KASPERSKY lab

# Kaspersky Embedded Systems Security

Руководство администратора

*Версия программы: 2.2.0.605*

Уважаемый пользователь!

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



Дата редакции документа: 29.10.2018



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

# Содержание

# Об этом руководстве

Kaspersky Embedded Systems Security 2.2.0.605 (далее также "Kaspersky Embedded Systems Security 2.2", "программа") адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Embedded Systems Security 2.2 на всех защищаемых устройствах, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Embedded Systems Security 2.2.

В этом руководстве вы можете найти информацию о настройке и использовании Kaspersky Embedded Systems Security 2.2.

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 2.2 содержит следующие разделы:

### Источники информации о Kaspersky Embedded Systems Security 2.2

Этот раздел содержит описание источников информации о программе.

### Kaspersky Embedded Systems Security 2.2

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Embedded Systems Security 2.2, перечень аппаратных и программных требований Kaspersky Embedded Systems Security 2.2.

### Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Embedded Systems Security 2.2.

### Интерфейс программы

Этот раздел содержит информацию об элементах интерфейса Kaspersky Embedded Systems Security 2.2.

### Лицензирование программы

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

### Запуск и остановка Kaspersky Embedded Systems Security 2.2

Этот раздел содержит информацию о запуске и остановке Плагина управления Kaspersky Embedded Systems Security 2.2 (далее также "Плагин управления") и службы Kaspersky Security.

### Права доступа к функциям Kaspersky Embedded Systems Security 2.2

Этот раздел содержит информацию о правах на управление Kaspersky Embedded Systems Security 2.2 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 задачами Kaspersky Embedded Systems Security 2.2 на нескольких компьютерах.

### Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security 2.2, их создании, настройке параметров выполнения, запуске и остановке.

### Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center.

### Постоянная защита компьютера

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

### Контроль активности на серверах

Этот раздел содержит информацию о функциональности Kaspersky Embedded Systems Security 2.2, которая позволяет контролировать запуски программ и подключения флеш-накопителей других 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 2.2 с функциями и технологиями сторонних производителей.

### Работа с Kaspersky Embedded Systems Security 2.2 из командной строки

Этот раздел содержит описание работы с Kaspersky Embedded Systems Security 2.2 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:<br>… | Примеры приведены в блоках на голубом фоне под заголовком "Пример". |
| Обновление – это...<br>Возникает событие Базы устарели. | Курсивом выделены следующие элементы текста:<br>• новые термины;<br>• названия статусов и событий программы. |
| Нажмите на клавишу ENTER.<br>Нажмите комбинацию клавиш ALT+F4. | Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами.<br>Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно. |
| Нажмите на кнопку Включить. | Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом. |

| Пример текста | Описание условного обозначения |
| --- | --- |
| ► *Чтобы настроить расписание задачи, выполните следующие действия:* | Вводные фразы инструкций выделены курсивом и значком "стрелка". |
| В командной строке введите текст `help`<br>Появится следующее сообщение:<br>Укажите дату в формате `ДД:ММ:ГГ`. | Специальным стилем выделены следующие типы текста:<br>• текст командной строки;<br>• текст сообщений, выводимых программой на экран;<br>• данные, которые требуется ввести с клавиатуры. |
| <Имя пользователя> | Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки. |

# Источники информации о Kaspersky Embedded Systems Security 2.2

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 2.2:

- страница Kaspersky Embedded Systems Security 2.2 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 2.2 на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Embedded Systems Security 2.2 (https://www.kaspersky.ru/enterprise-security/embedded-systems) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Embedded Systems Security 2.2 содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

### Страница Kaspersky Embedded Systems Security 2.2 в Базе знаний

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

На странице Kaspersky Embedded Systems Security 2.2 в Базе знаний (https://support.kaspersky.com/kess/) 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 2.2, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

### Документация Kaspersky Embedded Systems Security 2.2

В Руководстве администратора Kaspersky Embedded Systems Security 2.2 вы можете найти информацию об установке, удалении, настройке и использовании программы.

## Обсуждение программ "Лаборатории Касперского" на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и другими пользователями на нашем форуме http://forum.kaspersky.com/.

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

# Kaspersky Embedded Systems Security 2.2

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Embedded Systems Security 2.2, перечень аппаратных и программных требований Kaspersky Embedded Systems Security 2.2.

## В этом разделе



# О Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 защищает компьютеры и другие встроенные системы под управлением операционной системы Microsoft® Windows от вирусов и прочих угроз компьютерной безопасности. Пользователями Kaspersky Embedded Systems Security 2.2 являются администраторы сети организации и сотрудники, отвечающие за антивирусную защиту сети организации.

Kaspersky Embedded Systems Security 2.2 можно установить на различные встроенные системы под управлением Windows, включая устройства следующих типов:

- банковские автоматы;
- POS-терминалы.

Вы можете управлять Kaspersky Embedded Systems Security 2.2 следующими способами:

- через Консоль программы, установленную на одном компьютере с Kaspersky Embedded Systems Security 2.2 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 защитой многих компьютеров, на каждом из которых установлен Kaspersky Embedded Systems Security 2.2.

Вы можете просматривать счетчики производительности Kaspersky Embedded Systems Security 2.2 для программы "Системный монитор", а также счетчики и ловушки SNMP.

### Компоненты и функции Kaspersky Embedded Systems Security 2.2

В состав программы входят следующие компоненты:

- **Постоянная защита файлов**. Kaspersky Embedded Systems Security 2.2 проверяет объекты при обращении к ним. Kaspersky Embedded Systems Security 2.2 проверяет следующие объекты:
  - файлы;
  - альтернативные потоки файловых систем (NTFS-streams);
  - главную загрузочную запись и загрузочные секторы локальных жестких и съемных дисков.

- **Проверка по требованию**. Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 загружает обновления баз и модулей программы с FTP или HTTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или других источников обновлений.
- **Помещать на карантин** Kaspersky Embedded Systems Security 2.2 переносит объекты, которые он признает возможно зараженными, из исходного местоположения на *карантин*. В целях безопасности объекты на карантине хранятся в зашифрованном виде.
- **Резервное хранилище**. Kaspersky Embedded Systems Security 2.2 сохраняет зашифрованные копии объектов со статусами *зараженный* или *возможно зараженный* в *резервное 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 2.2 и состоянием антивирусной защиты компьютера.
- **Импорт и экспорт параметров**. Вы можете экспортировать параметры Kaspersky Embedded Systems Security 2.2 в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Embedded Systems Security 2.2 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 2.2.
- **Права доступа к функциям Kaspersky Embedded Systems Security**. Вы можете настраивать права пользователей и групп пользователей на управление Kaspersky Embedded Systems Security 2.2 и службами Windows, зарегистрированными программой.
- **Запись событий в журнал событий программы**. Kaspersky Embedded Systems Security 2.2 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 2.2, 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 2.2 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 2.2 появились следующие возможности и улучшения:

- Поддержка новых версий операционных систем Microsoft Windows.

  Реализованы механизмы самозащиты программы с помощью технологий ELAM и PPL: теперь во время установки программа автоматически регистрирует ELAM-драйвер, позволяющий запускать службу Kaspersky Security (kavfs.exe) с признаком Protected Process Light. Это позволяет усилить самозащиту программы и предотвратить широкий спектр атак.

  Функциональность доступна при установке программы на компьютеры под управлением операционных систем Microsoft Windows 10 RS2 (номер сборки: 15063) и более поздних версий.

- Поддержана проверка и обработка облачных файлов, расположенных в хранилище Microsoft OneDrive.

- Расширены возможности подсистемы контроля пакетов установки.

  Теперь вы можете указать, какие инсталляционные файлы могут передавать признак доверенного пакета установки по всей цепочке извлеченных из них файлов. Это позволяет повысить стабильность процессов установки программного обеспечения на компьютере с включенным контролем запуска программ, но также расширяет область потенциальной атаки через увеличение количества разрешенных запусков программ. Рекомендуется применять параметр в случаях, когда развертывание программного обеспечения выполняется по комплексной схеме, в том числе включающей необходимость перезагрузки компьютера в процессе распространения программного обеспечения.

- Реализована интеграция с инструментарием WMI.

