. В результате скорость выполнения задачи уменьшается при увеличении нагрузки и увеличивается при уменьшении нагрузки.

     Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Embedded Systems Security и другие программы. В этом случае увеличивается скорость выполнения задачи.

     По умолчанию флажок снят.

По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Embedded Systems Security, имеют приоритет *Средний*.

- Чтобы использовать создаваемую задачу в качестве задачи Проверка важных областей, в окне **Параметры** установите флажок **Считать выполнение задачи проверкой важных областей**.

  Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Выполнена проверка важных областей* и обновление статуса защиты компьютера. Kaspersky Security Center оценивает безопасность компьютеров по показателям производительности задач со статусом *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Embedded Systems Security. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

  Если флажок установлен, Сервер администрирования регистрирует завершение проверки важных областей и обновляет статус защиты компьютера по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

  Если флажок снят, задача выполняется с низким приоритетом.

  По умолчанию флажок не установлен для пользовательских задач проверки по требованию.

6. Нажмите на кнопку **Далее**.
7. В окне **Расписание** укажите параметры запуска задачи по расписанию.
8. Нажмите на кнопку **Далее**.
9. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
10. Нажмите на кнопку **Далее**.
11. Укажите название задачи.
12. Нажмите на кнопку **Далее**.

    Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы:
    " * < > & \ : |

    Откроется окно **Завершение создания задачи**.
13. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
14. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.

Будет создана новая задача проверки по требованию для выбранного компьютера или группы компьютеров.

В этом разделе

Присвоение задаче проверки по требованию статуса Проверка важных областей

По умолчанию Kaspersky Security Center присваивает компьютеру статус *Предупреждение*, если задача Проверка важных областей выполняется реже, чем указано пороговым параметром для формирования события в Kaspersky Embedded Systems Security – *Проверка важных областей компьютера давно не выполнялась*.

► *Чтобы настроить проверку всех компьютеров, входящих в одну группу администрирования, выполните следующие действия:*

1. Создайте групповую задачу проверки по требованию (см. раздел "Создание задачи проверки по требованию" на стр. 424).
2. В окне **Параметры** мастера создания задачи установите флажок **Считать выполнение задачи проверкой важных областей**. Указанные параметры задачи (область проверки и параметры безопасности) будут применены ко всем компьютерам группы администрирования. Настройте расписание задачи.

   Флажок **Считать выполнение задачи проверкой важных областей** можно установить при создании задачи проверки по требованию для группы компьютеров или позднее в окне **Свойства: <Название задачи>** (см. раздел "Переход к свойствам задачи проверки по требованию" на стр. 423).

3. С помощью новой или существующей политики выключите запуск по расписанию системных задач проверки по требованию на компьютерах группы (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 98).

С этого момента Сервер администрирования Kaspersky Security Center будет оценивать состояние безопасности защищаемого компьютера и уведомлять о нем по результатам последнего выполнения задачи со статусом *Проверка важных областей*, а не по результатам выполнения системной задачи Проверка важных областей.

Вы можете присваивать статус *Задача проверки важных областей* как групповым задачам проверки по требованию, так и задачам для наборов компьютеров.

В Консоли программы вы можете просмотреть, является ли задача проверки по требованию задачей проверки важных областей.

В Консоли программы флажок **Считать выполнение задачи проверкой важных областей** отображается в свойствах задачи, но не доступен для редактирования.

Выполнение задачи проверки по требованию в фоновом режиме

По умолчанию процессы, в которых выполняются задачи Kaspersky Embedded Systems Security, имеют базовый приоритет *Средний*.

Вы можете присвоить процессу, в котором будет выполняться задача проверки по требованию, базовый приоритет *Низкий*. Понижение приоритета процесса увеличивает время выполнения задачи, но также может положительно повлиять на скорость выполнения процессов других активных программ.

В одном рабочем процессе с низким приоритетом может выполняться несколько задач в фоновом режиме. Вы можете установить максимальное количество процессов для фоновых задач проверки по требованию.

► *Чтобы изменить приоритет задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "Переход к мастеру создания задачи проверки по требованию" на стр. 422).
2. Установите или снимите флажок **Выполнять задачу в фоновом режиме**.

   Флажок изменяет приоритет задачи.

   Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему компьютера со стороны других задач Kaspersky Embedded Systems Security и других программ. В результате скорость выполнения задачи уменьшается при увеличении нагрузки и увеличивается при уменьшении нагрузки.

   Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Embedded Systems Security и другие программы. В этом случае увеличивается скорость выполнения задачи.

   По умолчанию флажок снят.
3. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Регистрация выполнения Проверки важных областей

По умолчанию статус защиты компьютера отображается в панели результатов узла **Kaspersky Embedded Systems Security** и обновляется еженедельно после завершения задачи Проверка важных областей.

Время обновления статуса защиты компьютера привязано к расписанию задачи проверки по требованию, в параметрах которой установлен флажок **Считать выполнение задачи проверкой важных областей**. По умолчанию флажок установлен только для задачи Проверка важных областей и недоступен для редактирования в этой задаче.

Вы можете выбрать задачу проверки по требованию, связанную со статусом защиты компьютера, только в Kaspersky Security Center.

Настройка области проверки для задачи

Если вы изменили область проверки в задачах Проверка при старте операционной системы и Проверка важных областей, можно восстановить область проверки по умолчанию для этих задач, выполнив восстановление Kaspersky Embedded Systems Security (**Пуск** > **Программы** > **Kaspersky Embedded Systems Security** > **Изменение или удаление Kaspersky Embedded Systems Security**). В мастере установки выберите **Восстановление установленных компонентов** и нажмите на кнопку **Далее**. Затем установите флажок **Восстановить рекомендуемые параметры работы программы**.

► *Чтобы настроить область проверки для задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "Переход к свойствам задачи проверки по требованию" на стр. 423).
2. Выберите закладку **Область проверки**.
3. Чтобы включить элементы в область проверки:
   a. Откройте контекстное меню для списка областей проверки.
   b. В контекстном меню выберите пункт **Добавить область**.
   c. В открывшемся окне **Добавление в область проверки** выберите тип объекта, который требуется добавить:
      - **Предопределенная область**, чтобы включить в область проверки одну из стандартных областей на защищаемом сервере. Затем в раскрывающемся списке выберите необходимую область.
      - **Диск, папка или сетевой объект**, чтобы включить в область проверки отдельный диск, папку или сетевой объект. Затем выберите нужную область защиты по кнопке **Обзор**.
      - **Файл**, чтобы включить в область проверки отдельный файл. Затем выберите нужную область защиты по кнопке **Обзор**.

   Вы не можете добавить объект в область проверки, если он уже добавлен в качестве исключения из области защиты.
4. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов или выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В окне **Добавление исключения** выберите тип объекта, который вы хотите добавить в качестве исключения из области проверки, по аналогии с добавлением объекта в область проверки.
5. Чтобы изменить добавленную область проверки или исключение, в контекстном меню нужной области проверки выберите пункт **Изменить область**.
6. Чтобы скрыть отображение ранее добавленной области проверки или исключения в списке сетевых файловых ресурсов, в контекстном меню нужной области проверки выберите пункт **Удалить область**.

Область проверки исключается из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

7. Нажмите на кнопку **OK**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут сохранены.

Выбор стандартных уровней безопасности в задачах проверки по требованию

Для элемента, выбранного в списке сетевых файловых ресурсов, можно задать один из трех стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

► *Чтобы выбрать один из стандартных уровней безопасности, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 423).
2. Выберите закладку **Область проверки**.
3. В списке для компьютера выберите элемент, включенный в область проверки, чтобы задать для него стандартный уровень безопасности.
4. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.
5. На закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.
6. Нажмите на кнопку **OK**.
7. В окне **Свойства: Проверка по требованию** нажмите на кнопку **OK**.

   Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Настройка параметров безопасности вручную

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый** (см. раздел "Стандартные уровни безопасности" на стр. 242).

Вы можете изменять заданные по умолчанию значения параметров безопасности, настроив их как едиными для всей области защиты, так и различными для разных элементов / узлов в списке / дереве файловых ресурсов компьютера.

► *Чтобы настроить параметры безопасности вручную, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "Переход к свойствам задачи проверки по требованию" на стр. 423).
2. Выберите закладку **Область проверки**.
3. В списке областей проверки выберите элементы, для которых вы хотите настроить параметры безопасности.

   Стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 158) можно применить к выбранному узлу иди элементу в области проверки.

4. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.

5. Настройте требуемые параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
   - **Общие** параметры (см. раздел "Настройка общих параметров задачи" на стр. 431).
   - **Действия** (см. раздел "**Настройка действий**" на стр. 434).
   - **Производительность** (см. раздел "**Настройка производительности**" на стр. 436).
6. Нажмите на кнопку **OK** в окне **Настройка проверки по требованию**.
7. Нажмите на кнопку **OK** в окне **Область проверки**.

Новые параметры области проверки будут сохранены.

В этом разделе

Настройка общих параметров задачи

► *Чтобы настроить общие параметры задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 423).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.

4. Нажмите на кнопку **Настройка**.

5. На закладке **Общие** в блоке **Проверка объектов** укажите типы объектов, которые вы хотите включить в область проверки:

   - **Объекты проверки**
     - **Все объекты**

       Kaspersky Embedded Systems Security проверяет все объекты.

     - **Объекты, проверяемые по формату**

       Kaspersky Embedded Systems Security проверяет только потенциально заражаемые файлы на основании формата файла.

       Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security.

     - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

       Kaspersky Embedded Systems Security проверяет только потенциально заражаемые файлы на основании расширения файла.

       Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security.

     - **Объекты, проверяемые по указанному списку расширений**

       Kaspersky Embedded Systems Security проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

   - **Вложенные папки**
   - **Вложенные файлы**
   - **Загрузочные секторы дисков и MBR**

     Включение защиты загрузочных секторов дисков и основных загрузочных записей.

     Если флажок установлен, Kaspersky Embedded Systems Security проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках компьютера.

     По умолчанию флажок установлен.

   - **Альтернативные потоки NTFS**

     Проверка дополнительных потоков файлов и папок на дисках файловой системы NTFS.

     Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

     Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

     По умолчанию флажок установлен.

6. В блоке **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security новыми или измененными с момента последней проверки.

Если флажок установлен, Kaspersky Embedded Systems Security проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

Если флажок не установлен, можно выбрать, требуется ли проверка и защита только новых файлов или всех файлов, независимо от того, когда они были изменены.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**. Если выбран уровень безопасности **Максимальная защита** или **Рекомендуемый**, флажок не установлен.

Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

7. В блоке **Проверка составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

- **Все / Только новые архивы**

  Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет архивы.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые SFX-архивы**

  Проверка самораспаковывающихся архивов.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет SFX-архивы.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает SFX-архивы при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

  Параметр доступен, если снят флажок **Архивы**.

- **Все / Только новые почтовые базы**

  Проверка файлов почтовых баз Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает файлы почтовых баз при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые упакованные объекты**

  Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет исполняемые файлы, упакованные программами-упаковщиками.

Если флажок снят, Kaspersky Embedded Systems Security при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

Значение по умолчанию зависит от выбранного уровня защиты.

- **Все / Только новые файлы почтовых форматов**

  Проверка файлов почтовых форматов, например, сообщения форматов Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые вложенные OLE-объекты**

  Проверка встроенных в файл объектов (например, макрос Microsoft Word или вложение сообщения электронной почты).

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает встроенные в файл объекты при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

8. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

Настройка действий

► *Чтобы настроить действия над зараженными и другими обнаруженными объектами во время выполнения задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 423).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.
4. Нажмите на кнопку **Настройка**.
5. Выберите закладку **Действия**.
6. Выберите действие над зараженными и другими обнаруживаемыми объектами:

   - **Только сообщать**

     Когда выбран этот режим, Kaspersky Embedded Systems Security не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного*

объекта. В событии указана все доступная информация об обнаруженном объекте.

Режим **Только сообщать** требуется настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security автоматически изменит уровень безопасности на **Другой**.

- **Лечить**
- **Лечить. Лечить. Удалять, если лечение невозможно**
- **Удалять**
- **Выполнять рекомендуемое действие**

7. Выберите действие над возможно зараженными объектами:
   - **Только сообщать**

     Когда выбран этот режим, Kaspersky Embedded Systems Security не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен*. *Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** требуется настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security автоматически изменит уровень безопасности на **Другой**.
   - **Помещать на карантин**
   - **Удалять**
   - **Выполнять рекомендуемое действие**
8. Настройте действия над объектами в зависимости от типа обнаруженного объекта:
   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

      Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. При этом Kaspersky Embedded Systems Security не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Embedded Systems Security выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

      По умолчанию флажок снят.

   b. Нажмите на кнопку **Настройка**.

   c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.

   d. Нажмите на кнопку **OK**.

9. Выберите действие над неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

   Флажок включает или выключает форсированное удаление родительского составного файла при обнаружении вложенного вредоносного, возможно зараженного или другого обнаруживаемого объекта.

   Если флажок установлен и задача настроена на удаление зараженных или возможно зараженных объектов, Kaspersky Embedded Systems Security принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление составного объекта со всем его содержимым выполняется в случае, если программа не может удалить только вложенный обнаруженный объект (например, если составной объект неизменяем).

   Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security не выполняет выбранное действие, если родительский объект неизменяем.

10. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

► *Чтобы настроить производительность задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Свойства: Проверка по требованию** (см. раздел "**Переход к свойствам задачи проверки по требованию**" на стр. 423).
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.
4. Нажмите на кнопку **Настройка**.
5. Выберите закладку **Производительность**.
6. В блоке **Исключения**:
   - Снимите или установите флажок **Исключать файлы**.

     Исключение файлов из проверки по имени файла или маске имени файла.

     Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security проверяет все объекты.

     По умолчанию флажок снят.
   - Снимите или установите флажок **Не обнаруживать**.

     Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Embedded Systems Security обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

- Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.

7. В блоке **Дополнительные параметры**:

- **Останавливать проверку, если она длится более (сек.)**

  Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

  Если флажок установлен, максимальная продолжительность проверки объекта ограничена указанным значением.

  Если флажок снят, максимальная продолжительность проверки не ограничена.

  По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Не проверять составные объекты размером более (МБ)**

  Исключение из проверки составных объектов больше указанного размера.

  Если флажок установлен, Kaspersky Embedded Systems Security пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

  Если флажок снят, Kaspersky Embedded Systems Security проверяет составные объекты, не учитывая размер.

  По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет только новые файлы и файлы, изменившиеся с момента последней проверки системных объектов NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы во время выполнения задачи проверки и проверяет только новые файлы и файлы, измененные с момента последней проверки.

Если флажок установлен, Kaspersky Embedded Systems Security проверяет только новые и измененные файлы.

Если флажок снят, Kaspersky Embedded Systems Security проверяет файлы независимо от даты их создания и изменения.

По умолчанию флажок установлен.

8. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

Настройка проверки съемных дисков

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

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую требуется настроить.

   В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Настройка** в подразделе **Проверка съемных дисков**.

   Откроется окно **Проверка съемных дисков**.
6. В блоке **Параметры проверки при подключении** выполните следующие действия:
   - Установите флажок **Проверять съемные диски при их подключении по USB**, если вы хотите, чтобы программа Kaspersky Embedded Systems Security автоматически выполняла проверку съемных дисков при их подключении.
   - Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** и укажите максимальное значение объема данных в поле справа.
   - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съемных дисков.
7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены.

Управление задачей проверки по требованию с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи для локального компьютера.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

В этом разделе

Переход к параметрам задачи проверки по требованию

► *Чтобы перейти к общим параметрам задачи проверки по требованию в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов вложенного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

► *Чтобы перейти к параметрам области проверки в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.

Создание и настройка задачи проверки по требованию

Вы можете создавать пользовательские задачи для отдельного компьютера в узле **Проверка по требованию**. В других функциональных компонентах Kaspersky Embedded Systems Security создание пользовательских задач не предусмотрено.

► *Чтобы создать и настроить задачу проверки по требованию, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Проверка по требованию**.
2. Выберите пункт **Добавить задачу**.

   Откроется окно **Добавить задачу**.
3. Настройте следующие параметры задачи:
   - **Имя** – название задачи, содержащее не более 100 символов, может содержать любые символы, кроме **" * < > & \ : |**.

     Вы не можете сохранить новую задачу или перейти к настройке параметров новой задачи на закладках **Расписание**, **Дополнительно** и **Запуск с правами**, если не задано название задачи.
   - **Описание** – дополнительная информация о задаче, не более 2000 символов. Эта информация отображается в окне свойств задачи.
   - **Использовать эвристический анализатор**

     Флажок включает или выключает использование эвристического анализатора при проверке объектов.

     Если флажок установлен, эвристический анализатор включен.

     Если флажок снят, эвристический анализатор выключен.

     По умолчанию флажок установлен.
   - **Выполнять задачу в фоновом режиме**

     Флажок изменяет приоритет задачи.

     Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему компьютера со стороны других задач Kaspersky Embedded Systems Security и других программ. В результате скорость выполнения задачи уменьшается при увеличении нагрузки и увеличивается при уменьшении нагрузки.

     Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Embedded Systems Security и другие программы. В этом случае увеличивается скорость выполнения задачи.

     По умолчанию флажок снят.

- **Применять доверенную зону**

  Флажок включает или выключает применение доверенной зоны в работе задачи.

  Если флажок установлен, Kaspersky Embedded Systems Security добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

  Если флажок снят, Kaspersky Embedded Systems Security не учитывает файловые операции доверенных процессов при формировании области защиты для задачи.

  По умолчанию флажок установлен.

- **Считать выполнение задачи проверкой важных областей**

  Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Выполнена проверка важных областей* и обновление статуса защиты компьютера. Kaspersky Security Center оценивает безопасность компьютеров по показателям производительности задач со статусом *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Embedded Systems Security. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

  Если флажок установлен, Сервер администрирования регистрирует завершение проверки важных областей и обновляет статус защиты компьютера по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

  Если флажок снят, задача выполняется с низким приоритетом.

  По умолчанию флажок не установлен для пользовательских задач проверки по требованию.

- **Использовать KSN для проверки**

  Этот флажок включает или выключает использование облачных служб Kaspersky Security Network (KSN) в задаче.

  Если флажок установлен, программа использует данные, полученные от служб KSN, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

  Если флажок снят, задача проверки по требованию не использует службы KSN.

  По умолчанию флажок установлен.

4. Настройте расписание запуска задачи (см. раздел "Настройка расписания запуска задач" на стр. 151) на закладках **Расписание** и **Дополнительно**.
5. На закладке **Запуск с правами** настройте запуск задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 154).
6. В окне **Добавить задачу** нажмите на кнопку **ОК**.

   Новая пользовательская задача проверки по требованию будет создана. Узел с названием новой задачи будет отображен в дереве Консоли программы. Операция регистрируется в журнале системного аудита (стр. 204).
7. Если требуется, в панели результатов выбранного узла выберите **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
8. В дереве или в списке файловых ресурсов компьютера выберите узлы или элементы, которые вы хотите включить в область проверки.

9. Выберите один из стандартных уровней безопасности (см. раздел "О стандартных уровнях безопасности в задачах проверки по требованию" на стр. 416) или настройте параметры проверки вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 446).
10. Нажмите кнопку **Сохранить** в окне **Настройка области проверки**.

Настроенные параметры будут применены при последующем запуске задачи.

Область проверки в задачах проверки по требованию

Этот раздел содержит информацию о формировании и использовании области проверки в задачах проверки по требованию.

В этом разделе

Настройка параметров отображения сетевых файловых ресурсов

► *Чтобы выбрать способ отображения сетевых файловых ресурсов при настройке параметров области проверки, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. В левом верхнем углу открывшегося окна разверните раскрывающийся список. Выполните одно из следующих действий:
   - Выберите пункт **Показывать в виде дерева**, если вы хотите, чтобы сетевые файловые ресурсы отображались в виде дерева.
   - Выберите пункт **Показывать в виде списка**, если вы хотите, чтобы сетевые файловые ресурсы отображались в виде списка.

   По умолчанию сетевые файловые ресурсы защищаемого компьютера отображаются в виде списка.
3. Нажмите на кнопку **Сохранить**.

Окно параметров области проверки будет закрыто. Настроенные параметры задачи будут применены.

Формирование области проверки

Если вы управляете Kaspersky Embedded Systems Security на защищаемом компьютере удаленно через Консоль программы, установленную на рабочем месте администратора, вы должны входить в группу администраторов на защищаемом компьютере, чтобы просматривать папки на нем.

Названия параметров могут отличаться в разных операционных системах Windows.