  Теперь при установке программы автоматически создается пространство имен Kaspersky Security в корневом пространстве имен WMI на локальном компьютере. Вы можете использовать клиентские решения, поддерживающие запросы WMI, для получения данных о программе и о ее компонентах.

- Расширен формат вывода данных о программе и ее компонентах с помощью команды KAVSHELL OMSINFO: теперь вы можете получать данные о статусе задачи Контроль запуска программ, а также данные об установленных критических обновлениях модулей программы.

- Расширены возможности управления и мониторинга состояния программы с помощью Диагностического Окна:

  - Теперь вы можете просматривать изменения значений в счетчиках статистик для установленных компонентов с помощью Диагностического Окна на закладке **Статистика**.
  - Теперь вам не нужно вводить пароль на запросе доступа к Диагностическому окну при включенной парольной защите: программа ограничивает доступ к данным и элементам управления, отображаемым на Диагностическом Окне, только на основе установленных прав доступа на управление программой.

- Начиная с версии 2.2 в программе реализована возможность обеспечивать базовую защиту компьютера при запуске операционной системы в безопасном режиме.

  По умолчанию программа не работает в окружении, запущенном в безопасном режиме. Для того, чтобы программа запускалась при загрузке операционной системы в безопасном режиме, укажите значение 1 для параметра LoadInSafeMode в следующем ключе Реестра Windows:

  `HKLM\SYSTEM\CurrentControlSet\services\klam\Parameters`

  > При работе в окружении, запущенном в безопасном режиме, функциональность программы ограничена.

- Поддержаны отчеты Kaspersky Security Center о заблокированных стартах приложений и о статусе компонентов программы.

  Функциональность доступна при использовании Kaspersky Security Center 11.

- Ограничены права доступа для пользователей на изменение папки установки программы, а также на редактирование критичных веток реестра компонентов программы.

# Комплект поставки

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

- запустить мастер установки Kaspersky Embedded Systems Security 2.2;
- запустить мастер установки Консоли Kaspersky Embedded Systems Security 2.2;
- запустить мастер установки Плагина управления Kaspersky Embedded Systems Security 2.2, который позволяет управлять программой через Kaspersky Security Center;
- прочитать Руководство администратора;
- прочитать Руководство пользователя;
- перейти на страницу Kaspersky Embedded Systems Security 2.2 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 2.2.

Папка \console содержит файлы для установки Консоли программы (набор компонентов "Средства администрирования Kaspersky Embedded Systems Security 2.2").

Папка \product содержит следующие файлы:

- файлы для установки компонентов Kaspersky Embedded Systems Security 2.2 на компьютер под управлением 32-разрядной или 64-разрядной операционной системы Microsoft Windows;
- файл для установки Плагина управления Kaspersky Embedded Systems Security 2.2 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 плагина Kaspersky Embedded Systems Security 2.2 и компонентов программы 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 2.2*

| Файл | Назначение |
|---|---|
| autorun.inf | Файл автозапуска мастера установки Kaspersky Embedded Systems Security 2.2 при установке программы с переносных носителей. |
| ess_admin_guide_ru.pdf | Руководство администратора. |
| ess_user_guide_ru.pdf | Руководство пользователя. |
| 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 запуска мастера установки Kaspersky Embedded Systems Security 2.2 на защищаемом компьютере; запускает файл пакета установки ess.msi с указанными в мастере параметрами установки. |
| \product\ess_x86(x64).msi | Пакет установщика Windows; устанавливает Kaspersky Embedded Systems Security 2.2 на защищаемый компьютер. |
| \product\ess.kud | Файл в формате Kaspersky Unicode Definition с описанием пакета установки для удаленной установки Kaspersky Embedded Systems Security 2.2 через Kaspersky Security Center. |
| \product\klcfginst.exe | Программа установки Плагина управления Kaspersky Embedded Systems Security 2.2 через Kaspersky Security Center. Установите Плагин управления на каждый компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, если вы планируете с помощью нее управлять Kaspersky Embedded Systems Security 2.2. |
| \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. |

Вы можете запускать файлы, входящие в комплект поставки, с установочного компакт-диска. Если вы предварительно скопировали файлы на локальный диск, убедитесь, что сохранена структура файлов комплекта поставки.

# Аппаратные и программные требования

Перед установкой Kaspersky Embedded Systems Security 2.2 требуется удалить с компьютера другие антивирусные программы.

## Аппаратные требования к защищаемому компьютеру

Общие требования:

- x86-совместимые системы в однопроцессорной и многопроцессорной конфигурации.
- x64-совместимые системы в однопроцессорной и многопроцессорной конфигурации.

Объем дискового пространства для установки:

- компонента Контроль запуска программ – 50 МБ;
- для установки всех программных компонентов Kaspersky Embedded Systems Security 2.2 – 500 МБ.

Объем оперативной памяти:

- 256 МБ при установке компонента Контроль запуска программ на устройстве под управлением операционных систем Microsoft® Windows;
- 512 МБ при установке всех компонентов программы на устройстве под управлением операционных систем Microsoft Windows.

Минимальные требования к процессору:

- для 32-разрядных операционных систем Microsoft Windows: Intel® Pentium® III.
- для 64-разрядных операционных систем Microsoft Windows: Intel Pentium IV.

## Программные требования к защищаемому компьютеру

Вы можете установить Kaspersky Embedded Systems Security 2.2 на устройстве 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 Microsoft Windows Installer 3.1.

Для установки и работы Kaspersky Embedded Systems Security 2.2 на устройстве под управлением встроенных операционных систем требуется наличие компонентов Filter Manager и Administration Support Tools.

Вы можете установить Kaspersky Embedded Systems Security 2.2 на компьютере под управлением одной из следующих 32- или 64-разрядных операционных систем Microsoft Windows:

- Windows XP Embedded SP3
- Windows XP Professional SP2 / SP3
- Windows Embedded POSReady 2009

- Windows Embedded Standard 7 SP1
- Windows Embedded Enterprise 7 SP1
- Windows Embedded POSReady 7
- Windows 7 Professional / Enterprise SP1
- Windows Embedded 8.1 Industry Professional / Enterprise
- Windows Embedded 8.1 Professional
- Windows Embedded 8.0 Standard
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise
- Windows 10 IoT Enterprise
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise

# Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Embedded Systems Security 2.2.

## В этом разделе



# Программные компоненты Kaspersky Embedded Systems Security 2.2 и их коды для службы установщика Windows

По умолчанию файлы \server\ess_x86(x64).msi устанавливают все программные компоненты Kaspersky Embedded Systems Security 2.2. Вы можете включить установку данного компонента при выборочной установке программы.

Файлы \client\esstools_x86(x64).msi устанавливают все программные компоненты набора "Средства администрирования".

В следующих разделах приводятся коды компонентов Kaspersky Embedded Systems Security 2.2 для службы установщика Windows. Вы можете использовать эти коды, чтобы задать список устанавливаемых компонентов при установке Kaspersky Embedded Systems Security 2.2 из командной строки.

## В этом разделе

# Компоненты программы Kaspersky Embedded Systems Security 2.2

В следующей таблице содержатся коды и описание программных компонентов Kaspersky Embedded Systems Security 2.2.

*Таблица 3. Описание программных компонентов Kaspersky Embedded Systems Security 2.2*

| Компонент | Код | Выполняет функции |
|---|---|---|
| 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 его в соответствии с заданными правилами контроля запуска программ.<br>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.<br>Компонент реализуется в задаче Контроль устройств. |
| Антивирусная защита | AVProtection | Этот компонент обеспечивает антивирусную защиту и включает в себя следующие компоненты:<br>• Проверка по требованию<br>• Постоянная защита файлов |
| Проверка по требованию | Ods | Этот компонент устанавливает системные файлы Kaspersky Embedded Systems Security 2.2 и задачи проверки по требованию (проверка объектов защищаемого компьютера, выполняемая по требованию).<br>Если, устанавливая Kaspersky Embedded Systems Security 2.2 из командной строки, вы укажете другие компоненты Kaspersky Embedded Systems Security 2.2, не указывая компонент Core, компонент Core будет установлен автоматически. |
| Постоянная защита файлов | Oas | Этот компонент обеспечивает антивирусную проверку файлов на защищаемом компьютере при обращении к этим файлам.<br>Компонент реализует задачу Постоянная защита файлов. |

| Компонент | Код | Выполняет функции |
|---|---|---|
| Использование Kaspersky Security Network | Ksn | Этот компонент реализует защиту на основе облачных технологий "Лаборатории Касперского".<br>Компонент реализует задачу Использование KSN (отправка запросов и получение заключений от службы Kaspersky Security Network). |
| Мониторинг файловых операций | Fim | Этот компонент позволяет фиксировать операции производимые над файлами в выбранной области мониторинга.<br>Компонент реализуется в задаче 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 2.2.<br>Компонент реализуется в задаче Управление сетевым экраном. |
| Модуль интеграции с Агентом администрирования Kaspersky Security Center | AKIntegration | Обеспечивает связь Kaspersky Embedded Systems Security 2.2 с Агентом администрирования Kaspersky Security Center.<br>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. |
| Набор счетчиков производительности программы "Системный монитор" | PerfMonCounters | Компонент устанавливает набор счетчиков производительности программы "Системный монитор". Эти счетчики позволяют измерять производительность Kaspersky Embedded Systems Security 2.2 и находить возможные узкие места при совместной работе Kaspersky Embedded Systems Security 2.2 с другими программами. |
| Поддержка SNMP-протокола | SnmpSupport | Компонент публикует счетчики и ловушки Kaspersky Embedded Systems Security 2.2 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. |

| Компонент | Код | Выполняет функции |
|---|---|---|
| Значок Kaspersky Embedded Systems Security 2.2 в области уведомлений | TrayApp | Компонент отображает значок Kaspersky Embedded Systems Security 2.2 в области уведомлений панели задач защищаемого компьютера. Значок Kaspersky Embedded Systems Security 2.2 показывает состояние защиты компьютера и позволяет открыть Консоль Kaspersky Embedded Systems Security 2.2 в Microsoft Management Console, если она установлена, и окно **О программе**. |
| Утилита командной строки | Shell | Позволяет управлять Kaspersky Embedded Systems Security 2.2 из командной строки защищаемого компьютера. |

## Программные компоненты набора "Средства администрирования"

В следующей таблице содержатся 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 2.2 | MmcSnapin | Компонент устанавливает оснастку Microsoft Management Console для управления через Консоль Kaspersky Embedded Systems Security 2.2.<br>Если, устанавливая набор "Средства администрирования" из командной строки, вы укажете другие компоненты набора, не указывая компонент MmcSnapin, компонент MmcSnapin будет установлен автоматически. |
| Справка | Help | chm-файл справки; сохраняется в папке с файлами Средств администрирования Kaspersky Embedded Systems Security 2.2. Вы можете открыть файл справки из меню **Пуск** или с помощью клавиши **F1** при открытом окне Консоли программы. |
| Документация | Help | Kaspersky Embedded Systems Security 2.2 добавляет ярлык для перехода на веб-сайт "Лаборатории Касперского", где документы "Руководство администратора" и "Руководство пользователя" доступны в формате PDF. Вы можете открыть Руководство администратора из меню **Пуск**. |

# Изменения в системе после установки Kaspersky Embedded Systems Security 2.2

При установке Kaspersky Embedded Systems Security 2.2 и Консоли программы (из набора "Средства администрирования") служба установщика Windows выполняет на защищаемом компьютере следующие изменения:

- создает папки Kaspersky Embedded Systems Security 2.2 на защищаемом компьютере и на компьютере, где установлена Консоль программы;
- регистрирует службы Kaspersky Embedded Systems Security 2.2;
- создает группу пользователей Kaspersky Embedded Systems Security 2.2;
- регистрирует ключи Kaspersky Embedded Systems Security 2.2 в системном реестре.

Эти изменения описаны в таблице ниже.

### Папки Kaspersky Embedded Systems Security 2.2

*Таблица 5. Папки Kaspersky Embedded Systems Security 2.2 на защищаемом компьютере*

| Папка | Файлы Kaspersky Embedded Systems Security 2.2 |
|---|---|
| Заданная по умолчанию папка установки Kaspersky Embedded Systems Security 2.2:<br>в Microsoft Windows 32-разрядной версии – %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\<br>в Microsoft Windows 64-разрядной версии – %ProgramFiles(x86)%\Kaspersky Embedded Systems Security\ | Исполняемые файлы Kaspersky Embedded Systems Security 2.2 (папка назначения, указанная при установке). |
| Папка %Kaspersky Embedded Systems Security%\mibs | Файлы Management Information Base (MIB); содержат описание счетчиков и ловушек, публикуемых Kaspersky Embedded Systems Security 2.2 по протоколу SNMP. |
| Папка %Kaspersky Embedded Systems Security%\x64 | 64-разрядные версии исполняемых файлов Kaspersky Embedded Systems Security 2.2 (папка создается только при установке Kaspersky Embedded Systems Security 2.2 в Microsoft Windows 64-разрядной версии). |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Data\<br>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Settings\<br>%ALLUSERSPROFILE%\Application Data\Kaspersky Embedded Systems Security\2.2\Dskm\ | Служебные файлы Kaspersky Embedded Systems Security 2.2. |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\ | Файлы с параметрами источников обновлений. |

| Папка | Файлы Kaspersky Embedded Systems Security 2.2 |
|---|---|
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\Distribution\ | Обновления баз и программных модулей, полученные с помощью задачи Копирование обновлений (папка создается при первом получении обновлений с помощью задачи Копирование обновлений). |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Reports\ | Журналы выполнения задач и журнал системного аудита. |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Current\ | Набор баз, используемых в текущий момент. |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Backup\ | Резервная копия баз; перезаписывается при каждом обновлении баз. |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Temp\ | Временные файлы, создаваемые во время выполнения задач обновления. |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Quarantine\ | Объекты на карантине (папка по умолчанию). |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Backup\ | Объекты в резервном хранилище (папка по умолчанию). |
| %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored\ | Объекты, восстановленные из резервного хранилища и карантина (папка для восстановленных объектов по умолчанию). |

*Таблица 6. Папки, создаваемые при установке Консоли программы*

| Папка | Файлы Консоли Kaspersky Embedded Systems Security 2.2 |
|---|---|
| Заданная по умолчанию папка установки Консоли программы:<br>• в Microsoft Windows 32-разрядной версии – %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\<br>• в Microsoft Windows 64-разрядной версии – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\ | Файлы набора "Средства администрирования" (папка назначения, указанная при установке Консоли Kaspersky Embedded Systems Security 2.2). |

### Службы Kaspersky Embedded Systems Security 2.2

Службы Kaspersky Embedded Systems Security 2.2 запускаются под системной учетной записью "Локальная система" (SYSTEM).

*Таблица 7. Службы Kaspersky Embedded Systems Security 2.2*

| Служба | Назначение |
|---|---|
| Служба Kaspersky Security (KAVFS) | Основная служба Kaspersky Embedded Systems Security 2.2, которая управляет задачами и рабочими процессами Kaspersky Embedded Systems Security 2.2. |
| Служба Kaspersky Security Management (KAVFSGT) | Служба, предназначенная для управления Kaspersky Embedded Systems Security 2.2 через Консоль программы. |

### Группы Kaspersky Embedded Systems Security 2.2

*Таблица 8. Группы Kaspersky Embedded Systems Security 2.2*

| Группа | Назначение |
|---|---|
| ESS Administrators | Группа на защищаемом компьютере, пользователи которой имеют полный доступ к службе Kaspersky Security Management, а также доступ ко всем функциям Kaspersky Embedded Systems Security 2.2. |

### Ключи системного реестра

*Таблица 9. Ключи системного реестра*

| Ключ | Назначение |
|---|---|
| [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS] | Параметры службы Kaspersky Embedded Systems Security 2.2. |
| [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security] | Параметры журнала событий Kaspersky Embedded Systems Security 2.2 (Kaspersky Event Log). |
| [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT] | Параметры службы управления Kaspersky Embedded Systems Security 2.2. |
| В Microsoft Windows 32-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]<br>В Microsoft Windows 64-разрядной версии:<br>[[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]. | Параметры счетчиков производительности. |

| Ключ | Назначение |
|---|---|
| В Microsoft Windows 32-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\SnmpAgent]<br>В Microsoft Windows 64-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\SnmpAgent] | Параметры компонента "Поддержка SNMP-протокола". |
| В Microsoft Windows 32-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\CrashDump]<br>В Microsoft Windows 64-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\CrashDump] | Параметры записи файла дампа. |
| В Microsoft Windows 32-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\Trace]<br>В Microsoft Windows 64-разрядной версии:<br>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Trace] | Параметры файла трассировки. |
| [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Environment] | Параметры задач и функций программы. |