Если вы изменили область проверки в задачах Проверка при старте операционной системы и Проверка важных областей, можно восстановить область проверки по умолчанию для этих задач, выполнив восстановление Kaspersky Embedded Systems Security (**Пуск** > **Программы** > **Kaspersky Embedded Systems Security** > **Изменение или удаление Kaspersky Embedded Systems Security**). В мастере установки выберите **Восстановление установленных компонентов** и нажмите на кнопку **Далее**. Затем установите флажок **Восстановить рекомендуемые параметры работы программы**.

Процедура формирования области проверки в задачах проверки по требованию зависит от типа отображения сетевых файловых ресурсов (см. раздел "Настройка параметров отображения сетевых файловых ресурсов" на стр. 442). Вы можете настроить отображение сетевых файловых ресурсов в виде дерева или в виде списка (по умолчанию).

► *Чтобы сформировать область проверки, работая с деревом сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. В левой части окна разверните дерево сетевых файловых ресурсов, чтобы отобразить все узлы.
3. Выполните следующие действия:
   - Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:
     - Если вы хотите включить в область проверки все диски одного типа, установите флажок рядом с названием нужного типа дисков (например, чтобы включить все съемные диски компьютера, установите флажок **Съемные диски**).
     - Если вы хотите включить в область проверки отдельный диск определенного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем требуемого диска. Например, чтобы выбрать съемный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**.
     - если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.
4. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут сохранены.

► *Чтобы сформировать область проверки с помощью списка сетевых файловых ресурсов, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. Чтобы включить отдельные узлы в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область проверки**.

c. В открывшемся окне **Добавление области проверки** выберите тип объекта, который требуется добавить:

- **Предопределенная область**, чтобы включить в область проверки одну из стандартных областей на защищаемом компьютере. Затем в раскрывающемся списке выберите нужную область проверки.
- **Диск, папка или сетевой объект**, чтобы включить в область проверки отдельный диск, папку или сетевой объект. Затем выберите нужную область защиты по кнопке **Обзор**.
- **Файл**, чтобы включить в область проверки отдельный файл. Затем выберите нужную область защиты по кнопке **Обзор**.

Вы не можете добавить объект в область проверки, если он уже добавлен в качестве исключения из области защиты.

3. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов или выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В окне **Добавление исключения** выберите тип объекта, который вы хотите добавить в качестве исключения из области проверки, по аналогии с добавлением объекта в область проверки.
4. Чтобы изменить добавленную область проверки или исключение, в контекстном меню нужной области проверки выберите пункт **Изменить область**.
5. Чтобы скрыть отображение ранее добавленной области проверки или исключения в списке сетевых файловых ресурсов, в контекстном меню нужной области проверки выберите пункт **Удалить из списка**.

   Область проверки исключается из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

6. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут сохранены.

Включение в область проверки сетевых объектов

Вы можете включать в область проверки сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Вы можете проверять сетевые папки при работе под системной учетной записью.

► *Чтобы включить в область проверки сетевой объект, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.

3. В контекстном меню узла **Сетевое окружение** выполните следующие действия:
   - Выберите пункт **Добавить сетевую папку**, если вы хотите добавить сетевую папку в область проверки.
   - Выберите пункт **Добавить сетевой файл**, если вы хотите добавить сетевой файл в область проверки.
4. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention) и нажмите на клавишу **ENTER**.
5. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область проверки.
6. Если требуется, измените параметры безопасности для добавленного сетевого объекта.
7. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Создание виртуальной области проверки

Вы можете включать в область проверки динамические диски, папки и файлы – создавать виртуальную область проверки.

Вы можете включить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов (см. раздел "Настройка параметров отображения сетевых файловых ресурсов" на стр. 442).

► *Чтобы включить в область проверки виртуальный диск, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В дереве файловых ресурсов компьютера откройте контекстное меню узла **Виртуальные диски**, выберите пункт **Добавить виртуальный диск** и в списке доступных имен выберите имя виртуального диска.
4. Установите флажок рядом с добавленным диском, чтобы включить диск в область проверки.
5. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

► *Чтобы включить в область проверки виртуальную папку или виртуальный файл, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.

3. В дереве файловых ресурсов компьютера откройте контекстное меню узла, в который вы хотите добавить папку или файл, и выберите один из следующих пунктов:
   - **Добавить виртуальную папку**, если вы хотите добавить виртуальную папку в область проверки.
   - **Добавить виртуальный файл**, если вы хотите добавить виртуальный файл в область проверки.
4. В поле ввода задайте имя для папки или файла.
5. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область проверки.
6. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Выбор стандартных уровней безопасности в задачах проверки по требованию

Для узла или элемента, выбранного в дереве или в списке сетевых файловых ресурсов, можно задать один из трех стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

► *Чтобы выбрать один из стандартных уровней безопасности, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. В дереве или в списке сетевых файловых ресурсов компьютера выберите узел или элемент, для которого вы хотите задать стандартный уровень безопасности.
3. Убедитесь, что выбранный узел или элемент включен в область проверки.
4. В правой части окна на закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.
5. Нажмите на кнопку **Сохранить**.

   Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Настройка параметров безопасности вручную

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый** (см. раздел "Стандартные уровни безопасности" на стр. 242).

Вы можете изменять заданные по умолчанию значения параметров безопасности, настроив их как едиными для всей области защиты, так и различными для разных элементов / узлов в списке / дереве файловых ресурсов компьютера.

При работе с деревом сетевых файловых ресурсов параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

► *Чтобы настроить параметры безопасности вручную, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. В левой части окна выберите узел или элемент, параметры безопасности которого вы хотите настроить.

   Стандартный шаблон параметров безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 158) можно применить к выбранному узлу или элементу в области проверки.
3. На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
   - Общие параметры (см. раздел "Настройка общих параметров задачи" на стр. 447)
   - Действия (см. раздел "Настройка действий" на стр. 450)
   - Производительность (см. раздел "Настройка производительности" на стр. 452)
   - Иерархическое хранилище
4. Нажмите на кнопку **Сохранить** в окне **Настройка области проверки**.

Новые параметры области проверки будут сохранены.

В этом разделе

Настройка общих параметров задачи

► *Чтобы настроить общие параметры безопасности задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. Выберите закладку **Общие**.
3. В блоке **Проверка объектов** укажите типы объектов, которые требуется включить в область проверки:
   - **Объекты проверки**
     - **Все объекты**

       Kaspersky Embedded Systems Security проверяет все объекты.

- **Объекты, проверяемые по формату**

  Kaspersky Embedded Systems Security проверяет только потенциально заражаемые файлы на основании формата файла.

  Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**

  Kaspersky Embedded Systems Security проверяет только потенциально заражаемые файлы на основании расширения файла.

  Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security.

- **Объекты, проверяемые по указанному списку расширений**

  Kaspersky Embedded Systems Security проверяет файлы на основании расширения файла. Список расширений файлов можно настроить вручную в окне **Список расширений**, которое открывается по кнопке **Изменить**.

- **Загрузочные секторы дисков и MBR**

  Включение защиты загрузочных секторов дисков и основных загрузочных записей.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках компьютера.

  По умолчанию флажок установлен.

- **Альтернативные потоки NTFS**

  Проверка дополнительных потоков файлов и папок на дисках файловой системы NTFS.

  Если флажок установлен, программа выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом.

  Если флажок не установлен, программа проверяет только обнаруженный объект, который считается возможно зараженным.

  По умолчанию флажок установлен.

4. В блоке **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security новыми или измененными с момента последней проверки.

   Если флажок установлен, Kaspersky Embedded Systems Security проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

   Если флажок не установлен, можно выбрать, требуется ли проверка и защита только новых файлов или всех файлов, независимо от того, когда они были изменены.

   По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**. Если выбран уровень безопасности **Максимальная защита** или **Рекомендуемый**, флажок не установлен.

Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

5. В блоке **Проверка составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

   - **Все / Только новые архивы**

     Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

     Если флажок установлен, Kaspersky Embedded Systems Security проверяет архивы.

     Если флажок снят, Kaspersky Embedded Systems Security пропускает архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня защиты.

   - **Все / Только новые SFX-архивы**

     Проверка самораспаковывающихся архивов.

     Если флажок установлен, Kaspersky Embedded Systems Security проверяет SFX-архивы.

     Если флажок снят, Kaspersky Embedded Systems Security пропускает SFX-архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня защиты.

     Параметр доступен, если снят флажок **Архивы**.

   - **Все / Только новые почтовые базы**

     Проверка файлов почтовых баз Microsoft Outlook и Microsoft Outlook Express.

     Если флажок установлен, Kaspersky Embedded Systems Security проверяет файлы почтовых баз.

     Если флажок снят, Kaspersky Embedded Systems Security пропускает файлы почтовых баз при проверке.

     Значение по умолчанию зависит от выбранного уровня безопасности.

   - **Все / Только новые упакованные объекты**

     Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

     Если флажок установлен, Kaspersky Embedded Systems Security проверяет исполняемые файлы, упакованные программами-упаковщиками.

     Если флажок снят, Kaspersky Embedded Systems Security при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

     Значение по умолчанию зависит от выбранного уровня защиты.

   - **Все / Только новые файлы почтовых форматов**

     Проверка файлов почтовых форматов, например, сообщения форматов Microsoft Outlook и Microsoft Outlook Express.

     Если флажок установлен, Kaspersky Embedded Systems Security проверяет файлы почтовых форматов.

Если флажок снят, Kaspersky Embedded Systems Security пропускает файлы почтовых форматов при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые вложенные OLE-объекты**

  Проверка встроенных в файл объектов (например, макрос Microsoft Word или вложение сообщения электронной почты).

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Embedded Systems Security пропускает встроенные в файл объекты при проверке.

  Значение по умолчанию зависит от выбранного уровня защиты.

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка действий

► *Чтобы настроить действия, которые задача проверки по требованию выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**

     Когда выбран этот режим, Kaspersky Embedded Systems Security не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется следующее событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

     Режим **Только сообщать** требуется настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security автоматически изменит уровень безопасности на **Другой**.

   - **Лечить**
   - **Лечить. Лечить. Удалять, если лечение невозможно**
   - **Удалять**
   - **Выполнять рекомендуемое действие**
4. Выберите действие над возможно зараженными объектами:
   - **Только сообщать**

     Когда выбран этот режим, Kaspersky Embedded Systems Security не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется следующее

событие: *Объект не вылечен. Причина: в соответствии с заданными настройками не было предпринято действий для нейтрализации обнаруженного объекта.* В событии указана все доступная информация об обнаруженном объекте.

Режим **Только сообщать** требуется настроить отдельно для каждой области защиты или проверки. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security автоматически изменит уровень безопасности на **Другой**.

- **Помещать на карантин**
- **Удалять**
- **Выполнять рекомендуемое действие**

5. Настройте действия над объектами в зависимости от типа обнаруженного объекта:
   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

      Если флажок установлен, можно выбирать основное и дополнительное действие для каждого обнаруженного типа объектов независимо, нажав на кнопку **Настройка** рядом с флажком. При этом Kaspersky Embedded Systems Security не позволит открыть или запустить зараженный объект независимо от вашего выбора.

      Если флажок снят, Kaspersky Embedded Systems Security выполняет действия, выбранные в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** для указанных типов объектов.

      По умолчанию флажок снят.

   b. Нажмите на кнопку **Настройка**.
   c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.
   d. Нажмите на кнопку **OK**.
6. Выберите действие над неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

   Флажок включает или выключает форсированное удаление родительского составного файла при обнаружении вложенного вредоносного, возможно зараженного или другого обнаруживаемого объекта.

   Если флажок установлен и задача настроена на удаление зараженных или возможно зараженных объектов, Kaspersky Embedded Systems Security принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление составного объекта со всем его содержимым выполняется в случае, если программа не может удалить только вложенный обнаруженный объект (например, если составной объект неизменяем).

   Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Embedded Systems Security не выполняет выбранное действие, если родительский объект неизменяем.
7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

► *Чтобы настроить производительность задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. Выберите закладку **Производительность**.
3. В блоке **Исключения**:
   - Снимите или установите флажок **Исключать файлы**.

     Исключение файлов из проверки по имени файла или маске имени файла.

     Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security проверяет все объекты.

     По умолчанию флажок снят.
   - Снимите или установите флажок **Не обнаруживать**.

     Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Список имен обнаруживаемых объектов приведен на сайте Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/.

     Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.
   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.
4. В блоке **Дополнительные параметры**:
   - **Останавливать проверку, если она длится более (сек.)**

     Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

     Если флажок установлен, максимальная продолжительность проверки объекта ограничена указанным значением.

     Если флажок снят, максимальная продолжительность проверки не ограничена.

     По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.
   - **Не проверять составные объекты размером более (МБ)**

     Исключение из проверки составных объектов больше указанного размера.

     Если флажок установлен, Kaspersky Embedded Systems Security пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

     Если флажок снят, Kaspersky Embedded Systems Security проверяет составные объекты, не учитывая размер.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**.

- **Использовать технологию iSwift**

  iSwift сравнивает NTFS-идентификатор файла, хранящийся в базе данных, с текущим идентификатором. Проверка выполняется только для файлов, идентификаторы которых изменились (новые файлы и файлы, измененные с момента последней проверки системных объектов NTFS).

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет только новые файлы и файлы, изменившиеся с момента последней проверки системных объектов NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security проверяет объекты файловой системы NTFS независимо от их даты создания и изменения, за исключением файлов в сетевых папках.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker**

  iChecker рассчитывает и хранит контрольные суммы проверенных файлов. При изменении объекта меняется его контрольная сумма. Программа сравнивает все контрольные суммы во время выполнения задачи проверки и проверяет только новые файлы и файлы, измененные с момента последней проверки.

  Если флажок установлен, Kaspersky Embedded Systems Security проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Embedded Systems Security проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

5. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка иерархического хранилища

► *Чтобы настроить действия, которые задача проверки по требованию выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. стр. 439).
2. Выберите закладку **Иерархическое хранилище**.
3. Выберите действие над автономными файлами:
   - **Не проверять**
   - **Проверять только резидентную часть файла**
   - **Проверять весь файл**

     Если выбрано это действие, доступны следующие параметры проверки:

     - Снимите или установите флажок **Только если зарегистрированы обращения к файлу за указанный период (дней)** и укажите количество дней.

- Снимите или установите флажок **По возможности не копировать файл на локальный жесткий диск**.

4. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Проверка съемных дисков

► *Чтобы настроить проверку съемных дисков при их подключении к защищаемому компьютеру в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Security** и выберите пункт **Настроить проверку съемных дисков**.

   Откроется окно **Проверка съемных дисков**.

2. В блоке **Параметры проверки при подключении** выполните следующие действия:

   - Установите флажок **Проверять съемные диски при их подключении по USB**, если вы хотите, чтобы программа Kaspersky Embedded Systems Security автоматически выполняла проверку съемных дисков при их подключении.
   - Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** и укажите максимальное значение объема данных в поле справа.
   - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съемных дисков.

3. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены.

Статистика задач проверки по требованию

Пока выполняется задача проверки по требованию, вы можете просматривать информацию о количестве объектов, которые программа Kaspersky Embedded Systems Security обработала с момента запуска задачи до текущего момента.

Эта информация будет доступна, даже если вы приостановите задачу. Вы можете просмотреть статистику задачи в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задаче Kaspersky Embedded Systems Security в журналах выполнения задач" на стр. 208).

► *Чтобы просмотреть статистику задачи проверки по требованию, выполните следующие действия:*

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, статистику которой вы хотите просмотреть.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

В таблице ниже вы можете просмотреть информацию об объектах, которые программа Kaspersky Embedded Systems Security обработала с момента запуска задачи до текущего момента.

Таблица 61. Статистика задач проверки по требованию

Поле	Описание
Обнаружено	Количество объектов, которые обнаружила программа Kaspersky Embedded Systems Security. Например, если программа Kaspersky Embedded Systems Security обнаружила в пяти файлах одну вредоносную программу, значение в этом поле увеличится на единицу.
Зараженных и других обнаруживаемых объектов	Количество объектов, которые Kaspersky Embedded Systems Security признал зараженными, или обнаруженных объектов, которые не были исключены из области действия задач постоянной защиты или проверки по требованию и были определены как легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.
Возможно зараженных объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security признала возможно зараженными.
Объектов не вылечено	Количество объектов, которые программа Kaspersky Embedded Systems Security не вылечила по следующим причинам: • тип обнаруженного объекта не предполагает лечения; • при лечении возникла ошибка.
Объектов не помещено на карантин	Количество объектов, которые программа Kaspersky Embedded Systems Security попыталась поместить на карантин, но безуспешно, например, из-за отсутствия доступного пространства на диске.
Объектов не удалено	Количество объектов, которые программа Kaspersky Embedded Systems Security попыталась удалить, но безуспешно, например, если доступ к объекту был заблокирован другой программой.
Объектов не проверено	Количество объектов в области защиты, которые программа Kaspersky Embedded Systems Security не смогла проверить, например, если доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых программа Kaspersky Embedded Systems Security попыталась сохранить в резервном хранилище, но безуспешно, например, из-за отсутствия доступного пространства на диске.
Ошибок обработки	Количество объектов, во время обработки которых возникла ошибка задачи.
Вылечено объектов	Количество объектов, которые вылечила программа Kaspersky Embedded Systems Security.
Помещено на карантин	Количество объектов, которые поместила на карантин программа Kaspersky Embedded Systems Security.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Embedded Systems Security сохранила в резервном хранилище.
Удалено объектов	Количество объектов, которые удалила программа Kaspersky Embedded Systems Security.
Защищенных паролем объектов	Количество объектов (например, архивов), которые программа Kaspersky Embedded Systems Security пропустила, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security пропустила, так как их формат искажен.

Поле	Описание
Обработано объектов	Общее количество объектов, которые обработала программа Kaspersky Embedded Systems Security.

Вы также можете посмотреть статистику задачи проверки по требованию в журнале выполнения выбранной задачи по ссылке **Открыть журнал выполнения** в блоке **Управление** панели результатов.

По завершении выполнения задачи рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

Доверенная зона

Этот раздел содержит информацию о доверенной зоне Kaspersky Embedded Systems Security, а также инструкции по добавлению объектов в доверенную зону при выполнении задач.

В этом разделе

О доверенной зоне

Доверенная зона – это список исключений из области защиты или проверки, который вы можете сформировать и применять в задачах Проверка по требованию и Постоянная защита файлов.

Если при установке Kaspersky Embedded Systems Security вы установили флажки **Добавить к исключениям файлы, рекомендованные Microsoft** и **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**, Kaspersky Embedded Systems Security добавляет в доверенную зону файлы, рекомендованные Microsoft и "Лабораторией Касперского", для задач постоянной защиты компьютера.

Вы можете формировать доверенную зону Kaspersky Embedded Systems Security по следующим правилам:

- Доверенные процессы. В доверенную зону помещаются объекты, к которым обращаются процессы программ, чувствительных к файловым перехватам.
- Операции резервного копирования. В доверенную зону помещаются объекты, доступ к которым выполняется в операциях систем резервного копирования жестких дисков на внешние устройства.
- Исключения. В доверенную зону помещаются объекты, указанные по их местоположению и / или обнаруженному в них объекту.

Вы можете применить доверенную зону в задаче Постоянная защита файлов, во вновь созданных пользовательских задачах проверки по требованию, а также во всех системных задачах проверки по требованию, кроме задачи Проверка объектов на карантине.

По умолчанию доверенная зона применяется в задаче Постоянная защита файлов и в задачах проверки по требованию.

Вы можете экспортировать список правил формирования доверенной зоны в конфигурационный файл в формате XML, чтобы затем импортировать его в Kaspersky Embedded Systems Security на другом компьютере.

Доверенные процессы

Применяется в задачах Постоянная защита файлов и Защита трафика.

Некоторые программы на компьютере могут работать нестабильно, если файлы, к которым они обращаются, перехватываются программой Kaspersky Embedded Systems Security. К таким программам относятся, например, системные программы домен-контроллеров.

Чтобы не нарушать работу таких программ, вы можете выключить защиту файлов, к которым обращаются выполняющиеся процессы этих программ, сформировав в доверенной зоне список доверенных процессов.

Корпорация Microsoft рекомендует исключать из постоянной защиты некоторые файлы операционной системы Microsoft Windows и файлы программ корпорации Microsoft как неподверженные заражению. Имена некоторых из них приведены на веб-сайте Microsoft https://www.microsoft.com/ru-ru/ (код статьи: KB822158).

Вы можете включать и выключать применение доверенных процессов в доверенной зоне.

Если исполняемый файл процесса изменяется, например, обновляется, Kaspersky Embedded Systems Security исключает его из списка доверенных процессов.