# Процессы Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 запускает процессы, описанные в таблице ниже.

*Таблица 10. Процессы Kaspersky Embedded Systems Security 2.2*

| Имя файла | Назначение |
|---|---|
| kavfswp.exe | Рабочий процесс Kaspersky Embedded Systems Security 2.2 |
| kavtray.exe | Процесс значка области уведомлений |
| kavshell.exe | Процесс утилиты командной строки |
| kavfsrcn.exe | Процесс удаленного управления Kaspersky Embedded Systems Security 2.2 |
| 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 следующих таблицах описаны параметры установки и удаления Kaspersky Embedded Systems Security 2.2 и их значения по умолчанию, указаны ключи для изменения значений 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 2.2 из командной строки.

*Таблица 11. Параметры установки и ключи командной строки в установщике Windows*

| Параметр | Ключ командной строки для установщика Windows и его значения | Значение по умолчанию | Описание |
|---|---|---|---|
| Принятие условий Лицензионного соглашения | EULA=<значение><br>0 – вы отклоняете условия Лицензионного соглашения.<br>1 – вы принимаете условия Лицензионного соглашения. | 0 | Вам нужно принять условия Лицензионного соглашения для установки Kaspersky Embedded Systems Security 2.2. |
| Принятие Политики конфиденциальности | PRIVACYPOLICY=<значение><br>0 – вы отклоняете условия Политики конфиденциальности.<br>1 – вы принимаете условия Политики конфиденциальности. | 0 | Вам нужно принять условия Политики конфиденциальности для установки Kaspersky Embedded Systems Security 2.2. |
| Папка назначения | INSTALLDIR=<полный путь к папке> | Kaspersky Embedded Systems Security 2.2: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security<br>Средства администрирования: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools<br>В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%. | Папка, в которой будут сохранены файлы Kaspersky Embedded Systems Security 2.2 при его установке.<br>Вы можете указать другую папку. |

| Параметр | Ключ командной строки для установщика Windows и его значения | Значение по умолчанию | Описание |
|---|---|---|---|
| Запуск Постоянной защиты файлов при запуске Kaspersky Embedded Systems Security 2.2 (**Включить постоянную защиту после установки программы**) | RUNRTP=<значение><br>1 – запустить;<br>0 – не запускать. | 1 | Включите этот параметр, чтобы запустить Постоянную защиту файлов при запуске Kaspersky Embedded Systems Security 2.2 (рекомендуется). |
| Исключения из проверки, рекомендуемые корпорацией Microsoft (**Добавить к исключениям файлы, рекомендованные Microsoft**) | ADDMSEXCLUSION=<значение><br>1 – исключать;<br>0 – не исключать. | 1 | В задаче Постоянная защита файлов: исключать из области защиты объекты на компьютере, которые рекомендует исключать корпорация Microsoft.<br>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. |
| Исключения из проверки, рекомендуемые "Лабораторией Касперского" (**Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**) | ADDKLEXCLUSION=<значение><br>1 – исключать;<br>0 – не исключать. | 1 | В задаче Постоянная защита файлов: исключать из области защиты объекты на компьютере, которые рекомендует исключать "Лаборатория Касперского". |

| Параметр | Ключ командной строки для установщика Windows и его значения | Значение по умолчанию | Описание |
|---|---|---|---|
| Разрешить удаленное подключение к Консоли программы | ALLOWREMOTECON=<значение><br>1 – разрешать;<br>0 – не разрешать. | 0 | По умолчанию удаленное подключение к Консоли программы, установленной на защищаемом компьютере, не разрешено. Во время установки вы можете разрешить подключение. Kaspersky Embedded Systems Security 2.2 создаст разрешающие правила для процесса kavfsgt.exe по протоколу TCP для всех портов. |
| Путь к файлу ключа (**Ключ**) | LICENSEKEYPATH=<имя файла ключа> | Папка \product в комплекте поставки | По умолчанию программа установки пытается найти файл с расширением key в папке \product комплекта поставки.<br>Если в папке \product находится несколько файлов ключа, программа установки выбирает файл ключа с самой поздней датой истечения срока действия.<br>Можно предварительно сохранить файл ключа в папке \product или указать другой путь к файлу ключа с помощью параметра **Добавление ключа**. |

| Параметр | Ключ командной строки для установщика Windows и его значения | Значение по умолчанию | Описание |
|---|---|---|---|
| | | | Вы можете добавить ключ после установки Kaspersky Embedded Systems Security 2.2 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 2.2 не будет функционировать. |
| Путь к конфигурационному файлу | CONFIGPATH=<имя конфигурационного файла> | Не указан | Kaspersky Embedded Systems Security 2.2 импортирует параметры из указанного конфигурационного файла, созданного в программе.<br>Kaspersky Embedded Systems Security 2.2 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.<br>Если вы не укажете конфигурационный файл, после установки программа начнет работать с параметрами по умолчанию. |

| Параметр | Ключ командной строки для установщика Windows и его значения | Значение по умолчанию | Описание |
|---|---|---|---|
| Разрешение сетевых соединений для Консоли | ADDWFEXCLUSION=<значение><br>**1** – разрешать;<br>**0** – не разрешать. | 0 | Используйте этот параметр, если вы устанавливаете Kaspersky Embedded Systems Security 2.2 не на защищаемом компьютере. Вы можете удаленно управлять защитой компьютера с другого устройства, на котором установлена Консоль Kaspersky Embedded Systems Security 2.2.<br>В брандмауэре Microsoft Windows будет открыт TCP-порт 135, разрешены сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Embedded Systems Security 2.2 kavfsrcn.exe и открыт доступ к DCOM-программам.<br>После завершения установки добавьте пользователей, которые будут управлять программой удаленно, в группу ESS Administrators и разрешите сетевые подключения компьютера к службе Kaspersky Security Managment (файл kavfsgt.exe). |

| Параметр | Ключ командной строки для установщика Windows и его значения | Значение по умолчанию | Описание |
|---|---|---|---|
| | | | 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. 45). |
| Отключение проверки на наличие несовместимого программного обеспечения | SKIPINCOMPATIBLESW = <значение><br>0 - выполняется проверка на несовместимое программное обеспечение.<br>1 - проверка на наличие несовместимого программного обеспечения не выполняется. | 0 | Используйте этот параметр, чтобы включить или отключить проверку на наличие несовместимого программного обеспечения при установке программы на устройство в фоновом режиме.<br>Независимо от значения данного параметра, при установке Kaspersky Embedded Systems Security 2.2 программа всегда предупреждает о других версиях программы, установленных на этом же устройстве. |

*Таблица 12. Параметры удаления и ключи командной строки для установщика Windows*

| Параметр | Ключ командной строки для установщика Windows и его значения | Значение по умолчанию |
|---|---|---|
| Восстановление содержимого карантина | RESTOREQTN =<значение><br>**0** – удалить содержимое карантина;<br>**1** – восстановить содержимое карантина в папку, указанную параметром RESTOREPATH, в подпапку \Quarantine. | 0 – удалить |

| Параметр | Ключ командной строки для установщика Windows и его значения | Значение по умолчанию |
|---|---|---|
| Восстановление содержимого резервного хранилища | RESTOREBCK =<значение><br>**0** – удалить содержимое резервного хранилища;<br>**1** – восстановить содержимое резервного хранилища в папку, указанную параметром RESTOREPATH, во вложенную папку \Backup. | 0 – удалить |
| Ввод текущего пароля для подтверждения операции удаления (при активной функции применения пароля) | UNLOCK_PASSWORD=<заданный пароль> | Не указан |
| Папка для восстановленных объектов | RESTOREPATH=<полный путь к папке><br>Восстановленные объекты будут сохранены в указанной папке. | %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored |

# Журнал установки и удаления Kaspersky Embedded Systems Security 2.2

Если вы выполняете установку или удаление Kaspersky Embedded Systems Security 2.2 с помощью мастера установки (удаления), служба Windows Installer создает журнал установки (удаления). Файл журнала с именем ess_install_<uid>.log (где <uid> – уникальный восьмизначный идентификатор журнала) сохраняется в папке %temp% пользователя, с правами которого был запущен файл setup.exe.