Программа не использует значение пути к файлу на защищаемом компьютере для идентификации процесса как доверенного. Путь к файлу на защищаемом компьютере применяется только для поиска файла, расчета его контрольной суммы и для информирования пользователя об источнике исполняемого файла.

Операции резервного копирования

Применяется в задачах Постоянная защита компьютера.

На время резервного копирования данных, хранящихся на жестких дисках, на внешние устройства вы можете выключить защиту объектов, доступ к которым осуществляется при операциях резервного копирования. Kaspersky Embedded Systems Security не проверяет объекты, которые программа резервного копирования открывает на чтение с признаком FILE_FLAG_BACKUP_SEMANTICS.

Исключения

Применяется в задачах Постоянная защита файлов и Проверка по требованию.

Вы можете выбрать задачи, в которых вы хотите применять каждое исключение, добавленное в доверенную зону. Также вы можете исключать объекты из проверки в параметрах уровня безопасности каждой задачи Kaspersky Embedded Systems Security по отдельности.

Вы можете добавлять в доверенную зону объекты по их местоположению на компьютере, по имени или маске имени обнаруженного в них объекта или использовать оба критерия.

На основании исключения Kaspersky Embedded Systems Security может пропускать в указанных задачах объекты согласно следующим параметрам:

- указанные объекты, обнаруживаемые по имени или маске имени в указанных областях компьютера;
- все объекты, обнаруживаемые в указанных областях компьютера;
- указанные объекты, обнаруживаемые по имени или маске имени во всей области защиты или проверки.

Управление доверенной зоной с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка доверенной зоны для одного или всех компьютеров сети.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

В этом разделе

Управление программой с помощью Kaspersky Security Center

► *Чтобы перейти к доверенной зоне в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую требуется настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Дополнительные возможности**.
6. Нажмите на кнопку **Настройка** в разделе **Доверенная зона**.

   Откроется окно **Доверенная зона**.

Настройте политику в соответствии с вашими требованиями.

Если компьютер работает под управлением активной политики Kaspersky Security Center и в этой политике запрещено изменение параметров программы, эти параметры недоступны для изменения в Консоли программы.

Переход к окну параметров доверенной зоны

► *Чтобы настроить доверенную зону в окне свойств программы, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя компьютера>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого компьютера;
   - Выберите пункт **Свойства** в контекстном меню защищаемого компьютера.

   Откроется окно **Свойства: <Имя компьютера>**.
5. В разделе **Программы** выберите **Kaspersky Embedded Systems Security**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры Kaspersky Embedded Systems Security**.
7. Выберите раздел **Дополнительные возможности**.
8. Нажмите на кнопку **Настройка** в разделе **Доверенная зона**.

   Откроется окно **Доверенная зона**.

Настройте доверенную зону в соответствии с вашими требованиями.

Настройка параметров доверенной зоны с помощью Плагина управления

По умолчанию доверенная зона применяется ко всем новым создаваемым политикам и задачам.

Чтобы настроить параметры доверенной зоны, выполните следующие действия:

1. На закладке **Исключения** укажите объекты, которые Kaspersky Embedded Systems Security пропускает при выполнении задачи (см. раздел "Добавление исключений" на стр. 461).
2. На закладке **Доверенные процессы** укажите процессы, которые Kaspersky Embedded Systems Security пропускает при выполнении задачи (см. раздел "Добавление доверенных процессов" на стр. 462).
3. Примените маску not-a-virus (см. раздел "Использование маски not-a-virus" на стр. 465).

В этом разделе

Добавление исключений

► *Чтобы добавить исключение в доверенную зону в политике Kaspersky Security Center, выполните следующие действия:*

1. Откройте окно **Доверенная зона** (см. раздел **"Управление программой с помощью Kaspersky Security Center"** на стр. 459).
2. На закладке **Исключения** укажите объекты, которые Kaspersky Embedded Systems Security пропускает при проверке:
   - Чтобы создать рекомендуемые исключения, нажмите на кнопку **Добавить рекомендуемые исключения**.

     При нажатии на эту кнопку в список исключений добавляются исключения, рекомендованные корпорацией Microsoft и исключения, рекомендованные "Лабораторией Касперского".
   - Если вы хотите импортировать исключения, нажмите на кнопку **Импорт** и в открывшемся окне выберите файлы, которые Kaspersky Embedded Systems Security будет считать доверенными.
   - Если вы хотите вручную указать условия, при выполнении которых файл будет считаться доверенным, нажмите на кнопку **Добавить**.

     Откроется окно **Исключения**.
3. В разделе **Не проверять объект при выполнении следующих условий** укажите объекты, которые вы хотите исключить из области защиты / проверки, и объекты, которые требуется исключить из обнаруживаемых объектов:
   - Чтобы исключить объект из области защиты или проверки:
     a. Установите флажок **Проверяемый объект**.

        Добавляет файл, папку, диск или файл скрипта в исключения.

        Если флажок установлен, Kaspersky Embedded Systems Security пропускает указанный диапазон, файл, папку, диск или файл скрипта при запуске проверки с использованием компонентов Kaspersky Embedded Systems Security, выбранных в разделе **Область применения правил**.

        По умолчанию флажок снят.

     b. Нажмите на кнопку **Изменить**.

        Откроется окно **Выбор объекта**.

     c. Выберите объект, который требуется исключить из области проверки.

        > При задании объектов можно использовать специальные символы ? и *.

     d. Нажмите на кнопку **ОК**.

     e. Установите флажок **Применить ко вложенным папкам**, если требуется исключить все вложенные файлы и папки указанного объекта из области защиты или проверки.

- Если требуется указать имя обнаруживаемого объекта:
  a. Установите флажок **Обнаруживаемые объекты**.

     Исключение обнаруживаемых объектов из проверки по имени или маске имени объекта. Вы можете найти список имен обнаруживаемых объектов на сайте Вирусной энциклопедии.

     Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.

  b. Нажмите на кнопку **Изменить**.

     Откроется окно **Список обнаруживаемых объектов**.

  c. Укажите имя или маску имени обнаруживаемого объекта согласно классификации Вирусной энциклопедии.

  d. Нажмите на кнопку **Добавить**.

  e. Нажмите на кнопку **OK**.

4. В разделе **Область применения правил** установите флажки рядом с названиями задач, к которым требуется применить исключения.

   Название задачи Kaspersky Embedded Systems Security, в которой применяется правило.

5. Нажмите на кнопку **OK**.

Исключение отображается в списке на закладке **Исключения** окна **Доверенная зона**.

Добавление доверенных процессов

► *Чтобы добавить один или несколько процессов в список доверенных, выполните следующие действия:*

1. Откройте окно **Доверенная зона** (см. раздел "Управление программой с помощью Kaspersky Security Center" на стр. 459).
2. Выберите закладку **Доверенные процессы**.
3. Установите флажок **Не проверять файловые операции резервного копирования**, чтобы пропустить проверку операций чтения файлов.

   Флажок включает или выключает проверку операций чтения файлов, если эти операции выполняются установленными на компьютере инструментами резервного копирования.

   Если флажок установлен, Kaspersky Embedded Systems Security пропускает операции чтения файлов, выполняемые установленными на компьютере инструментами резервного копирования.

Если флажок снят, Kaspersky Embedded Systems Security проверяет операции чтения файлов, выполняемые установленными на компьютере инструментами резервного копирования.

По умолчанию флажок установлен.

4. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.

   Флажок включает или выключает проверку файловой активности доверенных процессов.

   Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке операции доверенных процессов.

   Если флажок снят, Kaspersky Embedded Systems Security проверяет файловые операции доверенных процессов.

   По умолчанию флажок снят.

5. Нажмите на кнопку **Добавить**.
6. Выберите один из следующих вариантов из контекстного меню кнопки:

   - **Несколько процессов**

     В открывшемся окне **Добавление процессов в список доверенных** настройте следующие параметры:

     a. **Использовать полный путь для определения доверенности процесса**

        Если флажок установлен, Kaspersky Embedded Systems Security использует полный путь к файлу для определения, является ли процесс доверенным.

        Если флажок не установлен, путь к файлу не будет учитываться при определении доверенности процесса.

        По умолчанию флажок снят.

     b. **Использовать хеш файла для определения доверенности процесса**

        Если флажок установлен, Kaspersky Embedded Systems Security использует хеш выбранного файла для определения статуса доверенности процесса.

        Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

        По умолчанию флажок установлен.

     c. Чтобы добавить данные на основе исполняемых файлов, нажмите на кнопку **Обзор**.

     d. Выберите исполняемый файл в открывшемся окне.

        Вы можете добавлять процессы только по одному. Повторите шаги c-d, чтобы добавить другие исполняемые файлы.

     e. Чтобы добавить данные на основе запущенных процессов, нажмите на кнопку **Процессы**.

     f. Выберите процессы в открывшемся окне. Чтобы выбрать несколько процессов, удерживайте клавишу **CTRL** при выборе.

     g. Нажмите на кнопку **OK**.

Для просмотра списка активных процессов необходимо, чтобы учетная запись, с правами которой запускается задача Постоянная защита файлов, имела права администратора на компьютере с установленной программой Kaspersky Embedded Systems Security. Вы можете отсортировать процессы в списке активных процессов по имени файла, идентификатору процесса (PID) или пути к исполняемому файлу процесса на локальном компьютере. Обратите внимание, что вы можете выбрать процесс из списка запущенных процессов, нажав на кнопку **Процессы**, только при работе через Консоль программы на локальном компьютере или в параметрах этого узла в Kaspersky Security Center.

- **Один процесс на основе имени файла и пути**

  В открывшемся окне **Добавление процесса** выполните следующие действия:

  a. Укажите путь к исполняемому файлу (включая имя файла)

  b. Нажмите на кнопку **ОК**.

- **Один процесс на основе свойств объекта**

  В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

  a. Нажмите на кнопку **Обзор** и выберите процесс.

  b. **Использовать полный путь для определения доверенности процесса**

     Если флажок установлен, Kaspersky Embedded Systems Security использует полный путь к файлу для определения, является ли процесс доверенным.

     Если флажок не установлен, путь к файлу не будет учитываться при определении доверенности процесса.

     По умолчанию флажок снят.

  c. **Использовать хеш файла для определения доверенности процесса**

     Если флажок установлен, Kaspersky Embedded Systems Security использует хеш выбранного файла для определения статуса доверенности процесса.

     Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

     По умолчанию флажок установлен.

  d. Нажмите на кнопку **ОК**.

  Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран как минимум один критерий доверенности.

7. В окне **Добавление доверенных процессов** нажмите на кнопку **ОК**.

Выбранный файл или процесс будет добавлен в список доверенных процессов в окне **Доверенная зона**.

Использование маски not-a-virus

Маска not-a-virus позволяет пропускать во время проверки легальное программное обеспечение и веб-ресурсы, которые могут быть расценены как вредоносные. Маска применяется при работе следующих задач:

- Постоянная защита файлов.
- Проверка по требованию.

Если маска не добавлена в список исключений, Kaspersky Embedded Systems Security выполнит действия, указанные в параметрах задачи, для программ, которые входят в эту категорию.

► *Чтобы использовать маску not-a-virus, выполните следующие действия:*

1. Откройте окно **Доверенная зона** (см. раздел "Управление программой с помощью Kaspersky Security Center" на стр. 459).
2. На закладке **Исключения** прокрутите список и выберите строку со значением **not-a-virus:*** в графе **Обнаруживаемые объекты**, если флажок снят.
3. Нажмите на кнопку **OK**.

Новые настройки будут применены.

Управление доверенной зоной с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка доверенной зоны для локального компьютера.

В этом разделе

Использование доверенной зоны для задач в Консоли программы

По умолчанию доверенная зона применяется в задаче Постоянная защита файлов, во вновь созданных пользовательских задачах проверки по требованию, а также во всех системных задачах проверки по требованию, кроме задачи Проверка объектов на карантине.

После того как вы включите или выключите доверенную зону, заданные в ней исключения начнут или перестанут действовать в выполняющихся задачах немедленно.

► *Чтобы включить или выключить применение доверенной зоны в задачах Kaspersky Embedded Systems Security, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню задачи, для которой вы хотите настроить использование доверенной зоны.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Общие** выполните одно из следующих действий:
   - Если вы хотите применять доверенную зону в задаче, установите флажок **Применять доверенную зону**.
   - Если вы хотите выключить применение доверенной зоны в задаче, снимите флажок **Применять доверенную зону**.
4. Чтобы настроить параметры доверенной зоны, перейдите по ссылке в названии флажка **Применять доверенную зону**.

   Откроется окно **Доверенная зона**.
5. Нажмите на кнопку **ОК** в окне **Параметры задачи**, чтобы сохранить изменения.

Настройка параметров доверенной зоны в Консоли программы

Чтобы настроить параметры доверенной зоны, выполните следующие действия:

1. На закладке **Исключения** укажите объекты, которые Kaspersky Embedded Systems Security пропускает при выполнении задачи (см. раздел "Добавление исключений в доверенную зону" на стр. 467).
2. На закладке **Доверенные процессы** укажите процессы, которые Kaspersky Embedded Systems Security пропускает при выполнении задачи (см. раздел "Доверенные процессы" на стр. 468).
3. Примените доверенную зону для задач программы (см. раздел "Использование доверенной зоны для задач в Консоли программы" на стр. 465).
4. Примените маску not-a-virus (см. раздел "Использование маски not-a-virus" на стр. 471).

В этом разделе

Добавление исключений в доверенную зону

► *Чтобы вручную добавить исключение в доверенную зону в Консоли программы, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите пункт меню **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. Выберите закладку **Исключения**.
4. Нажмите на кнопку **Добавить**.

   Откроется окно **Исключения**.
5. В разделе **Не проверять объект при выполнении следующих условий** укажите объекты, которые вы хотите исключить из области защиты / проверки, и объекты, которые требуется исключить из обнаруживаемых объектов:

   - Чтобы исключить объект из области защиты или проверки:

     a. Установите флажок **Проверяемый объект**.

        Добавляет файл, папку, диск или файл скрипта в исключения.

        Если флажок установлен, Kaspersky Embedded Systems Security пропускает указанный диапазон, файл, папку, диск или файл скрипта при запуске проверки с использованием компонентов Kaspersky Embedded Systems Security, выбранных в разделе **Область применения правил**.

        По умолчанию флажок снят.

     b. Нажмите на кнопку **Изменить**.

        Откроется окно **Выбор объекта**.

     c. Выберите объект, который требуется исключить из области проверки.

        > При задании объектов можно использовать специальные символы ? и *.

     d. Нажмите на кнопку **ОК**.

     e. Установите флажок **Применить ко вложенным папкам**, если требуется исключить все вложенные файлы и папки указанного объекта из области защиты или проверки.

   - Если требуется указать имя обнаруживаемого объекта:

     a. Установите флажок **Обнаруживаемые объекты**.

        Исключение обнаруживаемых объектов из проверки по имени или маске имени объекта. Вы можете найти список имен обнаруживаемых объектов на сайте Вирусной энциклопедии.

        Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Embedded Systems Security обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

b. Нажмите на кнопку **Изменить**.

Откроется окно **Список обнаруживаемых объектов**.

c. Укажите имя или маску имени обнаруживаемого объекта согласно классификации Вирусной энциклопедии.

d. Нажмите на кнопку **Добавить**.

e. Нажмите на кнопку **OK**.

6. В разделе **Область применения правил** установите флажки рядом с названиями задач, к которым требуется применить исключения.

Название задачи Kaspersky Embedded Systems Security, в которой применяется правило.

7. Нажмите на кнопку **OK**.

Исключение отображается в списке на закладке **Исключения** окна **Доверенная зона**.

Доверенные процессы

Вы можете добавить процесс в список доверенных процессов одним из следующих способов:

- выбрать процесс из списка процессов, выполняемых на защищаемом компьютере;
- выбрать исполняемый файл процесса независимо от того, выполняется ли процесс в текущий момент.

Если исполняемый файл процесса изменится, Kaspersky Embedded Systems Security исключит этот процесс из списка доверенных процессов.

► *Чтобы добавить один или несколько процессов в список доверенных, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите пункт меню **Настроить параметры доверенной зоны**.

Откроется окно **Доверенная зона**.

3. Выберите закладку **Доверенные процессы**.
4. Установите флажок **Не проверять файловые операции резервного копирования**, чтобы пропустить проверку операций чтения файлов.

Флажок включает или выключает проверку операций чтения файлов, если эти операции выполняются установленными на компьютере инструментами резервного копирования.

Если флажок установлен, Kaspersky Embedded Systems Security пропускает операции чтения файлов, выполняемые установленными на компьютере инструментами резервного копирования.

Если флажок снят, Kaspersky Embedded Systems Security проверяет операции чтения файлов, выполняемые установленными на компьютере инструментами резервного копирования.

По умолчанию флажок установлен.

5. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.

   Флажок включает или выключает проверку файловой активности доверенных процессов.

   Если флажок установлен, Kaspersky Embedded Systems Security пропускает при проверке операции доверенных процессов.

   Если флажок снят, Kaspersky Embedded Systems Security проверяет файловые операции доверенных процессов.

   По умолчанию флажок снят.

6. Нажмите на кнопку **Добавить**.
7. Выберите один из следующих вариантов из контекстного меню кнопки:

   - **Несколько процессов**

     В открывшемся окне **Добавление процессов в список доверенных** настройте следующие параметры:

     a. **Использовать полный путь для определения доверенности процесса**

        Если флажок установлен, Kaspersky Embedded Systems Security использует полный путь к файлу для определения, является ли процесс доверенным.

        Если флажок не установлен, путь к файлу не будет учитываться при определении доверенности процесса.

        По умолчанию флажок снят.

     b. **Использовать хеш файла для определения доверенности процесса**

        Если флажок установлен, Kaspersky Embedded Systems Security использует хеш выбранного файла для определения статуса доверенности процесса.

        Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

        По умолчанию флажок установлен.

     c. Чтобы добавить данные на основе исполняемых файлов, нажмите на кнопку **Обзор**.

     d. Выберите исполняемый файл в открывшемся окне.

        Вы можете добавлять процессы только по одному. Повторите шаги c-d, чтобы добавить другие исполняемые файлы.

     e. Чтобы добавить данные на основе запущенных процессов, нажмите на кнопку **Процессы**.

     f. Выберите процессы в открывшемся окне. Чтобы выбрать несколько процессов, удерживайте клавишу **CTRL** при выборе.

     g. Нажмите на кнопку **OK**.

Для просмотра списка активных процессов необходимо, чтобы учетная запись, с правами которой запускается задача Постоянная защита файлов, имела права администратора на компьютере с установленной программой Kaspersky Embedded Systems Security. Вы можете отсортировать процессы в списке активных процессов по имени файла, идентификатору процесса (PID) или пути к исполняемому файлу процесса на локальном компьютере. Обратите внимание, что вы можете выбрать процесс из списка запущенных процессов, нажав на кнопку **Процессы**, только при работе через Консоль программы на локальном компьютере или в параметрах этого узла в Kaspersky Security Center.

- **Один процесс на основе имени файла и пути**

  В открывшемся окне **Добавление процесса** выполните следующие действия:

  a. Укажите путь к исполняемому файлу (включая имя файла)

  b. Нажмите на кнопку **ОК**.

- **Один процесс на основе свойств объекта**

  В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

  a. Нажмите на кнопку **Обзор** и выберите процесс.

  b. **Использовать полный путь для определения доверенности процесса**

     Если флажок установлен, Kaspersky Embedded Systems Security использует полный путь к файлу для определения, является ли процесс доверенным.

     Если флажок не установлен, путь к файлу не будет учитываться при определении доверенности процесса.

     По умолчанию флажок снят.

  c. **Использовать хеш файла для определения доверенности процесса**

     Если флажок установлен, Kaspersky Embedded Systems Security использует хеш выбранного файла для определения статуса доверенности процесса.

     Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.

     По умолчанию флажок установлен.

  d. Нажмите на кнопку **ОК**.

Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран как минимум один критерий доверенности.

8. В окне **Добавление доверенных процессов** нажмите на кнопку **ОК**.

Выбранный файл или процесс будет добавлен в список доверенных процессов в окне **Доверенная зона**.

Использование маски not-a-virus

Маска not-a-virus позволяет пропускать во время проверки легальное программное обеспечение и веб-ресурсы, которые могут быть расценены как вредоносные. Маска применяется при работе следующих задач:

- Постоянная защита файлов.
- Проверка по требованию.

Если маска не добавлена в список исключений, Kaspersky Embedded Systems Security применит действия, указанные в параметрах задачи, для программ и веб-ресурсов, которые входят в эту категорию.

► *Чтобы использовать маску not-a-virus, выполните следующие действия:*

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите пункт меню **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. Выберите закладку **Исключения**.
4. Прокрутите список и выберите строку со значением **not-a-virus:***, если флажок не установлен.
5. Нажмите на кнопку **OK**.

Новые настройки будут применены.

Защита от эксплойтов

Этот раздел содержит инструкции по настройке параметров защиты памяти процессов от эксплуатации уязвимостей.

В этом разделе

О защите от эксплойтов

Kaspersky Embedded Systems Security предоставляет возможность защитить память процессов от эксплойтов. Эта возможность реализована в компоненте Защита от эксплойтов. Вы можете изменять статус активности компонента, а также настраивать параметры защиты процессов от эксплуатации уязвимостей.

Компонент выполняет защиту памяти процессов от эксплойтов с помощью внедрения внешнего Агента защиты процессов (далее Агент) в защищаемый процесс.

Внешний Агент защиты – это динамически загружаемый модуль Kaspersky Embedded Systems Security, который внедряется в защищаемые процессы с целью контроля их целостности и снижения рисков эксплуатации уязвимостей.

Функционирование Агента внутри защищаемого процесса зависит от итераций запуска и остановки этого процесса: первичная загрузка Агента в процесс, добавленный в список защищаемых, возможна только при перезапуске процесса. Выгрузка Агента из процесса после его удаления из списка защищаемых также возможна только после перезапуска процесса.

Выгрузка Агента из защищаемых процессов предполагает необходимость их остановки: при удалении компонента Защита от эксплойтов программа выполняет заморозку среды и форсирует выгрузку Агента из защищаемых процессов. Если при удалении компонента Агент внедрен хотя бы в один из защищаемых процессов, необходимо завершить данный процесс. Может потребоваться перезагрузка компьютера (например, если защищается системный процесс).

При обнаружении признаков атаки эксплойта на защищаемый процесс Kaspersky Embedded Systems Security выполняет одно из следующих действий:

- завершает процесс при попытке эксплуатации уязвимости;
- сообщает о факте дискредитации уязвимости в процессе.

Вы можете остановить защиту процессов одним из следующих способов:

- удалить компонент;

- удалить процесс из списка защищаемых и перезапустить его.

Служба Kaspersky Security Exploit Prevention

Для максимальной эффективности компоненту Защита от эксплойтов требуется наличие службы Kaspersky Security Exploit Prevention на защищаемом компьютере. Эта служба входит в состав рекомендуемой установки совместно с компонентом Защита от эксплойтов. Во время установки службы на защищаемый компьютер создается и запускается процесс kavfswh. Он передает информацию о защищаемых процессах от компонентов Агенту защиты.

После остановки службы Kaspersky Security Exploit Prevention программа продолжает защищать процессы, которые были добавлены в список защищаемых, а также загружается в новые добавленные процессы и применяет все доступные техники защиты от эксплойтов для защиты памяти процессов.

Если на компьютере установлена операционная система Windows 10 или более поздних версий, программа не будет продолжать защищать процессы и память процессов после остановки службы Kaspersky Security Exploit Prevention.

В случае остановки службы Kaspersky Security Exploit Prevention программа не будет получать данные о событиях, происходящих с защищаемыми процессами (в том числе данные об атаках эксплойтов и о завершении процессов). Также Агент не сможет получать данные о новых параметрах защиты и о добавлении новых процессов в список защищаемых процессов.

Режимы защиты от эксплойтов

Вы можете настраивать действия по снижению рисков эксплуатации уязвимостей в защищаемых процессах, выбрав один из двух режимов:

- **Завершать скомпрометированные процессы**: применяйте данный режим, чтобы завершать процесс при попытке эксплуатации уязвимости.

  При обнаружении попытки эксплуатации уязвимости в защищаемом процессе, которому присвоен уровень "критический" в операционной системе, Kaspersky Embedded Systems Security не выполняет завершение такого процесса независимо от режима, указанного в параметрах компонента Защита от эксплойтов.

- **Только сообщать**: применяйте этот режим, чтобы получать данные о фактах эксплуатации уязвимостей в защищаемых процессах с помощью событий в журнале безопасности.

  Если выбран данный режим, Kaspersky Embedded Systems Security регистрирует все попытки эксплуатации уязвимостей посредством создания событий.

Управление защитой от эксплойтов с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров компонентов для одного или всех компьютеров сети.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

В этом разделе

Переход к параметрам политики для защиты от эксплойтов

► *Чтобы перейти к параметрам защиты от эксплойтов в политике Kaspersky Security Center, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую требуется настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита компьютера**.
6. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.

Настройте защиту от эксплойтов в соответствии с вашими требованиями.

Переход к окну параметров защиты от эксплойтов

► *Чтобы перейти к окну **Свойства: <Имя сервера>** для защиты от эксплойтов, выполните следующие действия:*

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя компьютера>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого компьютера;
   - Выберите пункт **Свойства** в контекстном меню защищаемого компьютера.

   Откроется окно **Свойства: <Имя компьютера>**.
5. В разделе **Программы** выберите **Kaspersky Embedded Systems Security**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры Kaspersky Embedded Systems Security**.
7. Перейдите в раздел **Постоянная защита компьютера**.
8. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.

Настройте защиту от эксплойтов в соответствии с вашими требованиями.

Настройка защиты памяти процессов

► *Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:*

1. Откройте окно **Защита от эксплойтов** (см. раздел "**Переход к параметрам политики для защиты от эксплойтов**" на стр. 474).
2. В блоке **Режим защиты от эксплойтов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей**

     Если флажок установлен, Kaspersky Embedded Systems Security снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

     Если флажок снят, Kaspersky Embedded Systems Security не защищает процессы на компьютере от эксплуатации уязвимостей.

     По умолчанию флажок снят.
   - **Завершать скомпрометированные процессы**

     Если выбран данный режим, Kaspersky Embedded Systems Security завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.

- **Только сообщать**

  Если выбран данный режим, Kaspersky Embedded Systems Security сообщает о факте эксплуатации уязвимости посредством вывода терминального окна на экран. Скомпрометированный процесс продолжает выполняться.

  Если во время работы программы в режиме **Завершать скомпрометированные процессы** Kaspersky Embedded Systems Security обнаруживает факт эксплуатации уязвимости критического процесса, компонент принудительно переходит в режим **Только сообщать**.

3. В блоке **Действия по защите** настройте следующие параметры:

   - **Сообщать о скомпрометированных процессах посредством службы терминалов**

     Если флажок установлен, Kaspersky Embedded Systems Security выводит на экран терминальное окно с описанием причины срабатывания защиты и указанием на процесс, где была обнаружена попытка эксплуатации уязвимости.

     Если флажок снят, Kaspersky Embedded Systems Security не будет выводить на экран терминальное окно при обнаружении факта попытки эксплуатации уязвимости или завершения скомпрометированного процесса. Терминальное окно отображается независимо от статуса службы Kaspersky Security Exploit Prevention. По умолчанию флажок установлен.

   - **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security**

     Если флажок установлен, Kaspersky Embedded Systems Security снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Embedded Systems Security не защищает процессы, добавленные после остановки службы Kaspersky Security. После того как служба будет запущена, снижение рисков эксплуатации уязвимостей всех процессов будет остановлено.

     Если флажок снят, Kaspersky Embedded Systems Security не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

     По умолчанию флажок установлен.

4. Нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security сохранит и применит настроенные параметры защиты памяти процессов.

Добавление защищаемого процесса

Компонент Защита от эксплойтов защищает несколько процессов по умолчанию. Можно исключить процессы из области защиты, сняв соответствующие флажки в списке процессов.

► *Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:*

1. Откройте окно **Защита от эксплойтов** (см. раздел "**Переход к параметрам политики для защиты от эксплойтов**" на стр. 474).

2. На закладке **Защищаемые процессы**, нажмите на кнопку **Обзор**.

   Откроется окно проводника Windows.

3. Выберите процесс, который вы хотите добавить в список.
4. Нажмите на кнопку **Открыть**.

   Имя процесса будет отображено в строке.

5. Нажмите на кнопку **Добавить**.

   Указанный процесс добавится в список защищаемых процессов.

6. Выберите добавленный процесс.
7. Нажмите на кнопку **Указать техники защиты от эксплойтов**.

   Откроется окно **Техники защиты от эксплойтов**.

8. Выберите один из следующих вариантов применения техник снижения рисков:

   - **Применять все доступные техники защиты от эксплойтов**

     Если выбран этот вариант, редактирование списка недоступно. Все доступные для процесса техники будут применяться по умолчанию.

   - **Применять выбранные техники защиты от эксплойтов**

     Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

     a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.

     b. Установите или снимите флажок **Применять технику Attack Surface Reduction**.

9. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):

   - Внесите названия модулей, которые будут запрещены к запуску из защищаемого процесса в поле **Запрещать загрузку модулей**.
   - В поле **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, запуск модулей в которых вы хотите разрешить:
     - Интернет
     - Интранет
     - Доверенные веб-сайты
     - Сайты с ограниченным доступом
     - Компьютер

     > Данные параметры применимы только для Internet Explorer®.

10. Нажмите на кнопку **OK**.

Процесс будет добавлен в область защиты задачи.

Управление защитой от эксплойтов с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров компонента для локального компьютера.

В этом разделе

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

В этом разделе

Переход к основным параметрам защиты от эксплойтов

► *Чтобы перейти к окну **Параметры защиты от эксплойтов**, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security**.
2. Откройте контекстное меню и выберите пункт **Защита от эксплойтов: общие параметры защиты**.

   Откроется окно **Параметры защиты от эксплойтов**.

Настройте общие параметры защиты от эксплойтов в соответствии с вашими требованиями.

Переход к параметрам защиты процессов при защите от эксплойтов

► *Чтобы перейти к окну **Параметры защиты процессов**, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security**.
2. Откройте контекстное меню и выберите пункт **Защита от эксплойтов: параметры защиты процессов**.

   Откроется окно **Параметры защиты процессов**.

Настройте параметры защиты процессов для защиты от эксплойтов в соответствии с вашими требованиями.

Настройка защиты памяти процессов

► *Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:*

1. Откройте окно Параметры защиты от эксплойтов.
2. В блоке **Режим защиты от эксплойтов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей**

     Если флажок установлен, Kaspersky Embedded Systems Security снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

     Если флажок снят, Kaspersky Embedded Systems Security не защищает процессы на компьютере от эксплуатации уязвимостей.

     По умолчанию флажок снят.

   - **Завершать скомпрометированные процессы**

     Если выбран данный режим, Kaspersky Embedded Systems Security завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.

   - **Только сообщать**

     Если выбран данный режим, Kaspersky Embedded Systems Security сообщает о факте эксплуатации уязвимости посредством вывода терминального окна на экран. Скомпрометированный процесс продолжает выполняться.

     Если во время работы программы в режиме **Завершать скомпрометированные процессы** Kaspersky Embedded Systems Security обнаруживает факт эксплуатации уязвимости критического процесса, компонент принудительно переходит в режим **Только сообщать**.
3. В блоке **Действия по защите** настройте следующие параметры:
   - **Сообщать о скомпрометированных процессах посредством службы терминалов**

     Если флажок установлен, Kaspersky Embedded Systems Security выводит на экран терминальное окно с описанием причины срабатывания защиты и указанием на процесс, где была обнаружена попытка эксплуатации уязвимости.

     Если флажок снят, Kaspersky Embedded Systems Security не будет выводить на экран терминальное окно при обнаружении факта попытки эксплуатации уязвимости или завершения скомпрометированного процесса. Терминальное окно отображается независимо от статуса службы Kaspersky Security Exploit Prevention. По умолчанию флажок установлен.

   - **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security**

     Если флажок установлен, Kaspersky Embedded Systems Security снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Embedded Systems Security не защищает процессы, добавленные после остановки службы Kaspersky Security. После того как служба будет запущена, снижение рисков эксплуатации уязвимостей всех процессов будет остановлено.

Если флажок снят, Kaspersky Embedded Systems Security не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

По умолчанию флажок установлен.

4. В окне **Параметры защиты от эксплойтов** нажмите на кнопку **ОК**.

Kaspersky Embedded Systems Security сохранит и применит настроенные параметры защиты памяти процессов.

Добавление защищаемого процесса

Компонент Защита от эксплойтов защищает несколько процессов по умолчанию. Вы можете исключить какой-либо процесс из защиты, сняв флажок в соответствующей строке процесса.

► *Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:*

1. Откройте окно Параметры защиты процессов.
2. Чтобы защитить процесс от компрометации и снизить возможное влияние эксплуатации уязвимостей, выполните следующие действия:
   a. Нажмите на кнопку **Обзор**.

      Откроется стандартное окно Microsoft Windows **Открыть**.

   b. В открывшемся окне выберите процесс, который вы хотите добавить в список.
   c. Нажмите на кнопку **Открыть**.
   d. Нажмите на кнопку **Добавить**.

      Указанный процесс добавится в список защищаемых процессов.
3. Выберите добавленный процесс в списке.
4. На странице **Параметры защиты процесса** отображается текущая конфигурация:
   - **Имя процесса**
   - **Выполняется сейчас**
   - **Применяемые техники защиты от эксплойтов**
   - **Снижение области действия процесса (параметры техники Attack Surface Reduction)**
5. Чтобы отредактировать применяемые к данному процессу техники защиты от эксплойтов, выберите закладку **Техники защиты**.
6. Выберите один из следующих вариантов применения техник снижения рисков:
   - **Применять все доступные техники защиты от эксплойтов**

     Если выбран этот вариант, редактирование списка недоступно. Все доступные для процесса техники будут применяться по умолчанию.

- **Применять указанные техники защиты от эксплойтов**

  Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

  a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.

7. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):
   - Внесите названия модулей, которые будут запрещены к запуску из защищаемого процесса в поле **Запрещать загрузку модулей**.
   - В поле **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, запуск модулей в которых вы хотите разрешить:
     - Интернет
     - Интранет
     - Доверенные веб-сайты
     - Сайты с ограниченным доступом
     - Компьютер

     Данные параметры применимы только для Internet Explorer®.

8. Нажмите на кнопку **OK**.

Процесс будет добавлен в область защиты задачи.

Техники защиты от эксплойтов

Таблица 62. Техники защиты от эксплойтов

Техника защиты от эксплойтов	Описание
Data Execution Prevention (DEP)	Предотвращение выполнения данных - запрет исполнения произвольного кода в защищенной области памяти.
Address Space Layout Randomization (ASLR)	Изменение расположения структур данных в адресном пространстве процесса.
Structured Exception Handler Overwrite Protection (SEHOP)	Подмена записи в структуре исключений или подмена обработчика исключений.
Null Page Allocation	Предотвращение переориентации нулевого указателя.
LoadLibrary Network Call Check (Anti ROP)	Защита от загрузки динамических библиотек с сетевых путей.
Executable Stack (Anti ROP)	Запрет на несанкционированное исполнение областей стека.
Anti RET Check (Anti ROP)	Проверка безопасного вызова функции через CALL инструкцию.
Anti Stack Pivoting (Anti ROP)	Защита от перемещения указателя стека ESP на эксплуатируемый адрес.

Техника защиты от эксплойтов	Описание
Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Защита доступа на чтение таблицы экспорта адресов (Export Address Table) для модулей kernel32.dll, kernelbase.dll, ntdll.dll.
Heap Spray Allocation (Heapspray)	Защита от выделения памяти под исполнение вредоносного кода.
Execution Flow Simulation (Anti Return Oriented Programming)	Обнаружение подозрительных цепочек инструкций (возможный ROP гаджет) в компоненте Windows API.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Защита от эскалации привилегий через уязвимость в драйвере AFD (выполнение произвольного кода на нулевом кольце через вызов QueryIntervalProfile).
Attack Surface Reduction (ASR)	Блокирование запуска уязвимых модулей через защищаемый процесс.
Anti Process Hollowing (Hollowing)	Защита от создания и запуска вредоносных копий доверенных процессов.
Anti AtomBombing (APC)	Защита от эксплуатации глобальных атомных таблиц через асинхронные вызовы процедур (APC).
Anti CreateLocalThread (RThreadRemote)	Сторонний процесс создал поток в защищаемом процессе.
Anti CreateRemoteThread (RThreadRemote)	Защита внедрения потока защищаемого процесса в другой процесс.

Интеграция со сторонними системами

В этом разделе описана интеграция Kaspersky Embedded Systems Security с функциями и технологиями сторонних производителей.

В этом разделе

Контроль производительности. Счетчики Kaspersky Embedded Systems Security

Этот раздел содержит информацию о счетчиках Kaspersky Embedded Systems Security: счетчиках производительности системного монитора, счетчиках и ловушках SNMP.

В этом разделе

Счетчики производительности для программы Системный монитор

Этот раздел содержит информацию о счетчиках производительности для программы "Системный монитор" Microsoft Windows, которые регистрирует Kaspersky Embedded Systems Security во время установки.

В этом разделе

О счетчиках производительности Kaspersky Embedded Systems Security

В состав устанавливаемых компонентов Kaspersky Embedded Systems Security по умолчанию включен компонент **Счетчики производительности**. Во время установки Kaspersky Embedded Systems Security регистрирует свои счетчики производительности для программы "Системный монитор" Microsoft Windows.

С помощью счетчиков Kaspersky Embedded Systems Security вы можете контролировать производительность программы во время выполнения задач постоянной защиты. Вы можете обнаруживать узкие места при его совместной работе с другими программами и недостаточность ресурсов. Вы можете диагностировать неоптимальную настройку Kaspersky Embedded Systems Security и сбои в его работе.

Вы можете просматривать счетчики производительности Kaspersky Embedded Systems Security, открыв консоль **Производительность** в элементе **Администрирование** Панели управления Windows.

В следующих разделах приводятся определения счетчиков, рекомендуемые интервалы считывания показаний, пороговые значения и рекомендации по настройке Kaspersky Embedded Systems Security в случае, если значения счетчиков их превышают.

Общее количество отвергнутых запросов

Таблица 63. Общее количество отвергнутых запросов

Название	Общее количество отвергнутых запросов (Total number of requests denied).
Определение	Общее количество запросов драйвера файловых перехватов на обработку объектов, которые не были принятых рабочими процессами Kaspersky Embedded Systems Security; рассчитывается с момента последнего запуска Kaspersky Embedded Systems Security. Программа пропускает объекты, запросы на обработку которых отвергаются рабочими процессами Kaspersky Embedded Systems Security.

Назначение	Счетчик позволяет обнаруживать следующие ситуации: • снижение качества постоянной защиты из-за полной загрузки рабочих процессов Kaspersky Embedded Systems Security; • прерывание постоянной защиты из-за отказа диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1.
Рекомендуемый интервал считывания показаний	1 ч
Рекомендации по настройке, если значение превышает пороговое	Количество отвергнутых запросов на обработку соответствует количеству пропущенных объектов. Возможны следующие ситуации в зависимости от поведения счетчика: • Счетчик показывает несколько отвергнутых запросов в течение длительного времени: все рабочие процессы Kaspersky Embedded Systems Security были полностью загружены, поэтому программа Kaspersky Embedded Systems Security не смогла проверить объекты. Чтобы исключить пропуск объектов, увеличьте количество процессов программы для задач постоянной защиты. Можно использовать параметры Kaspersky Embedded Systems Security **Максимальное количество активных процессов** и **Количество процессов для постоянной защиты**. • Количество отвергнутых запросов значительно превышает критический порог и быстро растет: отказал диспетчер файловых перехватов. Kaspersky Embedded Systems Security не проверяет объекты при доступе. Перезапустите Kaspersky Embedded Systems Security.

Общее количество пропущенных запросов

Таблица 64. Общее количество пропущенных запросов

Название	Общее количество пропущенных запросов (Total number of requests skipped).
Определение	Общее количество запросов драйвера файловых перехватов на обработку объектов, принятых Kaspersky Embedded Systems Security, но не отправивших события о завершении обработки; рассчитывается с момента последнего запуска программы. Если запрос на обработку объекта, принятый одним из рабочих процессов, не отправил события о завершении обработки, драйвер передает этот запрос другому процессу и значение счетчика **Общее количество пропущенных запросов** увеличивается на 1. Если драйвер перебрал все рабочие процессы и ни один из них не принял запрос на обработку (был занят) или не отправил события о завершении обработки, Kaspersky Embedded Systems Security пропускает такой объект и на 1 увеличивается значение счетчика **Общее количество отвергнутых запросов**.

Назначение	Счетчик позволяет обнаруживать снижение производительности из-за простоя потоков диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 ч.
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нулевого, это означает, что зависли и простаивают один или несколько потоков диспетчера файловых перехватов. Значение счетчика соответствует количеству потоков, простаивающих в текущий момент. Если скорость проверки не удовлетворительна, перезапустите Kaspersky Embedded Systems Security, чтобы восстановить простаивающие потоки.