Если в меню **Пуск** вы выбрали пункт **Изменение или удаление** для Консоли программы или для Kaspersky Embedded Systems Security 2.2, в папке %temp% автоматически создается файл ess_2.2_maintenance.log.

Если вы выполняете установку или удаление Kaspersky Embedded Systems Security 2.2 из командной строки, по умолчанию журнал установки не создается.

► *Чтобы установить Kaspersky Embedded Systems Security 2.2 с созданием файла 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

Этот раздел содержит описание средств администрирования Kaspersky Embedded Systems Security 2.2, особенностей установки и удаления Kaspersky Embedded Systems Security 2.2 с помощью мастера установки (см. раздел "Установка и удаление программы с помощью мастера" на стр. 41), из командной строки (см. раздел "Установка и удаление программы из командной строки" на стр. 53), через Kaspersky Security Center (см. раздел "Установка и удаление программы через Kaspersky Security Center" на стр. 58) и через групповые политики Active Directory® (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. 63).

Перед тем как начать установку Kaspersky Embedded Systems Security 2.2, спланируйте основные этапы ее проведения:

1. Выберите средства администрирования, которые вы будете использовать для управления Kaspersky Embedded Systems Security 2.2 и его настройки.
2. Определите, какие программные компоненты требуется установить (см. раздел "Программные компоненты Kaspersky Embedded Systems Security 2.2 и их коды для службы Windows Installer" на стр. 23).
3. Выберите способ установки.

## В этом разделе



# Выбор средств администрирования

Определите, какие средства администрирования вы будете использовать для настройки параметров Kaspersky Embedded Systems Security 2.2 и управления им. В качестве средств администрирования Kaspersky Embedded Systems Security 2.2 вы можете использовать Консоль программы, утилиту командной строки и Консоль администрирования Kaspersky Security Center.

### Документация Kaspersky Embedded Systems Security 2.2

Консоль Kaspersky Embedded Systems Security 2.2 представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console. Вы можете управлять Kaspersky Embedded Systems Security 2.2 через Консоль программы, установленную на защищаемом компьютере или на другом компьютере в сети организации.

Вы можете добавить несколько оснасток Kaspersky Embedded Systems Security 2.2 в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких компьютеров, на которых установлена программа Kaspersky Embedded Systems Security 2.2.

Консоль программы входит в набор компонентов "Средства администрирования".

### Утилита командной строки

Вы можете управлять Kaspersky Embedded Systems Security 2.2 из командной строки защищаемого компьютера.

Утилита командной строки входит в набор программных компонентов Kaspersky Embedded Systems Security 2.2.

### Kaspersky Security Center

Если вы используете программу Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации, вы можете управлять Kaspersky Embedded Systems Security 2.2 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 2.2. Он обеспечивает связь Kaspersky Embedded Systems Security 2.2 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 обеспечивает взаимодействие между программой Kaspersky Embedded Systems Security 2.2, 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 2.2**. Дополнительно установите на компьютер, на котором установлен Сервер администрирования Kaspersky Security Center, Плагин управления Kaspersky Embedded Systems Security 2.2 для управления Kaspersky Embedded Systems Security 2.2 через Консоль администрирования. Он обеспечивает интерфейс управления программой через Kaspersky Security Center. Файл установки Плагина управления, \product\klcfginst.exe, входит в комплект поставки Kaspersky Embedded Systems Security 2.2.

## Выбор способа установки

После определения программных компонентов для установки Kaspersky Embedded Systems Security 2.2 (см. раздел "Программные компоненты Kaspersky Embedded Systems Security 2.2 и их коды для службы установщика Windows" на стр. 23) 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 2.2 или вы будете использовать параметры установки по умолчанию (см. раздел "Параметры установки и удаления и ключи командной строки для службы установщика Windows" на стр. 31);
- будут ли параметры установки едиными для всех компьютеров или индивидуальными для каждого компьютера.

Вы можете установить Kaspersky Embedded Systems Security 2.2 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 2.2: через групповые политики Active Directory или с помощью задачи удаленной установки Kaspersky Security Center.

Вы можете установить Kaspersky Embedded Systems Security 2.2 на одном компьютере, настроить его для работы и сохранить его параметры в конфигурационном файле, чтобы затем использовать созданный файл для установки Kaspersky Embedded Systems Security 2.2 на других компьютерах (эта возможность не применяется при установке программы через групповые политики Active Directory).

### Запуск мастера установки

С помощью мастера установки вы можете установить:

- компоненты Kaspersky Embedded Systems Security 2.2 (см. раздел "Программные компоненты Kaspersky Embedded Systems Security 2.2" на стр. 24) на защищаемом компьютере из файла \product\setup.exe, входящего в комплект поставки;
- Консоль Kaspersky Embedded Systems Security 2.2 (см. раздел "Установка Консоли Kaspersky Embedded Systems Security 2.2" на стр. 43) из файла \client\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 2.2 с параметрами установки по умолчанию. С помощью ключей Kaspersky Embedded Systems Security 2.2 вы можете изменять параметры установки.

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

Вы также можете использовать команды для установки Kaspersky Embedded Systems Security 2.2 и Консоли программы (см. раздел "Установка и удаление программы из командной строки" на стр. 53).

### Централизованная установка через Kaspersky Security Center

Если вы используете Kaspersky Security Center для управления антивирусной защитой компьютеров сети, можно установить Kaspersky Embedded Systems Security 2.2 на нескольких компьютерах с помощью задачи удаленной установки Kaspersky Security Center.

Компьютеры, на которых вы хотите установить Kaspersky Embedded Systems Security 2.2 через Kaspersky Security Center (см. раздел "Установка и удаление программы с помощью Kaspersky Security Center" на стр. 58), 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 2.2 на защищаемом компьютере. Вы можете установить Консоль программы на защищаемом компьютере или рабочем месте администратора.

Вы можете установить Kaspersky Embedded Systems Security 2.2, используя лишь параметры установки по умолчанию.

Компьютеры, на которых программа Kaspersky Embedded Systems Security 2.2 установлена с помощью групповых политик Active Directory (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. 63), 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

Этот раздел содержит описание процедуры установки и удаления Kaspersky Embedded Systems Security 2.2 и Консоли программы с помощью мастера установки, а также информацию о дополнительной настройке Kaspersky Embedded Systems Security 2.2 и действиях после установки программы.

## В этом разделе



# Установка с помощью мастера установки

В следующих разделах содержится информация о том, как установить Kaspersky Embedded Systems Security 2.2 и Консоль программы.

► *Чтобы установить и приступить к использованию Kaspersky Embedded Systems Security 2.2, выполните следующие действия:*

1. Установите Kaspersky Embedded Systems Security 2.2 на защищаемом компьютере.
2. На компьютерах, с которых вы планируете управлять Kaspersky Embedded Systems Security 2.2, 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 2.2.
4. Выполните действия после установки Kaspersky Embedded Systems Security 2.2.

## В этом разделе



### Установка Kaspersky Embedded Systems Security 2.2

Перед установкой Kaspersky Embedded Systems Security 2.2 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 2.2. Вы можете прервать установку Kaspersky Embedded Systems Security 2.2 на любом шаге мастера установки. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Вы можете прочитать подробнее о параметрах установки (удаления) (см. раздел "Параметры установки и удаления и их ключи командной строки для службы установщика Windows" на стр. 31).

► *Чтобы установить Kaspersky Embedded Systems Security 2.2 с помощью мастера установки, выполните следующие действия:*

1. На компьютере запустите файл программы-приветствия setup.exe.
2. В открывшемся окне в блоке Установка перейдите по ссылке **Установить Kaspersky Embedded Systems Security 2.2**.
3. В открывшемся окне приветствия мастера установки Kaspersky Embedded Systems Security 2.2 нажмите на кнопку **Далее**.

   Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.
4. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности.
5. Если вы прочитали Лицензионное соглашение и Политику 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 **Выборочная установка**.
7. Выберите компоненты, которые вы хотите установить.

   По умолчанию в список рекомендуемых к установке объектов включены все компоненты Kaspersky Embedded Systems Security 2.2, за исключением компонента Управление сетевым экраном.

   Компонент Поддержка SNMP-протокола Kaspersky Embedded Systems Security 2.2 отображается в списке устанавливаемых компонентов, только если на компьютере установлена Служба SNMP Microsoft Windows.
8. Чтобы отменить все изменения в окне **Выборочная установка**, нажмите на кнопку **Сбросить**. Нажмите на кнопку **Далее**.
9. В открывшемся окне **Выбор папки назначения** выполните следующие действия:
   - Если требуется, укажите папку, в которой будут сохранены файлы Kaspersky Embedded Systems Security 2.2.
   - Если требуется, просмотрите информацию о доступном пространстве на локальных жестких дисках по кнопке **Диск**.

   Нажмите на кнопку **Далее**.

10. В открывшемся 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**.

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

    a. Если вы хотите импортировать параметры Kaspersky Embedded Systems Security 2.2 из существующего конфигурационного файла, созданного в любой предыдущей совместимой версии программы, укажите конфигурационный файл.

    b. Затем нажмите на кнопку **Далее**.

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

    - Если вы хотите активировать программу, укажите файл ключа Kaspersky Embedded Systems Security 2.2 для активации программы.
    - Если вы хотите активировать программу позже, нажмите на кнопку **Далее**.
    - Если вы предварительно сохранили файл ключа в папке \server комплекта поставки, имя этого файла отобразится в поле **Ключ**.

      Если вы хотите добавить ключ с помощью файла ключа, который хранится в другой папке, укажите файл ключа.

      После добавления файла ключа в окне отобразится информация о лицензии. Kaspersky Embedded Systems Security 2.2 отображает расчетную дату окончания срока действия лицензии. Срок действия лицензии отсчитывается с момента добавления ключа, но истекает не позднее истечения срока годности файла ключа.

      Нажмите на кнопку **Далее**, чтобы применить ключ в программе.

13. В открывшемся окне **Готовность к установке** нажмите на кнопку **Установить**. Мастер приступит к установке компонентов Kaspersky Embedded Systems Security 2.2.
14. По завершении установки откроется окно **Установка завершена**.
15. Установите флажок **Прочитать Release Notes**, чтобы просмотреть информацию о версии после завершения работы мастера установки.
16. Нажмите на кнопку **ОК**.

Окно мастера установки будет закрыто. По завершении установки Kaspersky Embedded Systems Security 2.2 будет готов к работе, если вы добавили ключ для активации программы.

## Установка Консоли Kaspersky Embedded Systems Security 2.2

Следуя инструкциям мастера установки, задайте 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. Запустите файл приветствия setup.exe на компьютере.

   Откроется окно программы-приветствия.
3. Перейдите по ссылке **Установить Консоль Kaspersky Embedded Systems Security 2.2**.

   Откроется окно приветствия мастера установки. Нажмите на кнопку **Далее**.
4. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности в открывшемся окне и для продолжения установки установите флажки, свидетельствующие, что вы принимаете **положения и условия настоящего Лицензионного соглашения** и **Политику конфиденциальности, которая описывает обработку данных**. Нажмите на кнопку **Далее**.

   Откроется окно **Дополнительные параметры установки**.
5. В открывшемся окне **Дополнительные параметры установки** выполните следующие действия:

   - Если вы планируете с помощью Консоли программы управлять программой Kaspersky Embedded Systems Security 2.2, 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. Выберите компоненты набора средств администрирования из списка.

        По умолчанию устанавливаются все компоненты.

     c. Нажмите на кнопку **Далее**.

   Вы можете прочитать подробнее о компонентах Kaspersky Embedded Systems Security 2.2 (см. раздел "Программные компоненты Kaspersky Embedded Systems Security 2.2 и их коды для службы Windows Installer" на стр. 23).
6. В открывшемся окне **Выбор папки назначения** выполните следующие действия:

   a. Если требуется, укажите другую папку, в которой будут сохранены устанавливаемые файлы.

   b. Нажмите на кнопку **Далее**.
7. В открывшемся окне **Готовность к установке** нажмите на кнопку **Установить**.

   Мастер приступит к установке выбранных компонентов.
8. Нажмите на кнопку **ОК**.

Окно мастера установки будет закрыто. Консоль программы будет установлена на защищаемом компьютере.

Если вы установили набор "Средства администрирования" не на защищаемом сервере, а на другом компьютере сети, выполните дополнительную настройку (см. раздел "Дополнительная настройка после установки Консоли программы на другом компьютере" на стр. 45).

## Дополнительная настройка после установки Консоли программы на другом компьютере

Если вы установили Консоль программы не на защищаемом компьютере, а на другом компьютере сети, выполните описанные ниже действия для того, чтобы пользователи могли удаленно управлять Kaspersky Embedded Systems Security 2.2:

- Добавьте пользователей Kaspersky Embedded Systems Security 2.2 в группу ESS Administrators на защищаемом компьютере.
- Разрешать сетевые соединения для службы Kaspersky Security Management (kavfsgt.exe) (см. раздел "О правах доступа к службе Kaspersky Security Management" на стр. 83), если на защищаемом компьютере используется сетевой экран 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.

### Разрешение сетевых соединений для Консоли программы

Названия параметров могут отличаться в разных операционных системах Windows.

Консоль программы на удаленном компьютере использует протокол DCOM для получения информации о событиях Kaspersky Embedded Systems Security 2.2 (например, о проверенных объектах или завершении задач) от службы Kaspersky Security Management на защищаемом компьютере. Вам нужно 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 2.2 – kavfsrcn.exe.

  Клиентский компьютер, на котором установлена Консоль программы, обменивается информацией с защищаемым компьютером через порт TCP 135.
- Настройте правило исходящего трафика для брандмауэра Windows, чтобы разрешить сетевые соединения.

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

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

Если Консоль программы открыта во время настройки параметров соединения между защищаемым компьютером и компьютером, на котором установлена Консоль программы, требуется закрыть Консоль программы, дождаться завершения процесса удаленного управления Kaspersky Embedded Systems Security 2.2 kavfsrcn.exe и снова запустить Консоль программы. Новые параметры соединения будут применены.

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

1. На удаленном компьютере, на котором установлена Консоль Kaspersky Embedded Systems Security 2.2, 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 на узле **Мой компьютер**.
7. Выберите пункт **Свойства**.
8. В окне **Свойства** на закладке **Безопасность COM** нажмите на кнопку **Изменить ограничения** в группе 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**.

► *Чтобы открыть в брандмауэре Windows TCP-порт 135 и разрешить сетевые соединения для процесса удаленного управления Kaspersky Embedded Systems Security 2.2, выполните следующие действия:*

1. На удаленном компьютере закройте Консоль Kaspersky Embedded Systems Security 2.2.
2. Выполните одно из следующих действий:
   - В Microsoft Windows XP или Microsoft Windows Vista®:
     a. В Microsoft Windows XP с пакетом обновлений 2 или выше выберите **Пуск** > **Брандмауэр Windows**.

        В Microsoft Windows Vista выберите **Пуск** > **Панель управления** > **Брандмауэр Windows** и в окне **Брандмауэр Windows** выберите пункт **Изменить параметры**.

     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 2.2, 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 пункт **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 2.2 с помощью консоли Microsoft Management Console.
4. Нажмите на кнопку **ОК**.
5. Нажмите на кнопку **ОК** в окне **Брандмауэр Windows (Параметры брандмауэра Windows)**.

► *Добавление правила исходящего трафика для брандмауэра Windows:*

1. Выберите пункт **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 параметр **Протокол TCP**.
7. В поле **Определенные удаленные порты** укажите следующий диапазон портов, чтобы разрешить исходящие подключения: 1024–65535.
8. В окне **Действие** выберите параметр **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 2.2

Kaspersky Embedded Systems Security 2.2 запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Embedded Systems Security 2.2 был выбран пункт **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 2.2 выполняет задачу Проверка важных областей.