Количество запросов, не обработанных из-за нехватки системных ресурсов

Таблица 65. Количество запросов, не обработанных из-за нехватки системных ресурсов

Название	Количество запросов, не обработанных из-за нехватки системных ресурсов (Number of requests not processed due to lack of resources)
Определение	Общее количество запросов драйвера файловых перехватов, не обработанных из-за нехватки системных ресурсов (например, оперативной памяти); рассчитывается с момента последнего запуска Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security пропускает объекты, запросы на проверку которых не обрабатываются драйвером файловых перехватов.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты, возникающее из-за недостаточности системных ресурсов.
Нормальное / пороговое значение	0 / 1.
Рекомендуемый интервал считывания показаний	1 ч
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нулевого, рабочие процессы Kaspersky Embedded Systems Security нуждаются в увеличении объема оперативной памяти для обработки запросов. Возможно, активные процессы других программ используют всю доступную оперативную память.

Количество запросов, отданных на обработку

Таблица 66. Количество запросов, отданных на обработку

Название	Количество запросов, отданных на обработку (Number of requests sent to be processed).
Определение	Количество объектов, ожидающих обработки рабочими процессами.
Назначение	Счетчик позволяет отслеживать загрузку рабочих процессов Kaspersky Embedded Systems Security и общий уровень файловой активности на компьютере.
Нормальное / пороговое значение	Значение счетчика может колебаться в зависимости от уровня файловой активности на компьютере.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Нет

Среднее количество потоков диспетчера файловых перехватов

Таблица 67. Среднее количество потоков диспетчера файловых перехватов

Название	Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams).
Определение	Количество потоков диспетчера файловых перехватов в одном рабочем процессе, среднее по всем процессам, занятым в задачах постоянной защиты в текущий момент.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты из-за полной загрузки процессов Kaspersky Embedded Systems Security.
Нормальное / пороговое значение	Варьируется / 40.
Рекомендуемый интервал считывания показаний	1 мин.

Рекомендации по настройке, если значение превышает пороговое	В каждом рабочем процессе может быть создано до 60 потоков диспетчера файловых перехватов. Если значение счетчика приближается к 60, возникает риск того, что ни одному из рабочих процессов не удастся принять на обработку очередной запрос от драйвера файловых перехватов и Kaspersky Embedded Systems Security пропустит объект. Увеличьте количество процессов Kaspersky Embedded Systems Security для задач постоянной защиты. Можно использовать параметры Kaspersky Embedded Systems Security **Максимальное количество активных процессов** и **Количество процессов для постоянной защиты**.

Максимальное количество потоков диспетчера файловых перехватов

Таблица 68. Максимальное количество потоков диспетчера файловых перехватов

Название	Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).
Определение	Количество потоков диспетчера файловых перехватов в одном рабочем процессе, наибольшее из всех процессов, занятых в задачах постоянной защиты в текущий момент.
Назначение	Счетчик позволяет обнаруживать и устранять снижение производительности из-за неравномерного распределения нагрузки в выполняющихся рабочих процессах.
Нормальное / пороговое значение	Варьируется / 40.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Если значение этого счетчика значительно и продолжительно превышает значение счетчика **Среднее количество потоков диспетчера файловых перехватов**, Kaspersky Embedded Systems Security неравномерно распределяет нагрузку на выполняющиеся процессы. Перезапустите Kaspersky Embedded Systems Security.

Количество элементов в очереди зараженных объектов

Таблица 69. Количество элементов в очереди зараженных объектов

Название	Количество элементов в очереди зараженных объектов (Number of items in the infected object queue).
Определение	Количество зараженных объектов, ожидающих обработки (лечения или удаления) в текущий момент.

Назначение	Счетчик позволяет обнаруживать следующие ситуации: • прерывание постоянной защиты из-за возможного отказа диспетчера файловых перехватов; • перегруженность процессора из-за неравномерного распределения процессорного времени между другими работающими программами и Kaspersky Embedded Systems Security; • вирусную эпидемию.
Нормальное / пороговое значение	Значение счетчика может быть отличным от нуля, пока Kaspersky Embedded Systems Security обрабатывает обнаруженные зараженные или возможно зараженные объекты, но оно возвращается к нулю вскоре после окончания обработки / Значение счетчика остается ненулевым длительное время.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика остается ненулевым длительное время: • Kaspersky Embedded Systems Security не обрабатывает объекты (возможно, отказал диспетчер файловых перехватов). Перезапустите Kaspersky Embedded Systems Security. • Недостаточно процессорного времени для обработки объектов. Обеспечьте выделение дополнительного процессорного времени для Kaspersky Embedded Systems Security, например, снизив нагрузку на компьютер со стороны других программ. • Возникла вирусная эпидемия. О возникновении вирусной эпидемии говорит большое количество обнаруженных зараженных или возможно зараженных объектов в задаче Постоянная защита файлов. Вы можете просмотреть информацию о количестве обнаруженных объектов в статистике задачи или журнале выполнения задачи.

Количество объектов, обрабатываемых за секунду

Таблица 70. Количество объектов, обрабатываемых за секунду

Название	Количество объектов, обрабатываемых за секунду (Number of objects processed per second).
Определение	Количество обработанных объектов, разделенное на количество времени, в течение которого эти объекты были обработаны; рассчитывается за равные промежутки времени.
Назначение	Счетчик отражает скорость обработки объектов. Он позволяет обнаружить и устранить снижение производительности компьютера, возникшее из-за недостаточности процессорного времени, которое выделяется рабочим процессам Kaspersky Embedded Systems Security, или сбоя в работе Kaspersky Embedded Systems Security.

Нормальное / пороговое значение	Варьируется / Нет.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Значения счетчика зависят от значений параметров Kaspersky Embedded Systems Security и от загрузки компьютера процессами других программ. Наблюдайте средний уровень показаний счетчика в течение продолжительного времени. Если общий уровень показаний счетчика снизился, то могла произойти одна из следующих ситуаций: • Рабочим процессам Kaspersky Embedded Systems Security не хватает процессорного времени для обработки объектов. Обеспечьте выделение дополнительного процессорного времени для Kaspersky Embedded Systems Security, например, снизив нагрузку на компьютер со стороны других программ. • Возник сбой в работе Kaspersky Embedded Systems Security (простаивает несколько потоков). Перезапустите Kaspersky Embedded Systems Security.

Счетчики и ловушки SNMP Kaspersky Embedded Systems Security

Этот раздел содержит информацию о счетчиках и ловушках Kaspersky Embedded Systems Security.

В этом разделе

О счетчиках и ловушках SNMP Kaspersky Embedded Systems Security

Если вы включили компонент Счетчики и ловушки SNMP в состав устанавливаемых антивирусных компонентов, вы можете просматривать счетчики и ловушки Kaspersky Embedded Systems Security по протоколу Simple Network Management Protocol (SNMP).

Чтобы просматривать счетчики и ловушки Kaspersky Embedded Systems Security на рабочем месте администратора, запустите на защищаемом компьютере Службу SNMP, а на рабочем месте администратора – Службу SNMP и Службу ловушек SNMP.

SNMP-счетчики Kaspersky Embedded Systems Security

Этот раздел содержит таблицы с описанием параметров SNMP-счетчиков Kaspersky Embedded Systems Security.

В этом разделе

Счетчики производительности

Таблица 71. Счетчики производительности

Счетчик	Определение
currentRequestsAmount	Количество запросов, отправленных на обработку (см. стр. 487).
currentInfectedQueueLength	Количество элементов в очереди зараженных объектов (см. раздел "Количество элементов в очереди зараженных объектов" на стр. 488).
currentObjectProcessingRate	Количество объектов, обрабатываемых за секунду (см. стр. 489).
currentWorkProcessesNumber	Количество рабочих процессов Kaspersky Embedded Systems Security в текущий момент

Счетчики карантина

Таблица 72. Счетчики карантина

Счетчик	Определение
totalObjects	Количество объектов в папке карантина в текущий момент
totalSuspiciousObjects	Количество возможно зараженных объектов в папке карантина в текущий момент
currentStorageSize	Объем данных в папке карантина (МБ)

Счетчик резервного хранилища

Таблица 73. Счетчик резервного хранилища

Счетчик	Определение
currentBackupStorageSize	Объем данных в папке резервного хранилища (МБ)

Общие счетчики

Таблица 74. Общие счетчики

Счетчик	Определение
lastCriticalAreasScanAge	Период с момента проведения последней полной проверки важных областей компьютера (промежуток времени в секундах с момента последнего завершения задачи *Проверка важных областей*).
licenseExpirationDate	Дата окончания срока действия лицензии. Если добавлены активный и дополнительный ключи, отображается дата окончания срока действия лицензии, связанной с дополнительным ключом.
currentApplicationUptime	Время работы Kaspersky Embedded Systems Security с момента его последнего запуска, в сотых долях секунды
currentFileMonitorTaskStatus	Статус задачи Постоянная защита файлов: **Вкл.** – запущена; **Выкл.** – остановлена или приостановлена.

Счетчик обновления

Таблица 75. Счетчик обновления

Счетчик	Определение
avBasesAge	"Возраст" баз (промежуток времени в сотых долях секунды между датой создания последних установленных обновлений баз и текущим моментом).

Счетчики постоянной защиты

Таблица 76. Счетчики постоянной защиты

Счетчик	Определение
totalObjectsProcessed	Общее количество проверенных объектов с момента последнего запуска задачи Постоянная защита файлов
totalInfectedObjectsFound	Общее количество обнаруженных зараженных и других объектов с момента последнего запуска задачи Постоянная защита файлов
totalSuspiciousObjectsFound	Общее количество обнаруженных возможно зараженных объектов с момента последнего запуска задачи Постоянная защита файлов
totalVirusesFound	Общее количество обнаруженных объектов с момента последнего запуска задачи Постоянная защита файлов

Счетчик	Определение
totalObjectsQuarantined	Общее количество зараженных, возможно зараженных и других объектов, которые Kaspersky Embedded Systems Security поместил на карантин; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotQuarantined	Общее количество зараженных или возможно зараженных объектов, которые Kaspersky Embedded Systems Security пытался поместить на карантин, но это ему не удалось; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsDisinfected	Общее количество зараженных объектов, которые Kaspersky Embedded Systems Security вылечил; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotDisinfected	Общее количество зараженных и других объектов, которые Kaspersky Embedded Systems Security пытался вылечить, но это ему не удалось; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsDeleted	Общее количество зараженных, возможно зараженных и других объектов, которые Kaspersky Embedded Systems Security удалил; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotDeleted	Общее количество зараженных, возможно зараженных и других объектов, которые Kaspersky Embedded Systems Security должен был удалить, но это ему не удалось; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsBackedUp	Общее количество зараженных и других объектов, которые Kaspersky Embedded Systems Security поместил в резервное хранилище; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotBackedUp	Общее количество зараженных и других объектов, которые Kaspersky Embedded Systems Security пытался поместить в резервное хранилище, но это ему не удалось; рассчитывается с момента последнего запуска задачи Постоянная защита файлов

SNMP-ловушки Kaspersky Embedded Systems Security

Предусмотрены следующие параметры SNMP-ловушек Kaspersky Embedded Systems Security:

- eventThreatDetected: Обнаружен объект.

  Ловушка использует следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName

- objectName
- threatName
- detectType
- detectCertainty

- eventBackupStorageSizeExceeds: Превышен максимальный размер резервного хранилища. Общий объем данных в папке резервного хранилища превысил значение, указанное параметром **Максимальный размер резервного хранилища (МБ)**. Kaspersky Embedded Systems Security продолжает резервировать зараженные объекты.

  Ловушка использует следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventThresholdBackupStorageSizeExceeds: Достигнут порог свободного места в резервном хранилище. Размер свободного пространства в папке резервного хранилища, заданный параметром **Порог доступного пространства (МБ)**, уменьшился до указанного значения. Kaspersky Embedded Systems Security продолжает резервировать зараженные объекты.

  Ловушка использует следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventQuarantineStorageSizeExceeds: Превышен максимальный размер карантина. Общий объем данных в папке карантина превысил значение, указанное параметром **Максимальный размер карантина (МБ)**. Kaspersky Embedded Systems Security продолжает помещать возможно зараженные объекты на карантин.

  Ловушка использует следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventObjectNotQuarantined: Ошибка карантина.

  Ловушка использует следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason
- eventObjectNotBackuped: Ошибка сохранения копии объекта в резервном хранилище.

Ловушка использует следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- objectName
- userName
- computerName
- storageObjectNotAddedEventReason

- eventQuarantineInternalError: Внутренняя ошибка карантина.

  Ловушка использует следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventBackupInternalError: Ошибка резервного хранилища.

  Ловушка использует следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated: Базы программы устарели. Рассчитывается количество дней с момента последнего выполнения задачи обновления баз программы (локальной, групповой или задачи для наборов компьютеров).

  Ловушка использует следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventAVBasesTotallyOutdated: Базы программы сильно устарели. Рассчитывается количество дней с момента последнего выполнения задачи обновления баз программы (локальной, групповой или задачи для наборов компьютеров).

  Ловушка использует следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventApplicationStarted: программа Kaspersky Embedded Systems Security запущена.

  Ловушка использует следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventApplicationShutdown: программа Kaspersky Embedded Systems Security остановлена.

  Ловушка использует следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventCriticalAreasScanWasntPerformForALongTime: Проверка важных областей давно не выполнялась. Рассчитывается как количество дней с момента последнего завершения задачи Проверка важных областей.

  Ловушка использует следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventLicenseHasExpired: Срок действия лицензии истек.

  Ловушка использует следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventLicenseExpiresSoon: Срок действия лицензии скоро истечет. Рассчитывается количество дней, оставшихся до окончания срока действия лицензии.

  Ловушка использует следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventTaskInternalError: Ошибка выполнения задачи.

  Ловушка использует следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode

    - knowledgeBaseId
    - taskName
- eventUpdateError: Ошибка выполнения задачи обновления.

  Ловушка использует следующие параметры:

    - eventSeverity
    - eventDateAndTime
    - taskName
    - updaterErrorEventReason

Предусмотрены следующие параметры ловушек и их возможные значения:

- eventDateAndTime: дата и время события.
- eventSeverity: уровень важности.

  Параметр может принимать следующие значения:

    - critical (1) – критический;
    - warning (2) – предупреждение;
    - info (3) – информационный.
- userName: имя пользователя (например, пользователя, который пытался получить доступ к зараженному файлу).
- computerName: имя компьютера (например, компьютера, с которого пользователь пытался получить доступ к зараженному файлу).
- eventSource: функциональный компонент, в работе которого возникло событие.

  Параметр может принимать следующие значения:

    - unknown (0) – функциональный компонент не определен;
    - quarantine (1) – Карантин;
    - backup (2) – Резервное хранилище;
    - reporting (3) – Журналы выполнения задач;
    - updates (4)– Обновление;
    - realTimeProtection (5) – Постоянная защита файлов;
    - onDemandScanning (6) – Проверка по требованию;
    - product (7) – событие связано не с работой отдельных компонентов, а с работой Kaspersky Embedded Systems Security в целом;
    - systemAudit (8) – Журнал системного аудита.

- eventReason: причина возникновения события.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена;
  - reasonInvalidSettings (1) – только для событий резервного хранилища и карантина. Отображается, если недоступна папка карантина или папка резервного хранилища (недостаточно прав для доступа или папка неверно указана в параметрах карантина, например, указан сетевой путь). В этом случае Kaspersky Embedded Systems Security будет использовать папку резервного хранилища или папку карантина, установленную по умолчанию.

- objectName: имя объекта (например, имя файла, в котором обнаружен вирус).
- threatName: имя объекта согласно классификации Вирусной энциклопедии https://encyclopedia.kaspersky.ru/knowledge/classification/. Это имя входит в полное название обнаруженного объекта, которое Kaspersky Embedded Systems Security возвращает при обнаружении объекта. Полное имя обнаруженного объекта можно просмотреть в журнале выполнения задач (см. раздел "Настройка параметров журналов" на стр. 101).
- detectType: тип обнаруженного объекта.

  Параметр может принимать следующие значения:

  - undefined (0) – не определен;
  - virware – классические вирусы и сетевые черви;
  - trojware – троянские программы;
  - malware – прочие вредоносные программы;
  - adware – рекламные программы;
  - pornware – порнографические программы;
  - riskware – легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или личным данным.

- detectCertainty: степень уверенности обнаружения угрозы.

  Параметр может принимать следующие значения:

  - Suspicion (возможно зараженный) – программа Kaspersky Embedded Systems Security обнаружила частичное совпадение участка кода объекта с известным вредоносным кодом.
  - Sure (зараженный) – программа Kaspersky Embedded Systems Security обнаружила полное совпадение участка кода объекта с известным вредоносным кодом.

- days: количество дней (например, количество дней до окончания срока действия лицензии).
- errorCode: код ошибки.
- knowledgeBaseId: адрес статьи в базе знаний (например, адрес статьи, описывающей какую-либо ошибку).
- taskName: название задачи.
- updaterErrorEventReason: причина, по которой обновление не было применено.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена;
  - reasonAccessDenied – доступ запрещен;

- reasonUrlsExhausted – список источников обновлений исчерпан;
- reasonInvalidConfig – неправильный файл конфигурации;
- reasonInvalidSignature – неверная подпись;
- reasonCantCreateFolder – невозможно создать папку;
- reasonFileOperError – файловая ошибка;
- reasonDataCorrupted – объект поврежден;
- reasonConnectionReset – сброс соединения;
- reasonTimeOut – истекло время ожидания при соединении;
- reasonProxyAuthError – ошибка проверки подлинности на прокси-сервере;
- reasonServerAuthError – ошибка проверки подлинности на сервере;
- reasonHostNotFound – компьютер не найден;
- reasonServerBusy – сервер недоступен;
- reasonConnectionError – ошибка соединения;
- reasonModuleNotFound – объект не найден;
- reasonBlstCheckFailed(16) – ошибка проверки черного списка ключей. Возможно, в момент обновления публиковались обновления баз; повторите обновление через несколько минут.

- storageObjectNotAddedEventReason: причина, по которой объект не был помещен в резервное хранилище или на карантин.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена;
  - reasonStorageInternalError – ошибка базы данных; необходимо восстановление Kaspersky Embedded Systems Security.
  - reasonStorageReadOnly – база данных доступна только для чтения; необходимо восстановление Kaspersky Embedded Systems Security.
  - reasonStorageIOError – ошибка ввода-вывода: а) программа Kaspersky Embedded Systems Security повреждена и нуждается в восстановлении; б) диск, на котором хранятся файлы Kaspersky Embedded Systems Security, поврежден.
  - reasonStorageCorrupted – хранилище повреждено; необходимо восстановление Kaspersky Embedded Systems Security.
  - reasonStorageFull – база данных заполнена; требуется свободное место на диске.
  - reasonStorageOpenError – не удается открыть файл базы данных; необходимо восстановление Kaspersky Embedded Systems Security.
  - reasonStorageOSFeatureError – некоторые особенности операционной системы не отвечают требованиям Kaspersky Embedded Systems Security.
  - reasonObjectNotFound – помещаемый на карантин объект отсутствует на диске.
  - reasonObjectAccessError – недостаточно прав для использования Backup API: учетная запись, с правами которой выполняется операция, не обладает правами Backup Operator.
  - reasonDiskOutOfSpace – недостаточно места на диске.

Интеграция с WMI

Kaspersky Embedded Systems Security поддерживает интеграцию со стандартным инструментарием управления Windows - Windows Management Instrumentation (далее «WMI»): вы можете использовать клиентские системы, которые получают данные по стандарту Web-Based Enterprise Management (WBEM) с помощью WMI, для сбора данных о статусе программы Kaspersky Embedded Systems Security и ее компонентов.

В момент установки Kaspersky Embedded Systems Security регистрирует в системе собственный модуль, который обеспечивает создание пространства имен Kaspersky Embedded Systems Security в корневом пространстве имен WMI на локальном компьютере. Пространство имен Kaspersky Embedded Systems Security позволяет работать с классами, экземплярами классов и их свойствами в Kaspersky Embedded Systems Security.

Значения некоторых свойств экземпляра класса зависят от типа задачи.

Нецикличные задачи – это задачи программы, которые не имеют ограниченного срока действия и либо постоянно выполняются, либо остановлены. Для таких задач невозможно указать прогресс выполнения. Результаты выполнения задач фиксируются непрерывно в ходе работы задачи и представляют собой отдельные события (например, событие обнаружения зараженного объекта задачей постоянной защиты компьютера). Вы можете управлять задачами такого типа через политики Kaspersky Security Center.

Цикличные задачи – это задачи программы, срок выполнения которых ограничен, а прогресс выполнения может быть отображен в виде процента выполнения. Результаты выполнения таких задач фиксируются единожды по завершении задачи и представляют собой единый сформированный артефакт или факт изменения состояния программы (например, установленное обновление баз программы, сформированные конфигурационные файлы для задач формирования правил). На одном компьютере в одновременно может исполняться несколько цикличных задач одного типа (например, три задачи проверки по требованию с разными областями проверки). Вы можете управлять цикличными задачами через запуск групповых задач Kaspersky Security Center.

Если в вашей корпоративной сети используются инструменты, которые могут формировать запросы к пространству имен WMI и получать из них динамические данные, вы сможете получить следующие данные о текущем состоянии программы:

Таблица 77. Данные о состоянии программы

Свойство экземпляра класса	Описание	Значения
ProductName	The name of the application installed.	Полное название программы без номера версии.
ProductVersion	The full version of the application installed	Полный номер версии программы, включая номер сборки.
InstalledPatches	The array of patch display names that are deployed for the application.	Перечень критических исправлений, установленных для программы.

Свойство экземпляра класса	Описание	Значения
IsLicenseInstalled	The application activation state.	Статус ключа, с помощью которого активирована программа. Возможные значения: • False – В программе не задан ключ или код активации. • True - В программе добавлен ключ или код активации.
LicenseDaysLeft	Shows how many days are left before a current license expiration.	Количество дней, оставшихся до истечения срока действия текущей лицензии. Возможные неположительные значения: • 0 - Срок действия лицензии истек • -1 - Не удалось получить данные о текущем ключе или указанный ключ не может быть использован для активации программы (например, заблокирован по чёрному списку ключей).
AVBasesDatetime	The timestamp for a current anti-virus database version.	Дата и время формирования антивирусных баз, используемых в текущий момент. Если установленная программа не использует антивирусные базы, поле содержит значение “Not installed”.
IsExploitPreventionEnabled	The Exploit Prevention component state.	Статус компонента Защита от эксплойтов. Возможные значения: • True - Компонент Защита от эксплойтов включен и выполняет функции защиты. • False - Компонент Защита от эксплойтов не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение.
ProtectionTasksRunning	The array of protection tasks that are currently running.	Перечень задач защиты, контроля и мониторинга, запущенных в текущий момент. В данном поле должны учитываться все запущенные нецикличные задачи. Если ни одна из нецикличных задач не запущена, поле содержит значение «No».

Свойство экземпляра класса	Описание	Значения
IsAppControlRunning	The Applications Launch Control task state.	Статус выполнения задачи Контроль запуска программ. • True - Задача Контроль запуска программ выполняется в текущий момент. • False - Задача Контроль запуска программ не выполняется в текущий момент или компонент Контроль запуска программ не установлен.
AppControlMode	The Applications Launch Control task mode.	Описание текущего состояния компонента Контроль запуска программ, а также описывает режим, выбранный для соответствующей задачи. Возможные значения: • Active - в параметрах задачи указан **Активный** режим. • Statistics Only - в параметрах задачи указан режим **Только статистика**. • Not installed - Компонент Контроль запуска программ не установлен
AppControlRulesNumber	Total number of the applications launch control rules.	Количество правил, заданных в параметрах задачи Контроль запуска программ в текущий момент.
AppControlLastBlocking	The timestamp for the last application launch blocking by the Applications Launch Control task in any mode.	Дата и время последней блокировки запуска программы, выполненной компонентом Контроль запуска программ. При заполнении поля учитываются все блокировки программ, независимо от режима выполнения задачи. Если ни одно блокирование запуска не было зарегистрировано на момент выполнения запроса WMI, поле заполняется значением “No”.
PeriodicTasksRunning	The array of periodic tasks that are currently running.	Перечень задач проверки по требованию, обновления и инвентаризации, запущенных в текущий момент. В данном поле должны учитываться все запущенные задачи, которые относятся к типу цикличных. Если ни одна цикличная задача не запущена в текущий момент, поле содержит значение “No”.

Свойство экземпляра класса	Описание	Значения
ConnectionState	The state of the connection between WMI Provider component and the Kaspersky Security Service (KAVFS).	Информацию о статусе соединения между модулем WMI Provider и службой Kaspersky Security. Возможные значения: • Success - Соединение успешно установлено: клиент WMI может принимать данные о статусе программы. • Failed. Error Code: <code> - Соединение не удалось установить из-за ошибки с указанным кодом.

Указанные данные являются свойствами экземпляра класса KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security, где

- KasperskySecurity_ProductInfo – имя класса Kaspersky Embedded Systems Security;
- .ProductName=Kaspersky Embedded Systems Security – ключевой параметр Kaspersky Embedded Systems Security.

Экземпляр класса создается в пространстве имен ROOT\Kaspersky\Security.

Работа с Kaspersky Embedded Systems Security из командной строки

Этот раздел содержит описание работы с Kaspersky Embedded Systems Security из командной строки.

В этом разделе

Команды командной строки

Вы можете выполнять основные команды управления Kaspersky Embedded Systems Security из командной строки защищаемого компьютера, если при установке Kaspersky Embedded Systems Security вы включили компонент Утилита командной строки в список устанавливаемых.

С помощью команд командной строки вы можете управлять только функциями, доступными вам в соответствии с вашими правами в Kaspersky Embedded Systems Security.

Некоторые из команд Kaspersky Embedded Systems Security выполняются в следующих режимах:

- Синхронный режим: управление возвращается на Консоль только после завершения выполнения команды.
- Асинхронный режим: управление возвращается на Консоль сразу после запуска команды.

► *Чтобы прервать выполнение команды в синхронном режиме,*

нажмите на комбинацию клавиш **CTRL**+C.

При вводе команд Kaspersky Embedded Systems Security применяйте следующие правила:

- Вводите ключи и команды символами верхнего или нижнего регистра.
- Разделяйте ключи символом пробела.
- Если имя файла или папки, которое вы указываете в качестве значения ключа, содержит символ пробела, заключите путь к файлу или папке в кавычки, например: `"C:\TEST\test cpp.exe"`
- Если требуется, в масках имен файлов или путей используйте заместительные символы, например: “`C:\Temp\Temp*\`”, “`C:\Temp\Temp???.doc`”, “`C:\Temp\Temp*.doc`”

При помощи командной строки вы можете выполнить полный спектр операций по управлению и администрированию Kaspersky Embedded Systems Security (см. таблицу ниже).

Таблица 78. Команды Kaspersky Embedded Systems Security

Команда	Описание
KAVSHELL APPCONTROL (см. раздел "Заполнение списка правил контроля запуска программ из файла. KAVSHELL APPCONTROL" на стр. 519).	Дополняет список сформированных правил контроля запуска программ в соответствии с выбранным принципом добавления.
KAVSHELL APPCONTROL /CONFIG (см. раздел "Управление задачей Контроль запуска программ. KAVSHELL APPCONTROL /CONFIG" на стр. 516).	Управляет режимами работы задачи Контроль запуска программ.
KAVSHELL APPCONTROL /GENERATE (см. раздел "Формирование правил контроля запуска программ. KAVSHELL APPCONTROL /GENERATE" на стр. 517).	Запускает задачу Формирование правил контроля запуска программ.
KAVSHELL VACUUM (см. раздел "Дефрагментация файлов журнала событий Kaspersky Embedded Systems Security.KAVSHELL VACUUM" на стр. 528).	Дефрагментирует файлы журнала выполнения Kaspersky Embedded Systems Security.
KAVSHELL PASSWORD	Управляет параметрами защиты паролем.
KAVSHELL HELP (см. раздел "Вызов справки о командах Kaspersky Embedded Systems Security.KAVSHELL HELP" на стр. 507).	Вызывает справку о командах Kaspersky Embedded Systems Security.
KAVSHELL START (см. раздел "Запуск и остановка службы Kaspersky Security. KAVSHELL START, KAVSHELL STOP" на стр. 507)	Запускает службу Kaspersky Embedded Systems Security.
KAVSHELL STOP (см. раздел "Запуск и остановка службы Kaspersky Security. KAVSHELL START, KAVSHELL STOP" на стр. 507).	Останавливает службу Kaspersky Embedded Systems Security.
KAVSHELL SCAN (см. раздел "Проверка выбранной области.KAVSHELL SCAN" на стр. 508).	Создает и запускает временную задачу проверки по требованию с областью проверки и параметрами безопасности, заданными ключами команды.

Команда	Описание
KAVSHELL SCANCRITICAL (см. раздел "Запуск задачи Проверка важных областей.KAVSHELL SCANCRITICAL" на стр. 512).	Запускает системную задачу Проверка важных областей.
KAVSHELL TASK (см. раздел "Управление указанной задачей в асинхронном режиме.KAVSHELL TASK" на стр. 513).	Запускает, приостанавливает, возобновляет, останавливает указанную задачу в асинхронном режиме. Возвращает текущее состояние задачи / статистику задачи.
KAVSHELL RTP (см. раздел "Запуск и остановка задачи Постоянная защита.KAVSHELL RTP" на стр. 515).	Запускает или останавливает все задачи постоянной защиты.
KAVSHELL UPDATE (см. раздел "Запуск задачи Обновление баз Kaspersky Embedded Systems Security.KAVSHELL UPDATE" на стр. 521).	Запускает задачу обновления баз Kaspersky Embedded Systems Security с параметрами, указанными с помощью ключей команды.
KAVSHELL ROLLBACK (см. раздел "Откат обновления баз Kaspersky Embedded Systems Security.KAVSHELL ROLLBACK" на стр. 525).	Откатывает базы до предыдущей версии.
KAVSHELL LICENSE	Добавляет или удаляет ключи. Отображает информацию о добавленных ключах.
KAVSHELL TRACE (см. раздел "Включение, настройка и выключение журнала трассировки.KAVSHELL TRACE" на стр. 525).	Включает или выключает запись файла трассировки, управляет параметрами файла трассировки.
KAVSHELL DUMP (см. раздел "Включение и выключение файла дампа.KAVSHELL DUMP" на стр. 529).	Включает или выключает создание файлов дампов памяти процессов Kaspersky Embedded Systems Security при аварийном завершении процессов.
KAVSHELL IMPORT (см. раздел "Импорт параметров.KAVSHELL IMPORT" на стр. 531).	Импортирует общие параметры Kaspersky Embedded Systems Security, параметры его функций и задач из предварительно созданного конфигурационного файла.
KAVSHELL EXPORT (см. раздел "Экспорт параметров.KAVSHELL EXPORT" на стр. 531).	Экспортирует все параметры Kaspersky Embedded Systems Security и существующих задач в конфигурационный файл.

Команда	Описание
KAVSHELL DEVCONTROL (см. раздел "Наполнение списка правил контроля устройств.KAVSHELL DEVCONTROL" на стр. 520).	Дополняет список сформированных правил контроля устройств в соответствии с выбранным принципом добавления.

Отображение справки о командах Kaspersky Embedded Systems Security. KAVSHELL HELP

Чтобы получить список всех команд Kaspersky Embedded Systems Security, выполните одну из следующих команд:

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Чтобы получить описание и синтаксис команды, выполните одну из следующих команд:

```
KAVSHELL HELP <команда>

KAVSHELL <команда> /?
```

Примеры команды KAVSHELL HELP

Чтобы просмотреть подробную информацию о команде KAVSHELL SCAN, выполните команду

```
KAVSHELL HELP SCAN
```

Запуск и остановка службы Kaspersky Security. KAVSHELL START, KAVSHELL STOP

Чтобы запустить службу Kaspersky Security, выполните команду

```
KAVSHELL START
```

По умолчанию при запуске службы Kaspersky Security запускаются задачи Постоянная защита файлов и Проверка при старте системы, а также другие задачи, в расписании которых указана частота запуска **При запуске программы**.

Чтобы остановить службу Kaspersky Security, выполните команду

```
KAVSHELL STOP
```

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

Проверка указанной области. KAVSHELL SCAN

Чтобы запустить задачу проверки отдельных областей защищаемого компьютера, используйте команду `KAVSHELL SCAN`. Ключи этой команды задают параметры области проверки и параметры безопасности выбранного узла.

Задача проверки по требованию, запущенная с помощью команды `KAVSHELL SCAN`, является временной. Она отображается в Консоли программы только во время ее выполнения (в Консоли программы не отображаются параметры задачи). В то же время создается журнал выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** Консоли программы.

Указывая пути в задаче проверки отдельных областей, вы можете использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполняйте команду `KAVSHELL SCAN` с правами этого пользователя.

Команда `KAVSHELL SCAN` выполняется в синхронном режиме.

Чтобы запустить из командной строки существующую задачу проверки по требованию, используйте команду KAVSHELL TASK (см. раздел "Управление указанной задачей в асинхронном режиме.KAVSHELL TASK на стр. 513).

Синтаксис команды KAVSHELL SCAN

```
KAVSHELL SCAN <области проверки>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<имя файла со
списком областей проверки>] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>]
[/EM:<"маски">] [/ES:<размер>] [/ET:<количество секунд>] [/TZOFF]
[/OF:<SKIP|RESIDENT|SCAN[=<дни>] [NORECALL]>]
[/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/W:<имя файла журнала выполнения
задачи>] [/ANSI] [/ALIAS:<альтернативное название задачи>]
```

У команды KAVSHELL SCAN есть обязательные и дополнительные ключи (см. таблицу ниже).

Примеры команды KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA
/E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1
/NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Таблица 79. Ключи команды KAVSHELL SCAN

Ключ	Описание
Область проверки. Обязательный ключ.	
<файлы> <папки> <сетевой путь>	Область проверки – список файлов, папок, сетевых путей и стандартных областей. Указывайте сетевые пути в формате UNC (Universal Naming Convention). В следующем примере папка Folder4 указана без пути к ней – она находится в папке, из которой вы запускаете команду KAVSHELL: KAVSHELL SCAN Folder4 Если имя объекта, который вы хотите проверить, содержит пробелы, требуется заключить его в кавычки. Если вы выбрали папку, то Kaspersky Embedded Systems Security проверит также все вложенные подпапки для данной папки. Для проверки группы файлов вы можете использовать символы * или ?.
/MEMORY	Проверять объекты в оперативной памяти.
/SHARED	Проверять папки общего доступа на компьютере.
/STARTUP	Проверять объекты автозапуска.
/REMDRIVES	Проверять съемные диски.
/FIXDRIVES	Проверять жесткие диски.
/MYCOMP	Проверять все области защищаемого компьютера.
/L: <имя файла со списком областей проверки>	Имя файла со списком областей проверки, включая полный путь к файлу. Разделяйте области проверки в файле символом перевода строки. Вы можете указывать стандартные области проверки, как показано в следующем в примере файла со списком областей проверки: C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
Проверяемые объекты (File types). Если вы не укажете никаких значений этого ключа, Kaspersky Embedded Systems Security будет проверять объекты по формату.	
/FA	Проверять все объекты
/FC	Проверять объекты по формату (по умолчанию). Kaspersky Embedded Systems Security проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам.
/FE	Проверять объекты по расширению. Kaspersky Embedded Systems Security проверяет только объекты с расширениями, которые входят в список расширений, свойственных заражаемым объектам.
/NEWONLY	Проверять только новые и измененные файлы. Если вы не укажете этот ключ, Kaspersky Embedded Systems Security будет проверять все объекты.

Ключ	Описание
Действия над зараженными и другими обнаруженными объектами. Если вы не зададите никаких значений этого ключа, Kaspersky Embedded Systems Security будет выполнять действие **Пропускать**.	
DISINFECT	Лечить, если невозможно, пропускать. Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Embedded Systems Security для обеспечения совместимости с предыдущими версиями. Вы можете использовать эти параметры вместо ключей команд /AI: и /AS: В этом случае Kaspersky Embedded Systems Security не будет обрабатывать возможно зараженные объекты.
DISINFDEL	Лечить, если невозможно, удалять.
DELETE	Удалять Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Embedded Systems Security для обеспечения совместимости с предыдущими версиями. Вы можете использовать эти параметры вместо ключей команд /AI: и /AS: В этом случае Kaspersky Embedded Systems Security не будет обрабатывать возможно зараженные объекты.
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие
/AS: **Действия над возможно зараженными объектами**. Если вы не зададите никаких значений этого ключа, Kaspersky Embedded Systems Security выполнит действие **Пропускать**.	
QUARANTINE	Карантин
DELETE	Удалять
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие
Исключения	
/E:ABMSPO	Ключ исключает составные объекты следующих типов: A – SFX-архивы; B – почтовые базы; M – файлы почтовых форматов; S – архивы (включая SFX-архивы); P – упакованные объекты; O – вложенные OLE-объекты.
/EM:<"маски">	Исключать файлы по маске Можно указать несколько масок, например: EM:″*.txt; *.png; C\Videos*.avi″.
/ET:<количество секунд>	Прекращать обработку объекта, если она продолжается дольше указанного количества секунд. По умолчанию ограничений в продолжительности проверки нет.
/ES:<размер>	Исключать из проверки составные объекты, размер которых в мегабайтах превышает указанный значением <размер>. По умолчанию Kaspersky Embedded Systems Security проверяет объекты любого размера.

Ключ	Описание
/TZOFF	Отменить исключения доверенной зоны.
Дополнительные параметры (Options)	
/NOICHECKER	Выключить использование технологии iChecker (по умолчанию включено).
/NOISWIFT	Выключить использование технологии iSwift (по умолчанию включено).
/ANALYZERLEVEL:<уровень анализа>	Включить использование эвристического анализатора, настроить уровень анализа. Доступны следующие уровни эвристического анализа: 1 – поверхностный; 2 – средний; 3 – глубокий. Если вы опустите этот ключ, Kaspersky Embedded Systems Security не будет использовать эвристический анализатор.
/ALIAS:<альтернативное название задачи>	Ключ позволяет присвоить задаче проверки по требованию временное имя, по которому к задаче можно обращаться во время ее выполнения, например, чтобы просмотреть ее статистику с помощью команды TASK. Альтернативное название задачи должно быть уникальным среди альтернативных названий задач всех функциональных компонентов Kaspersky Embedded Systems Security. Если этот ключ не задан, задаче присваивается альтернативное название scan_<kavshell_pid>, например, scan_1234. В Консоли программы задаче присваивается название Проверка объектов (<дата и время>), например, Проверка объектов 16.08.2007 17:13:14.
Параметры журналов выполнения задач (Report settings)	
/W:<путь к файлу журнала выполнения задачи>	Если вы укажете этот ключ, Kaspersky Embedded Systems Security сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа. Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней. В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий Kaspersky Embedded Systems Security в оснастке "Просмотр событий". Вы можете указать как абсолютный, так и относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле Журналы выполнения задач Консоли программы. Если Kaspersky Embedded Systems Security не удается создать файл журнала, он не прерывает выполнение команды, но выдает сообщение об ошибке.

Ключ	Описание
/ANSI	Ключ позволяет записывать события в журнал выполнения задач в кодировке ANSI. Ключ ANSI не будет применяться, если не задан ключ W. Если ключ ANSI не указан, то журнал выполнения задач ведется в кодировке UNICODE.

Запуск задачи Проверка важных областей. KAVSHELL SCANCRITICAL

Используйте команду `KAVSHELL SCANCRITICAL`, чтобы запустить системную задачу проверки по требованию Проверка важных областей с параметрами, заданными в Консоли программы.