После установки Kaspersky Embedded Systems Security 2.2 рекомендуется выполнить следующие действия:

- Запустить задачу Обновление баз программы. После установки Kaspersky Embedded Systems Security 2.2 проверяет объекты с использованием баз, которые входили в состав программы при поставке.

  Рекомендуется сразу же обновить базы Kaspersky Embedded Systems Security 2.2, так как базы могли устареть.

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

- Выполнить Проверку важных областей компьютера, если перед установкой Kaspersky Embedded Systems Security 2.2 на защищаемом компьютере не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.
- Настроить уведомления администратора о событиях Kaspersky Embedded Systems Security 2.2.

## В этом разделе



## Запуск и настройка задачи обновления баз Kaspersky Embedded Systems Security 2.2

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

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

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

1. Запустите Консоль программы одним из следующих способов:
   - Откройте Консоль программы на защищаемом компьютере. Для этого выберите **Пуск** > **Все программы** > **Kaspersky Embedded Systems Security 2.2** > **Средства администрирования** > **Консоль Kaspersky Embedded Systems Security 2.2**.
   - Если вы запустили Консоль программы не на защищаемом компьютере, подключитесь к защищаемому компьютеру:
     a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems 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. 83), 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** откройте закладку **Параметры соединения**.

6. Выполните следующие действия:

   a. Если в вашей сети не настроен протокол Web Proxy Auto-Discovery Protocol (WPAD) для автоматического распознавания параметров прокси-сервера в локальной сети, укажите параметры прокси-сервера: в блоке **Параметры прокси-сервера** установите флажок **Использовать параметры указанного прокси-сервера**, в поле **Адрес** введите адрес, а в поле **Порт** – номер порта прокси-сервера.

   b. Если в вашей сети требуется проверка подлинности при доступе к прокси-серверу, выберите нужный метод проверки подлинности в раскрывающемся списке блока **Параметры аутентификации на прокси-сервере**:

      - **Использовать NTLM-аутентификацию**, если прокси-сервер поддерживает встроенную проверку подлинности Microsoft Windows (NTLM authentication). Kaspersky Embedded Systems Security 2.2 будет использовать для доступа к прокси-серверу учетную запись, указанную в параметрах задачи (по умолчанию задача выполнится под учетной записью **Локальная система** {**SYSTEM**}).
      - **Использовать NTLM-аутентификацию с именем и паролем**, если прокси-сервер поддерживает встроенную проверку подлинности Microsoft Windows. Kaspersky Embedded Systems Security 2.2 будет использовать для доступа к прокси-серверу учетную запись, указанную вами. Введите имя и пароль пользователя или выберите пользователя в списке.
      - **Применить имя и пароль пользователя**, чтобы выбрать обычную проверку подлинности. Введите имя и пароль пользователя или выберите пользователя в списке.

7. В окне **Параметры задачи** нажмите на кнопку **ОК**.

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 Embedded Systems Security**.

## Проверка важных областей

После обновления баз Kaspersky Embedded Systems Security 2.2, 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 рабочей области 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 2.2

Вы можете добавлять или удалять компоненты Kaspersky Embedded Systems Security 2.2. Вам нужно предварительно остановить задачу Постоянная защита файлов, если вы хотите удалить компонент Постоянная защита файлов. В остальных случаях останавливать задачу постоянной защиты или службу Kaspersky Security не требуется.

Если доступ к управлению программой защищен паролем, Kaspersky Embedded Systems Security 2.2 запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов на дополнительном шаге мастера.

► *Чтобы изменить состав компонентов Kaspersky Embedded Systems Security 2.2, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы > Kaspersky Embedded Systems Security 2.2 > Изменение или удаление**.

   Откроется окно мастера установки программы **Изменение, восстановление или удаление установки**.

2. Выберите **Изменение состава компонентов программы**. Нажмите на кнопку **Далее**.

   Откроется окно **Выборочная установка**.

3. В окне **Выборочная установка** в списке компонентов, доступных для использования, выберите компоненты, которые вы хотите добавить в Kaspersky Embedded Systems Security 2.2 или удалить. Для этого выполните следующие действия:

   - Чтобы изменить состав компонентов, нажмите на кнопку рядом с названием выбранного компонента и в контекстном меню выберите:
     - пункт **Компонент будет установлен на локальный жесткий диск**, если хотите установить один компонент;
     - пункт **Компонент и его подкомпоненты будут установлены на локальный жесткий диск**, если хотите установить группу компонентов.
   - Чтобы удалить ранее установленные компоненты, нажмите на кнопку рядом с названием выбранного компонента и в контекстном меню выберите пункт **Компонент будет недоступен**.

   Нажмите на кнопку **Установить**.

4. В окне **Готовность к установке** подтвердите операцию изменения состава компонентов программы, нажав на кнопку Установить.

5. В окне, открывшемся по завершении установки, нажмите на кнопку **ОК**.

Состав компонентов Kaspersky Embedded Systems Security 2.2 будет изменен в соответствии с заданными параметрами.

Если в работе Kaspersky Embedded Systems Security 2.2 возникли проблемы (Kaspersky Embedded Systems Security 2.2 завершается аварийно; задачи завершаются аварийно или не запускаются), вы можете попробовать восстановить Kaspersky Embedded Systems Security 2.2. Вы можете выполнить восстановление, сохранив текущие значения параметров Kaspersky Embedded Systems Security 2.2, или выбрать режим, при котором все параметры Kaspersky Embedded Systems Security 2.2 примут значения по умолчанию.

► *Чтобы восстановить Kaspersky Embedded Systems Security 2.2 после аварийного завершения работы программы или задач, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы > Kaspersky Embedded Systems Security 2.2 > Изменение или удаление**.

   Откроется окно мастера установки программы **Изменение, восстановление или удаление**.

2. Выберите пункт **Восстановление установленных компонентов**. Нажмите на кнопку **Далее**.

   Откроется окно **Восстановление установленных компонентов**.

3. В окне **Восстановление установленных компонентов** установите флажок **Восстановить рекомендуемые параметры работы программы**, если хотите сбросить настроенные параметры программы и восстановить Kaspersky Embedded Systems Security 2.2 с параметрами по умолчанию. Нажмите на кнопку **Установить**.

4. В окне **Готовность к восстановлению** подтвердите операцию восстановления программы, нажав на кнопку **Установить**.

5. В окне, открывшемся по завершении восстановления, нажмите на кнопку **ОК**.

Kaspersky Embedded Systems Security 2.2 будет восстановлен в соответствии с заданными параметрами.

## Удаление с помощью мастера установки

Этот раздел содержит инструкции по удалению Kaspersky Embedded Systems Security 2.2 и Консоли программы с защищаемого компьютера с помощью мастера установки.

### Удаление Консоли Kaspersky Embedded Systems Security 2.2

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Kaspersky Embedded Systems Security 2.2 с защищаемого компьютера с помощью мастера установки / удаления.

После удаления Kaspersky Embedded Systems Security 2.2 может потребоваться перезагрузка компьютера. Вы можете отложить перезагрузку.

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

Если доступ к управлению программой защищен паролем, Kaspersky Embedded Systems Security 2.2 запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов на дополнительном шаге мастера.

► *Чтобы удалить Консоль Kaspersky Embedded Systems Security 2.2, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы > Kaspersky Embedded Systems Security 2.2 > Изменение или удаление**.

   Откроется окно мастера установки программы **Изменение, восстановление или удаление установки**.

2. Выберите пункт **Удаление компонентов программы**. Нажмите на кнопку **Далее**.

   Откроется окно **Дополнительные параметры удаления программы**.

3. Если требуется, в окне **Дополнительные параметры удаления программы** выполните следующие действия:

   a. Установите флажок **Экспортировать объекты на карантине**, чтобы программа Kaspersky Embedded Systems Security 2.2 экспортировала объекты, помещенные на карантин. По умолчанию флажок снят.

   b. Установите флажок **Экспортировать объекты резервного хранилища**, чтобы программа Kaspersky Embedded Systems Security 2.2 экспортировала объекты из резервного хранилища. По умолчанию флажок снят.

   c. Нажмите на кнопку **Сохранить в** и укажите папку, в которую вы хотите экспортировать восстановленные объекты. По умолчанию экспорт объектов осуществляется в папку %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Uninstall.