Синтаксис команды KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<имя файла журнала выполнения задачи>]
```

Примеры команды KAVSHELL SCANCRITICAL

Чтобы выполнить задачу проверки по требованию Проверка важных областей; сохранить журнал выполнения задачи в файле scancritical.log в текущей папке, выполните следующую команду:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

В зависимости от синтаксиса ключа /W вы можете настраивать местоположение файла журнала выполнения задачи (см. таблицу ниже).

Таблица 80. Синтаксис ключа /W команды KAVSHELL SCANCRITICAL

Ключ	Описание
/W:<имя файла журнала выполнения задачи>	Если вы укажете этот ключ, Kaspersky Embedded Systems Security сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа. Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней. В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий программы в оснастке "Просмотр событий". Вы можете указать как абсолютный, так и относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** Консоли программы. Если Kaspersky Embedded Systems Security не удается создать файл журнала, он не прерывает выполнение команды, но выдает сообщение об ошибке.

Управление указанной задачей в асинхронном режиме. KAVSHELL TASK

С помощью команды `KAVSHELL TASK` вы можете управлять указанной задачей: запускать, приостанавливать, возобновлять и останавливать задачу, а также просматривать ее текущее состояние и статистику. Команда выполняется в асинхронном режиме.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

Синтаксис команды KAVSHELL TASK

```
KAVSHELL TASK [<альтернативное название задачи> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS>]
```

Примеры команды KAVSHELL TASK

```
KAVSHELL TASK
```

```
KAVSHELL TASK on-access /START
```

```
KAVSHELL TASK user-task_1 /STOP
```

```
KAVSHELL TASK scan-computer /STATE
```

Команда `KAVSHELL TASK` может быть выполнена как без ключей, так и с использованием одного либо нескольких ключей (см. таблицу ниже).

Таблица 81. Ключи команды KAVSHELL TASK

Ключ	Описание
Без ключей	Команда возвращает список всех существующих задач Kaspersky Embedded Systems Security. Список содержит поля: альтернативное название задачи, категория задачи (системная или пользовательская) и текущий статус задачи.
<альтернативное название задачи>	Вместо названия задачи в команде SCAN TASK используйте ее альтернативное название (Task alias) – дополнительное, краткое имя, которое Kaspersky Embedded Systems Security присваивает задачам. Чтобы просмотреть альтернативные названия задач Kaspersky Embedded Systems Security, введите команду KAVSHELL TASK без ключей.
/START	Запустить указанную задачу в асинхронном режиме
/STOP	Остановить указанную задачу
/PAUSE	Приостановить указанную задачу
/RESUME	Возобновить указанную задачу в асинхронном режиме
/STATE	Получить текущее состояние задачи (например, *Выполняется*, *Завершена*, *Приостановлена*, *Остановлена*, *Завершена с ошибкой*, *Запускается*, *Восстанавливается*)
/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи по текущий момент

Обратите внимание, что не все задачи Kaspersky Embedded Systems Security полностью поддерживают эти ключи.

Коды возврата команды KAVSHELL TASK (см. раздел "Коды возврата команды KAVSHELL TASK" на стр. 535).

Регистрация KAVFS как системного защищенного процесса. Команда KAVSHELL CONFIG

Команда `KAVSHELL CONFIG` позволяет управлять регистрацией службы Kaspersky Security в качестве системного защищенного процесса (Protected Process Light) с помощью драйвера ELAM, установленного в операционной системе во время установки программы.

Синтаксис команды KAVSHELL CONFIG

```
KAVSHELL CONFIG /PPL:<ON|OFF>
```

Таблица 82. Ключи команды KAVSHELL CONFIG

Ключ	Описание
/PPL:ON	Регистрировать службу Kaspersky Security Service как PPL.
/PPL:OFF	Снять атрибут PPL со службы Kaspersky Security.

Программа отменяет регистрацию службы автоматически при выполнении любого из следующих действий:

- удаление программы;
- обновление программы;
- установка патча;
- восстановление компонентов программы.

Коды возврата команды KAVSHELL CONFIG.

Запуск и остановка задач постоянной защиты. KAVSHELL RTP

С помощью команды `KAVSHELL RTP` вы можете запустить или остановить все задачи постоянной защиты.

> Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

Синтаксис команды KAVSHELL RTP

```
KAVSHELL RTP </START | /STOP>
```

Примеры команды KAVSHELL RTP

Чтобы запустить все задачи постоянной защиты, выполните следующую команду:

```
KAVSHELL RTP /START
```

Команда `KAVSHELL RTP` может включать любой из двух обязательных ключей (см. таблицу ниже).

Таблица 83. Ключи команды KAVSHELL RTP

Ключ	Описание
/START	Запустить все задачи постоянной защиты компьютера: Постоянная защита файлов и Использование KSN.
/STOP	Остановить все задачи постоянной защиты.

Управление задачей Контроль запуска программ. KAVSHELL APPCONTROL /CONFIG

С помощью команды `KAVSHELL APPCONTROL /CONFIG` вы можете настраивать режим работы задачи Контроль запуска программ и контролировать загрузку DLL-модулей.

Синтаксис команды KAVSHELL APPCONTROL /CONFIG

```
 /config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
/savetofile:<полный путь к XML файлу>
```

Примеры команды KAVSHELL APPCONTROL /CONFIG

► *Чтобы выполнять задачу Контроль запуска программ в режиме **Активный** без загрузки DLL-модуля и сохранить параметры задачи по завершении, выполните команду:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Вы можете настраивать параметры задачи Контроль запуска программ с помощью ключей (см. таблицу ниже).

Таблица 84. Ключи команды KAVSHELL APPCONTROL /GENERATE

Ключ	Описание
`/mode:<applyrules|statistics>`	Режим работы задачи Контроль запуска программ. Вы можете выбрать один из следующих режимов работы задачи: • active - применяются правила контроля запуска программ; • statistics - Только статистика.
`/dll:<no|yes>`	Выключить или включить контроль загрузки DLL-модулей.
`/savetofile: <путь к xml-файлу>`	Экспортировать заданные правила в указанный файл в формате XML.
`/savetofile: <полное имя xml-файла>`	Сохранить список правил в файл.

Ключ	Описание
`/savetofile: <полное имя xml-файла> /sdc`	Сохранить список правил контроля распространения программного обеспечения в файл.
`/clearsdc`	Удалить все правила контроля распространения программного обеспечения.

Формирование правил контроля запуска программ. KAVSHELL APPCONTROL /GENERATE

С помощью команды `KAVSHELL APPCONTROL /GENERATE` вы можете формировать списки правил контроля запуска программ.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

Синтаксис команды KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <путь к папке> | /source:<путь к файлу со списком папок> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<пользователь или группа пользователей>] [/export:<полный путь к XML файлу>] [/import:<a|r|m>] [/prefix:<префикс для названий правил>] [/unique]
```

Примеры команды KAVSHELL APPCONTROL /GENERATE

- *Чтобы сформировать правила для файлов из указанных папок, выполните команду:*

  ```
  KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt /export:c:\rules\appctrlrules.xml
  ```

- *Чтобы сформировать правила для исполняемых файлов всех доступных расширений в указанной папке и по завершении задачи сохранить сформированные правила в указанный файл формата XML, выполните команду:*

  ```
  KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml
  ```

В зависимости от синтаксиса ключей вы можете настраивать параметры автоматического формирования правил контроля запуска программ (см. таблицу ниже).

Таблица 85. Ключи команды KAVSHELL APPCONTROL /GENERATE

Ключ	Описание
Область применения разрешающих правил	
<путь к папке>	Путь к папке, содержащей исполняемые файлы, для которых требуется автоматически создать разрешающие правила.
/source: <путь к файлу со списком папок>	Путь к файлу в формате TXT, содержащий список папок с исполняемыми файлами, для которых требуется автоматически создать разрешающие правила.
/masks: <edms>	Расширения исполняемых файлов, для которых требуется создать разрешающие правила контроля запуска программ. Вы можете включить в область срабатывания создаваемых правил файлы следующих расширений: • e - файлы с расширением exe; • d - файлы с расширением dll; • m - файлы с расширением msi; • s - скрипты.
/runapp	Учитывать при формировании разрешающих правил программы, запущенные на защищаемом компьютере в момент выполнения задачи.
Действия при автоматическом формировании разрешающих правил	
/rules: <ch|cp|h>	Указать действия, которые задача совершает во время формирования разрешающих правил контроля запуска программ: • ch - использовать цифровой сертификат. Если сертификат отсутствует, использовать хеш SHA256. • cp - использовать цифровой сертификат. Если сертификат отсутствует, использовать значение пути к исполняемому файлу. • h - использовать хеш SHA256.
/strong	Использовать заголовок и отпечаток цифрового сертификата при автоматическом формировании разрешающих правил контроля запуска программ. Команда выполняется, если указан параметр /rules: <ch|cp>.
/user: <пользователь или группа пользователей>	Указать имя пользователя или группы пользователей, для которых должны применяться правила. Программа будет контролировать запуски программ указанным пользователем и / или группой.
Действия по завершении формирования правил контроля запуска программ	
/export: <путь к XML-файлу>	Сохранять сформированные правила в файл формата XML.

Ключ	Описание
/unique	Добавлять информацию о компьютере, по программам которого формируются разрешающие правила контроля запуска программ.
/prefix: <префикс для названий правил>	Префикс названий при создании разрешающих правил контроля запуска программ.
/import: <a|r|m>	Импортировать сформированные правила в список заданных правил контроля запуска программ в соответствии с указанным принципом добавления новых правил: • a - **Добавлять к существующим правилам** (одинаковые правила дублируются); • r - **Заменять существующие правила** (новые правила добавляются вместо заданных правил); • m - **Объединять с существующими правилами** (добавляются новые правила, параметры которых не совпадают с параметрами уже заданных правил).

Заполнение списка правил контроля запуска программ. KAVSHELL APPCONTROL

С помощью команды `KAVSHELL APPCONTROL` вы можете добавлять правила в список правил задачи Контроль запуска программ из файла формата XML в соответствии с выбранным принципом, а также удалять все заданные правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

Синтаксис команды KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <полный путь к XML файлу> | /replace <полный путь к XML файлу> | /merge <полный путь к XML файлу> | /clear
```

Пример команды KAVSHELL APPCONTROL

► *Чтобы добавить к заданным правилам контроля запуска программ правила из файла формата XML по принципу Добавить к существующим правилам, выполните команду:*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

В зависимости от синтаксиса ключей вы можете выбирать принцип добавления новых правил из указанного файла формата XML в список заданных правил задачи Контроль запуска программ (см. таблицу ниже).

Таблица 86. Ключи команды KAVSHELL APPCONTROL

Ключ	Описание
/append <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного файла в формате XML. Принцип добавления - **Добавить к существующим правилам** (одинаковые правила дублируются).
/replace <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного файла в формате XML. Принцип добавления - **Заменить существующие правила** (новые правила добавляются вместо заданных правил).
/merge <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного файла в формате XML. Принцип добавления – **Объединить правила с существующими** (новые правила не дублируют уже заданные правила).
/clear	Очистить список правил контроля запуска программ.

Наполнение списка правил контроля устройств из файла. KAVSHELL DEVCONTROL

С помощью команды `KAVSHELL DEVCONTROL` вы можете добавлять правила в список правил задачи Контроль устройств из файла формата XML в соответствии с выбранным принципом, а также удалять все заданные правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

Синтаксис команды KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <полный путь к XML файлу> | /replace <полный путь к XML файлу> | /merge <полный путь к XML файлу> | /clear
```

Пример команды KAVSHELL DEVCONTROL

► *Чтобы добавить к заданным правилам контроля устройств правила из файла формата XML по принципу **Добавить к существующим правилам**, выполните команду:*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

В зависимости от синтаксиса ключей вы можете выбирать принцип добавления новых правил из указанного файла формата XML в список заданных правил задачи Контроль устройств (см. таблицу ниже).

Таблица 87. Ключи команды KAVSHELL DEVCONTROL

Ключ	Описание
/append <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного файла в формате XML. Принцип добавления - **Добавить к существующим правилам** (одинаковые правила дублируются).
/replace <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного файла в формате XML. Принцип добавления - **Заменить существующие правила** (новые правила добавляются вместо заданных правил).
/merge <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного файла в формате XML. Принцип добавления – **Объединить правила с существующими** (новые правила не дублируют уже заданные правила).
/clear	Очистить список правил контроля устройств.

Запуск задачи обновления баз Kaspersky Embedded Systems Security. KAVSHELL UPDATE

С помощью команды KAVSHELL UPDATE вы можете запускать задачу обновления баз Kaspersky Embedded Systems Security в синхронном режиме.

Задача обновления баз Kaspersky Embedded Systems Security, запущенная с помощью команды KAVSHELL UPDATE, является временной. Она отображается в Консоли программы только во время ее выполнения. В то же время создается журнал выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** Консоли программы. К задачам обновления, созданным и запущенным с помощью команды KAVSHELL UPDATE, и к задачам обновления, созданным в Консоли программы, могут применяться политики Kaspersky Security Center. Об управлении Kaspersky Embedded Systems Security на компьютерах с помощью программы Kaspersky Security Center читайте в разделе "Управление Kaspersky Embedded Systems Security из Kaspersky Security Center".

Указывая путь к источнику обновлений в этой задаче, вы можете использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполняйте команду KAVSHELL UPDATE с правами этого пользователя.

Синтаксис команды KAVSHELL UPDATE

```
KAVSHELL UPDATE <Источник обновления | /AK | /KL> [/NOUSEKL]
[/PROXY:<адрес>:<порт>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<имя пользователя>]
[/PROXYPWD:<пароль>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL]
[/NOFTPPASSIVE] [/TIMEOUT:<количество секунд>] [/REG:<код iso3166>] [/W:<имя
файла журнала выполнения задачи>] [/ALIAS:<альтернативное название задачи>]
```

У команды KAVSHELL UPDATE есть обязательные и дополнительные ключи (см. таблицу ниже).

Пример команды KAVSHELL UPDATE

► *Чтобы запустить пользовательскую задачу обновления баз программы, выполните следующую команду:*

```
KAVSHELL UPDATE
```

► *Чтобы запустить задачу обновления баз программы, файлы обновлений для которой хранятся в сетевой папке \\server\databases, выполните следующую команду:*

```
KAVSHELL UPDATE \\server\bases
```

► *Чтобы запустить задачу обновления с FTP-сервера ftp://dnl-ru1.kaspersky-labs.com/ и записать все события задачи в файл c:\update_report.log, выполните следующую команду:*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

► *Чтобы загрузить обновления баз Kaspersky Embedded Systems Security с сервера обновлений "Лаборатории Касперского", подключитесь к источнику обновлений с помощью прокси-сервера (адрес прокси-сервера: proxy.company.com, порт: 8080). Для доступа к компьютеру с помощью встроенной проверки подлинности Microsoft Windows (NTLM) с именем пользователя netuser и паролем 123456, выполните следующую команду:*

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1
/PROXYUSER:inetuser /PROXYPWD:123456
```

Таблица 88. Ключи команды KAVSHELL UPDATE

Ключ	Описание
Источники обновления (обязательный ключ). Укажите один или несколько источников. Kaspersky Embedded Systems Security будет обращаться к источникам в порядке их перечисления. Разделяйте источники символом пробела.	
<путь в формате UNC>	Пользовательские источники обновления. Путь к сетевой папке с обновлениями в формате UNC.
<URL>	Пользовательские источники обновления. Пользовательский источник обновлений – адрес HTTP- или FTP-сервера, на котором помещается папка с обновлениями.
<Локальная папка>	Пользовательские источники обновления. Папка на защищаемом компьютере.
/AK	Сервер администрирования Kaspersky Security Center в качестве источника обновлений.
/KL	Серверы обновлений "Лаборатории Касперского" в качестве источника обновлений
/NOUSEKL	Не использовать серверы обновлений "Лаборатории Касперского", если другие указанные источники обновлений недоступны (по умолчанию используются).

Ключ	Описание
Параметры прокси-сервера	
/PROXY:<адрес>:<порт>	Сетевое имя или IP-адрес прокси-сервера и его порт. Если вы не укажете этот ключ, Kaspersky Embedded Systems Security будет автоматически распознавать параметры прокси-сервера, который используется в локальной сети.
/AUTHTYPE:<0-2>	Этот ключ задает метод проверки подлинности для доступа к прокси-серверу. Он может принимать следующие значения: **0** – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Kaspersky Embedded Systems Security будет обращаться к прокси-серверу под учетной записью **Локальная система** (**SYSTEM**); **1** – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Kaspersky Embedded Systems Security будет обращаться к прокси-серверу под учетной записью, данные которой описаны ключами /PROXYUSER и /PROXYPWD; **2** – проверка подлинности по имени и паролю пользователя, заданным ключами /PROXYUSER и /PROXYPWD (Basic authentication). Если для доступа к прокси-серверу не требуется проверка подлинности, указывать этот ключ нет необходимости.
/PROXYUSER:<имя пользователя>	Имя пользователя, которое будет использоваться для доступа к прокси-серверу. Если вы укажете значение ключа /AUTHTYPE:0, то ключи /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются.
/PROXYPWD:<пароль>	Пароль пользователя, который будет использоваться для доступа к прокси-серверу. Если вы укажете значение ключа /AUTHTYPE:0, то ключи /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются. Если вы укажете ключ /PROXYUSER, а ключ /PROXYPWD опустите, считается что пароль пустой.
/NOPROXYFORKL	Не использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" (по умолчанию используются)
/USEPROXYFORCUSTOM	Использовать параметры прокси-сервера для соединения с пользовательскими источниками обновлений (по умолчанию не используются)
/USEPROXYFORLOCAL	Использовать параметры прокси-сервера для соединения с локальными источниками обновлений. Если не указано, применяется значение **Не использовать прокси-сервер для локальных адресов**.
Общие параметры FTP- и HTTP-сервера	
/NOFTPPASSIVE	Если указан этот ключ, Kaspersky Embedded Systems Security будет использовать активный режим FTP-сервера для соединения с защищаемым компьютером. Если вы не укажете этот ключ, Kaspersky Embedded Systems Security будет использовать пассивный режим FTP-сервера, если возможно.
/TIMEOUT:<количество секунд>	Время ожидания при соединении с FTP- или HTTP-сервером. Если вы не укажете этот ключ, Kaspersky Embedded Systems Security использует значение по умолчанию: 10 секунд. Значение ключа должно быть целым числом.

Ключ	Описание
/REG:<код iso3166>	Региональные параметры. Этот ключ используется при получении обновлений с серверов обновлений Лаборатории Касперского". Kaspersky Embedded Systems Security оптимизирует загрузку обновлений на защищаемый компьютер, выбирая ближайший к нему сервер обновлений. В качестве значения ключа укажите буквенный код страны местоположения защищаемого компьютера в соответствии со стандартом ISO 3166-1, например, /REG:gr или /REG:RU. Если ключ не указан или указан несуществующий код страны, Kaspersky Embedded Systems Security распознает местоположение защищаемого компьютера в соответствии с региональными параметрами компьютера, на котором установлена Консоль программы.
/ALIAS:<альтернативное название задачи>	Этот ключ позволяет присвоить задаче временное имя, по которому к ней можно обращаться во время ее выполнения. Например, вы можете просмотреть статистику задачи с помощью команды TASK. Альтернативное название задачи должно быть уникальным среди альтернативных названий задач всех функциональных компонентов Kaspersky Embedded Systems Security. Если этот ключ не задан, задаче присваивается альтернативное название update_<kavshell_pid>, например, update_1234. В Консоли программы задаче присваивается название Обновление баз программы (<дата и время>), например: Обновление баз программы 16.08.2007 17:41:02.
/W:<имя файла журнала выполнения задачи>	Если вы укажете этот ключ, Kaspersky Embedded Systems Security сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа. Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней. В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий Kaspersky Embedded Systems Security в оснастке "Просмотр событий". Вы можете указать как абсолютный, так и относительный путь к файлу журнала. Если вы укажите только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** Консоли программы. Если Kaspersky Embedded Systems Security не удается создать файл журнала, он не прерывает выполнение команды и не отображает сообщение об ошибке.

Коды возврата команды KAVSHELL UPDATE (на стр. 536).

Откат обновления баз Kaspersky Embedded Systems Security. KAVSHELL ROLLBACK

С помощью команды `KAVSHELL ROLLBACK` вы можете выполнить системную задачу Откат обновления баз – откатить базы Kaspersky Embedded Systems Security до предыдущих установленных обновлений. Команда выполняется синхронно.

Синтаксис команды

```
KAVSHELL ROLLBACK
```

Коды возврата команды KAVSHELL ROLLBACK (на стр. 536).

Управление анализом журналов. KAVSHELL TASK LOG-INSPECTOR

Команда `KAVSHELL TASK LOG-INSPECTOR` позволяет настроить контроль целостности среды, основываясь на анализе журнала событий Windows.

Синтаксис команды

```
KAVSHELL TASK LOG-INSPECTOR
```

Пример команды

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Таблица 89. Ключи команды KAVSHELL TASK LOG-INSPECTOR

Ключ	Описание
/START	Запустить указанную задачу в асинхронном режиме
/STOP	Остановить указанную задачу
/STATE	Получить текущее состояние задачи (например, *Выполняется*, *Завершена*, *Приостановлена*, *Остановлена*, *Завершена с ошибкой*, *Запускается*, *Восстанавливается*)
/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи по текущий момент

Команда "Коды возврата команды KAVSHELL TASK LOG-INSPECTOR" (см. раздел "Коды возврата команды KAVSHELL TASK LOG-INSPECTOR" на стр. 534).

Включение, настройка и выключение создания журнала трассировки. KAVSHELL TRACE

С помощью команды `KAVSHELL TRACE` вы можете включать или выключать ведение журнала трассировки всех подсистем Kaspersky Embedded Systems Security, а также устанавливать уровень детализации информации в журнале.

Kaspersky Embedded Systems Security записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде.

Синтаксис команды KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<папка с файлами журнала трассировки> [/S:<максимальный размер файла журнала в мегабайтах>] [/LVL:debug|info|warning|error|critical] | /OFF>
```

Если ведется журнал трассировки и вы хотите изменить его параметры, введите команду `KAVSHELL TRACE` с ключом /ON и задайте параметры журнала трассировки с помощью значений ключей /S и /LVL (см. таблицу ниже).

Таблица 90. Ключи команды KAVSHELL TRACE

Ключ	Описание
/ON	Включить ведение журнала трассировки.
/F:<папка с файлами журнала трассировки>	Этот ключ указывает полный путь к папке, в которой будут сохранены файлы журнала трассировки (обязательный ключ). Если вы укажете путь к несуществующей папке, журнал трассировки не будет создан. Пути к папкам на сетевых дисках других компьютеров указывать нельзя. Если имя папки, путь к которой вы указываете в качестве значения ключа, содержит символ пробела, заключите этот путь в кавычки, например: /F:"C\Trace Folder". Указывая путь к папке с файлами журнала трассировки, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/S: <максимальный размер файла журнала в мегабайтах>	Этот ключ устанавливает максимальный размер одного файла журнала трассировки. Как только файл журнала достигнет максимального размера, Kaspersky Embedded Systems Security начнет записывать информацию в новый файл; предыдущий файл журнала сохранится. Если вы не укажете этот ключ, максимальный размер одного файла журнала составит 50 МБ.
/LVL:debug|info|warning|error|critical	Этот ключ устанавливает уровень детализации журнала от максимального (**Вся отладочная информация**), при котором в журнал записываются все события, до минимального (**Критические события**), при котором в журнал записываются только критические события. Если вы не укажете этот ключ, в журнал трассировки будут записываться события с уровнем детализации **Вся отладочная информация**.
/OFF	Этот ключ выключает ведение журнала трассировки.

Примеры команды KAVSHELL TRACE

► *Чтобы включить ведение журнала трассировки с уровнем детализации **Вся отладочная информация** и максимальным размером файла журнала 200 МБ и сохранить файл журнала в папке C:\Trace Folder, выполните команду:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

► *Чтобы включить ведение журнала трассировки с уровнем детализации **Важные события** и сохранить файл журнала в папке C:\Trace Folder, выполните команду:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

► *Чтобы выключить ведение журнала трассировки, выполните команду:*

```
KAVSHELL TRACE /OFF
```

Коды возврата команды KAVSHELL TRACE (см. раздел "Коды возврата команды KAVSHELL TRACE" на стр. 537).

Дефрагментация файлов журнала событий Kaspersky Embedded Systems Security. KAVSHELL VACUUM

С помощью команды `KAVSHELL VACUUM` вы можете провести дефрагментацию файлов журнала событий программы. Она позволяет избежать системных ошибок и ошибок программы благодаря хранению большого количества файлов журнала, сформированных на основе событий программы.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

Рекомендуется применять команду `KAVSHELL VACUUM` для оптимизации хранения файлов отчетов при частых запусках задач проверки по требованию или задач обновления. При выполнении команды Kaspersky Embedded Systems Security обновляет логическую структуру файлов журнала событий программы, хранящихся на защищаемом компьютере по указанному пути.

По умолчанию файлы журнала событий программы сохраняются в папку C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports. Если вы вручную указали другой путь для хранения файлов журнала, команда `KAVSHELL VACUUM` выполняет дефрагментацию файлов в папке, указанной в параметрах журнала событий Kaspersky Embedded Systems Security.

Большой размер файлов журнала событий при дефрагментации увеличивает время выполнения команды `KAVSHELL VACUUM`.

Во время выполнения команды `KAVSHELL VACUUM` невозможно выполнение задач постоянной защиты компьютера и контроля компьютера. Процедура дефрагментации блокирует доступ к журналу событий Kaspersky Embedded Systems Security и запрещает запись событий в журнал. Во избежание снижения уровня безопасности рекомендуется заранее планировать выполнение команды `KAVSHELL VACUUM` в нерабочее время.

► *Чтобы выполнить дефрагментацию файлов журнала событий Kaspersky Embedded Systems Security, выполните команду:*

```
KAVSHELL VACUUM
```

Выполнение команды доступно при запуске с правами учетной записи локального администратора.

Очищение базы iSwift. KAVSHELL FBRESET

Kaspersky Embedded Systems Security использует технологию iSwift, позволяющую не проверять файл повторно, если с момента последней проверки он не был изменен (**Использовать технологию iSwift**).

Kaspersky Embedded Systems Security создает файлы klamfb.dat и klamfb2.dat в папке %SYSTEMDRIVE%\System Volume Information. Они содержат информацию об уже проверенных незараженных объектах. Размер файла klamfb.dat (klamfb2.dat) увеличивается пропорционально количеству файлов, проверенных Kaspersky Embedded Systems Security. В данном файле хранится только актуальная информация о существующих в системе файлах: если какой-либо файл удален, то Kaspersky Embedded Systems Security удаляет информацию о нем из файла klamfb.dat.

Для очищения данного файла используйте команду `KAVSHELL FBRESET`.

Учитывайте следующие особенности работы команды `KAVSHELL FBRESET`:

- При очистке файла klamfb.dat с помощью команды KAVSHELL FBRESET Kaspersky Embedded Systems Security не приостанавливает защиту (в отличие от удаления файла klamfb.dat вручную).
- После очистки файла klamfb.dat Kaspersky Embedded Systems Security может увеличить нагрузку на компьютер. При этом после очистки файла klamfb.dat Kaspersky Embedded Systems Security проверяет все файлы, к которым обращается впервые. После проверки Kaspersky Embedded Systems Security вновь заносит информацию о проверенных объектах в файл klamfb.dat. При повторном обращении к этому же объекту технология iSwift позволит не проверять файл повторно, если он не был изменен.

Для выполнения команды `KAVSHELL FBRESET` необходимо запускать командную строку под учетной записью SYSTEM.

Включение и выключение создания файла дампа. KAVSHELL DUMP

С помощью команды `KAVSHELL DUMP` можно включать и выключать создание образов памяти (файлов дампов) процессов Kaspersky Embedded Systems Security при аварийном завершении (см. таблицу ниже). Кроме этого вы можете в любой момент снять образы памяти выполняющихся процессов Kaspersky Embedded Systems Security.

Для успешного создания файла дампа, команда `KAVSHELL DUMP` должна быть запущена под учетной записью локальной системы (SYSTEM).

Синтаксис команды KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<папка с файлом дампа>|/SNAPSHOT /F:<папка с файлом дампа>
/ P:<pid> | /OFF>
```

Таблица 91. Ключи команды KAVSHELL DUMP

Ключ	Описание
/ON	Включает создание файла дампа процесса при его аварийном завершении.
/F:<папка с файлами дампов>	Это обязательный ключ. Обязательный ключ; указывает путь к папке, в которой будет сохранен файл дампа. Пути к папкам на сетевых дисках других незащищенных компьютеров указывать нельзя. Указывая путь к папке с файлом дампа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/SNAPSHOT	Снимает образ памяти выполняющегося процесса с указанным идентификатором и сохраняет файл дампа в папку, путь к которой указан ключом /F.
/P	Идентификатор PID процесса; отображается в Диспетчере задач Microsoft Windows.
/OFF	Выключает создание файла дампа при аварийном завершении.

Коды возврата команды KAVSHELL DUMP (см. раздел "Коды возврата команды KAVSHELL DUMP" на стр. 538).

Примеры команды KAVSHELL DUMP

► *Чтобы включить создание файла дампа; сохранять файл дампа в папку C:\Dump Folder, выполните команду:*

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

► *Чтобы снять образ памяти процесса с идентификатором 1234 в папку C:/Dumps, выполните команду:*

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /F:1234
```

► *Чтобы выключить создание файла дампа, выполните команду:*

```
KAVSHELL DUMP /OFF
```

Импорт параметров. KAVSHELL IMPORT

С помощью команды `KAVSHELL IMPORT` вы можете импортировать параметры Kaspersky Embedded Systems Security, функций и задач программы из конфигурационного файла в Kaspersky Embedded Systems Security на защищаемом компьютере. Вы можете создать конфигурационный файл с помощью команды `KAVSHELL EXPORT`.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

Синтаксис команды KAVSHELL IMPORT

```
KAVSHELL IMPORT <имя конфигурационного файла и путь к файлу>
```

Пример команды KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Таблица 92. Ключи команды KAVSHELL IMPORT

Ключ	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, из которого будут импортированы параметры. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Коды возврата команды KAVSHELL IMPORT (см. раздел "Коды возврата команды KAVSHELL IMPORT" на стр. 538).

Экспорт параметров. KAVSHELL EXPORT

С помощью команды `KAVSHELL EXPORT` вы можете экспортировать все параметры Kaspersky Embedded Systems Security и текущих задач программы в конфигурационный файл, чтобы потом импортировать их в Kaspersky Embedded Systems Security на другом компьютере.

Синтаксис команды KAVSHELL EXPORT

```
KAVSHELL EXPORT <имя конфигурационного файла и путь к файлу>
```

Пример команды KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Таблица 93. Ключи команды KAVSHELL EXPORT

Ключ	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, в котором будут сохранены параметры. Вы можете присвоить конфигурационному файлу любое расширение. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Коды возврата команды KAVSHELL EXPORT (см. раздел "Коды возврата команды KAVSHELL EXPORT" на стр. 539).

Интеграция с Microsoft Operations Management Suite. KAVSHELL OMSINFO

С помощью команды KAVSHELL OMSINFO можно просматривать статус программы и информацию об угрозах, обнаруженных антивирусными базами и службой KSN. Данные об угрозах поступают из доступных журналов событий.

Синтаксис команды KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <полный путь к сгенерированному файлу с именем файла>
```

Пример команды KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Таблица 94. Ключи команды KAVSHELL OMSINFO

Ключ	Описание
<путь к сгенерированному файлу с именем файла>	Имя сгенерированного файла, который будет содержать информацию о статусе программы и обнаруженных угрозах.

Коды возврата командной строки

В этом разделе

Коды возврата команд KAVSHELL START и KAVSHELL STOP

Таблица 95. Коды возврата команд KAVSHELL START и KAVSHELL STOP

Код возврата	Описание
0	Операция выполнена успешно
-3	Ошибка прав доступа
-5	Неверный синтаксис команды
-6	Неверная операция (например, служба Kaspersky Embedded Systems Security уже запущена или уже остановлена)
-7	Служба не зарегистрирована
-8	Автоматический запуск службы отключен
-9	Попытка запустить службу под другой учетной записью не была успешной (по умолчанию служба Kaspersky Embedded Systems Security работает под учетной записью Локальная система).
-99	Неизвестная ошибка

Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL

Таблица 96. Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL

Код возврата	Описание
0	Операция выполнена успешно (Угроз не обнаружено)
1	Операция отменена
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден файл со списком областей проверки)
-5	Неверный синтаксис команды или не определена область проверки
-80	Зараженных и других обнаруживаемых объектов
-81	Возможно зараженных объектов
-82	Обнаружены ошибки обработки
-83	Обнаружены непроверенные объекты
-84	Обнаружены поврежденные объекты
-85	Не удалось создать файл журнала выполнения задачи
-99	Неизвестная ошибка
-301	Недействительный ключ

Коды возврата команды KAVSHELL TASK LOG-INSPECTOR

Таблица 97. Код возврата команды KAVSHELL TASK LOG-INSPECTOR

Код возврата	Описание
0	Операция выполнена успешно
-6	Неверная операция (например, служба Kaspersky Embedded Systems Security уже запущена или уже остановлена)
402	Задача уже запущена (для ключа /STATE)

Коды возврата команды KAVSHELL TASK

Таблица 98. Коды возврата команды KAVSHELL TASK

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (задача не найдена)
-5	Неверный синтаксис команды
-6	Неверная операция (например, задача не запущена, уже запущена или не может быть приостановлена)
-99	Неизвестная ошибка
-301	Недействительный ключ
401	Задача не запущена (для ключа /STATE)
402	Задача уже запущена (для ключа /STATE)
403	Задача уже приостановлена (для ключа /STATE)
-404	Ошибка выполнения операции (изменение состояния задачи привело ее к сбою)

Коды возврата команды KAVSHELL RTP

Таблица 99. Коды возврата команды KAVSHELL RTP

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найдена какая-либо из задач постоянной защиты или все задачи постоянной защиты)
-5	Неверный синтаксис команды
-6	Неверная операция (например, задача уже запущена или уже остановлена)
-99	Неизвестная ошибка
-301	Недействительный ключ

Коды возврата команды KAVSHELL UPDATE

Таблица 100. Коды возврата команды KAVSHELL UPDATE

Код возврата	Описание
0	Операция выполнена успешно
200	Все объекты актуальны (базы или программные компоненты в актуальном состоянии)
-2	Служба не запущена
-3	Ошибка прав доступа
-5	Неверный синтаксис команды
-99	Неизвестная ошибка
-206	Файлы обновлений отсутствуют в указанном источнике или имеют неизвестный формат
-209	Ошибка подключения к источнику обновлений
-232	Ошибка аутентификации при подключении к прокси-серверу
-234	Ошибка подключения к программе Kaspersky Security Center
-235	Kaspersky Embedded Systems Security не прошел проверку подлинности при соединении с источником обновлений
-236	Базы программы повреждены
-301	Недействительный ключ

Коды возврата команды KAVSHELL ROLLBACK

Таблица 101. Коды возврата команды KAVSHELL ROLLBACK

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-99	Неизвестная ошибка
-221	Резервная копия баз не найдена
-222	Резервная копия баз повреждена

Коды возврата команды KAVSHELL LICENSE

Таблица 102. Коды возврата команды KAVSHELL LICENSE

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Недостаточно прав для управления ключами
-4	Ключ с указанным номером не найден
-5	Неверный синтаксис команды
-6	Неверная операция (ключ уже добавлен)
-99	Неизвестная ошибка
-301	Недействительный ключ
-303	Лицензия распространяется на другую программу

Коды возврата команды KAVSHELL TRACE

Таблица 103. Коды возврата команды KAVSHELL TRACE

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден путь, указанный в качестве пути к папке с файлами журнала трассировки)
-5	Неверный синтаксис команды
-6	Неверная операция (попытка выполнения команды KAVSHELL TRACE /OFF, если создание журнала трассировки уже выключено)
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL FBRESET

Таблица 104. Коды возврата команды KAVSHELL FBRESET

Код возврата	Описание
0	Операция выполнена успешно
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL DUMP

Таблица 105. Коды возврата команды KAVSHELL DUMP

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден путь, указанный в качестве пути к папке с файлом дампа; не найден процесс с указанным PID)
-5	Неверный синтаксис команды
-6	Неверная операция (попытка выполнения команды KAVSHELL DUMP /OFF, если создание файла дампа уже выключено)
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL IMPORT

Таблица 106. Коды возврата команды KAVSHELL IMPORT

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден импортируемый конфигурационный файл)
-5	Неверный синтаксис
-99	Неизвестная ошибка

Код возврата	Описание
501	Операция выполнена успешно, однако во время выполнения команды возникла ошибка / замечание, например, Kaspersky Embedded Systems Security не импортировал параметры какого-либо из функциональных компонентов
-502	Импортируемый файл отсутствует или имеет неизвестный формат
-503	Несовместимые параметры (конфигурационный файл экспортирован из другой программы или Kaspersky Embedded Systems Security более поздней или несовместимой версии)

Коды возврата команды KAVSHELL EXPORT

Таблица 107. Коды возврата команды KAVSHELL EXPORT

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-5	Неверный синтаксис
-10	Не удалось создать конфигурационный файл (например, нет доступа к папке, указанной в пути к файлу)
-99	Неизвестная ошибка
501	Операция выполнена успешно, однако во время выполнения команды возникла ошибка / замечание, например, Kaspersky Embedded Systems Security не экспортировал параметры какого-либо из функциональных компонентов

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить в Службу технической поддержки по телефону.
- Отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Получение технической поддержки по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2b).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "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.

Дополнительную информацию о Kaspersky CompanyAccount см. на веб-сайте Службы технической поддержки (http://support.kaspersky.ru/faq/companyaccount_help).

Использование файла трассировки и скрипта AVZ

После того как вы сообщите специалистам Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, вас могут попросить сформировать отчет с информацией о работе Kaspersky Embedded Systems Security и отправить его в Службу технической поддержки "Лаборатории Касперского". Также специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас создать файл трассировки. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

В результате анализа присланных вами данных специалисты Службы технической поддержки "Лаборатории Касперского" могут создать и отправить вам скрипт AVZ. Выполнение скриптов AVZ позволяет проводить анализ запущенных процессов на наличие угроз, проверять компьютер на наличие угроз, лечить или удалять зараженные файлы и создавать отчеты о результатах проверки системы.

Для более эффективного оказания поддержки в случае возникновения вопросов по работе программы специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить параметры программы. Для этого может потребоваться выполнение следующих действий:

- Активировать функциональность обработки и сохранения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения и отправки сохраняемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Глоссарий

K

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе данных "Лаборатории Касперского" с постоянно обновляемой информацией о репутации файлов, интернет-ресурсов и программного обеспечения. Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

O

OLE-объект

Объект, прикрепленный к другому файлу или вложенный в другой файл путем использования технологии Object Linking and Embedding (OLE). Например, OLE-объектом является таблица Microsoft Office Excel®, встроенная в документ Microsoft Office Word.

S

SIEM

Технология, которая обеспечивает анализ событий безопасности, исходящих от различных сетевых устройств и приложений.

A

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать вредоносный код в проверяемых объектах. Антивирусные базы создаются специалистами "Лаборатории Касперского" и обновляются каждый час.

Архив

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

З

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка компьютера и Обновление баз программы.

Зараженный объект

Объект, часть кода которого полностью совпадает с частью кода известной вредоносной программы. "Лаборатория Касперского" не рекомендует обрабатывать такие объекты.

К

Карантин

Папка, в которую программа "Лаборатории Касперского" перемещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде во избежание их воздействия на компьютер.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

Локальная задача

Задача, определенная и работающая на отдельном клиентском компьютере.

М

Маска файла

Представление имени файла с помощью специальных символов. Стандартными специальными символами, используемыми в масках файлов, являются * и ?, где * представляет любое количество символов, а ? представляет любой отдельный символ.

О

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Объекты автозапуска

Набор программ, 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.

П

Параметры задачи

Параметры программы, специфические для каждого типа задач.

Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на компьютерах одной группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

Постоянная защита

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект (на чтение, запись и исполнение) и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю, объекты, содержащие угрозы, или возможно зараженные объекты обрабатываются в соответствии с параметрами задачи (лечатся, удаляются или помещаются на карантин).

Потенциально заражаемый файл

Файл, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например, с расширением com, exe и dll. Риск проникновения вредоносного кода в такие файлы весьма высок.

Р

Резервное хранилище

Специальное хранилище для резервных копий файлов, которые создаются перед попыткой дезинфекции или удаления.

С

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского". Его также можно использовать для управления этими программами.

Срок действия лицензии

Период, в течение которого у вас есть доступ к функциям программы и право использовать дополнительные службы. Службы, которые вы можете использовать, зависят от типа лицензии.

Статус защиты

Текущий статус защиты, характеризующий степень защищенности компьютера.

У

Уровень безопасности

Уровень безопасности представляет собой предварительно заданный набор параметров компонентов программы.

Уровень важности события

Характеристика события, зафиксированного в работе программы "Лаборатории Касперского". Существуют четыре уровня важности:

- Критическое событие.
- Ошибка.
- Предупреждение.
- Информационное сообщение.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями

вредоносного программного обеспечения для проникновения в операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

Э

Эвристический анализатор

Технология обнаружения угроз, информация о которых еще не занесена в базы "Лаборатории Касперского". Эвристический анализатор позволяет обнаруживать объекты, поведение которых в операционной системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем защиты компьютеров от цифровых угроз: вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей (IDC Endpoint Tracker 2014).

"Лаборатория Касперского" основана в России в 1997 году. Сегодня “Лаборатория Касперского” – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3 000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программ: среди них Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu и ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей, а количество организаций, являющихся ее клиентами, превышает 270 000.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru

Kaspersky VirusDesk:	http://virusdesk.kaspersky.ru (для проверки подозрительных файлов и веб-сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Intel и Pentium – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Excel, Internet Explorer и Windows – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Предметный указатель

F

H

А

Б

В

Г

Д

Ж

З

И

К

Л

М

Н

О

П

Р

С

Т

Ф