      Нажмите на кнопку **Далее**.

4. В окне **Готовность к удалению** подтвердите операцию удаления, нажав на кнопку **Удалить**.

5. В окне, открывшемся по завершении удаления, нажмите на кнопку **ОК**.

Программа Kaspersky Embedded Systems Security 2.2 будет удалена с защищаемого компьютера.

## Удаление Консоли Kaspersky Embedded Systems Security 2.2

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 > Kaspersky Embedded Systems Security 2.2 > Средства администрирования > Изменение или удаление**.

2. Откроется окно мастера **Изменение, восстановление или удаление**.

   Выберите пункт **Удаление компонентов программы** и нажмите на кнопку **Далее**.

3. Откроется окно **Готовность к удалению**. Нажмите на кнопку **Удалить**.

   Откроется окно **Удаление завершено**.

4. Нажмите на кнопку **ОК**.

Операция удаления будет завершена; окно мастера будет закрыто.

# Установка и удаление программы из командной строки

Этот раздел содержит описание особенностей установки и удаления Kaspersky Embedded Systems Security 2.2 из командной строки, примеры команд для установки и удаления Kaspersky Embedded Systems Security 2.2 из командной строки, примеры команд для добавления и удаления компонентов Kaspersky Embedded Systems Security 2.2 из командной строки.

## В этом разделе



## Об установке и удалении Kaspersky Embedded Systems Security 2.2 из командной строки

Вы можете устанавливать и удалять Kaspersky Embedded Systems Security 2.2, добавлять или удалять компоненты, запустив из командной строки файлы инсталляционного пакета \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 инсталляционный пакет \client\esstools.msi.

Выполняйте установку с правами учетной записи, входящей в группу администраторов на компьютере, на котором вы выполняете установку.

Если вы запустите на защищаемом компьютере один из файлов \product\ess_x86(x64).msi без дополнительных ключей, программа Kaspersky Embedded Systems Security 2.2 будет установлена с параметрами установки по умолчанию.

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 2.2

В этом разделе приводятся примеры команд для установки Kaspersky Embedded Systems Security 2.2.

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 службы Windows Installer содержится в документации, предоставляемой корпорацией Microsoft.

## Примеры установки Kaspersky Embedded Systems Security 2.2 с помощью файла setup.exe

► *Чтобы установить Kaspersky Embedded Systems Security 2.2 с параметрами установки по умолчанию без взаимодействия с пользователем, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Embedded Systems Security 2.2 со следующими параметрами:*

- установить только компоненты Постоянная защита файлов и Проверка по требованию;
- не запускать постоянную защиту при запуске Kaspersky Embedded Systems Security 2.2;
- не исключать из проверки файлы, рекомендованные к исключению корпорацией Microsoft;

*выполните следующую команду:*

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

## Примеры команд для установки: запуск msi-файла инсталляционного пакета

► *Чтобы установить Kaspersky Embedded Systems Security 2.2 с параметрами установки по умолчанию без взаимодействия с пользователем, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Embedded Systems Security 2.2 с параметрами установки по умолчанию; показать интерфейс установки, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Embedded Systems Security 2.2 с активацией с помощью файла ключа C:\0000000A.key:*

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

- *Чтобы установить Kaspersky Embedded Systems Security 2.2 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 2.2, сохранив файлы в папке назначения C:\ESS, выполните следующую команду:*

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

- *Чтобы установить Kaspersky Embedded Systems Security 2.2, сохраните файл журнала установки с именем ess.log в папке, в которой хранится msi-файл инсталляционного пакета Kaspersky Embedded Systems Security 2.2, и выполните следующую команду:*

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

- *Чтобы установить Консоль Kaspersky Embedded Systems Security 2.2, выполните следующую команду:*

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

- *Чтобы установить Kaspersky Embedded Systems Security 2.2 с активацией с помощью файла ключа C:\0000000A.key; настроить Kaspersky Embedded Systems Security 2.2 в соответствии с параметрами, описанными 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, когда Kaspersky Embedded Systems Security 2.2 защищен паролем, выполните следующую команду:*

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

## Действия после установки Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Embedded Systems Security 2.2 был выбран пункт **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 2.2 выполняет задачу "Проверка важных областей".

После установки Kaspersky Embedded Systems Security 2.2 рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз Kaspersky Embedded Systems Security 2.2. После установки Kaspersky Embedded Systems Security 2.2 проверяет объекты с использованием баз, которые входили в его состав при поставке. Рекомендуется сразу же обновить базы Kaspersky Embedded Systems Security 2.2. 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 2.2 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 компьютера, если перед установкой Kaspersky Embedded Systems Security 2.2 на защищаемом компьютере не была установлена антивирусная программа с включенной 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 2.2.

## Добавление и удаление компонентов. Примеры команд

Компонент Контроль запуска программ устанавливается автоматически. Вам не нужно указывать его в списке значений ключа ADDLOCAL, добавляя или удаляя компоненты Kaspersky Embedded Systems Security 2.2.

► *Чтобы добавить компонент Проверка по требованию к ранее установленным компонентам, выполните следующую команду:*

```
msiexec /i ess.msi ADDLOCAL=Oas,Ods /qn EULA=1 PRIVACYPOLICY=1
```

или

```
\computer\setup.exe /s /p "ADDLOCAL=Oas,Ods" /p EULA=1 /p PRIVACYPOLICY=1
```

Если вы укажете не только компоненты, которые хотите установить, но и уже установленные компоненты, Kaspersky Embedded Systems Security 2.2 переустановит указанные установленные компоненты.

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

```
msiexec /i ess.msi "ADDLOCAL=Oas,AppCtrl,Ksn,AntiExploit,DevCtrl,Firewall,
LogInspector,AKIntegration,PerfMonCounters,SnmpSupport,TrayApp,AVPro
tection,RamDisk REMOVE=Ods,Fim" /qn
```

## Удаление Kaspersky Embedded Systems Security 2.2. Примеры команд

► *Чтобы удалить Kaspersky Embedded Systems Security 2.2 с защищаемого компьютера, выполните следующую команду:*

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

или

- Для x32-разрядной операционной системы:

```
msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} /qn
```

- Для x64-разрядной операционной системы:

```
msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} /qn
```

► *Чтобы удалить Консоль Kaspersky Embedded Systems Security 2.2, выполните следующую команду:*

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

или

- Для x32-разрядной операционной системы:

```
msiexec /x {A727008F-F8CC-4B35-848A-1AECEEF22178} /qn
```

- Для x64-разрядной операционной системы:

```
msiexec /x {D978C311-2D2D-41A3-8158-BDF97149CCD4} /qn
```

► *Чтобы удалить Kaspersky Embedded Systems Security 2.2 с защищаемого компьютера, на котором установлена защита паролем, выполните следующую команду:*

- Для x32-разрядной операционной системы:

```
msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} UNLOCK_PASSWORD=*** /qn
```

- Для x64-разрядной операционной системы:

```
msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} UNLOCK_PASSWORD=*** /qn
```

## Коды возврата

В таблице ниже приведено описание кодов возврата командной строки.

*Таблица 13. Коды возврата*

| Код | Описание |
|---|---|
| 1324 | Имя папки назначения содержит недопустимые символы. |
| 25001 | Недостаточно прав для установки Kaspersky Embedded Systems Security 2.2. Чтобы установить программу, запустите мастер установки с правами локального администратора. |
| 25003 | Kaspersky Embedded Systems Security 2.2 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 2.2 через Kaspersky Security Center, описание процедуры установки и удаления Kaspersky Embedded Systems Security 2.2 через Kaspersky Security Center, а также описание действий после установки Kaspersky Embedded Systems Security 2.2.

### В этом разделе

## Общие сведения об установке через Kaspersky Security Center

Вы можете установить Kaspersky Embedded Systems Security 2.2 через Kaspersky Security Center с помощью задачи удаленной установки.

После выполнения задачи удаленной установки программа Kaspersky Embedded Systems Security 2.2 будет установлена с одинаковыми параметрами на нескольких компьютерах.

Вы можете объединить все компьютеры в одну группу администрирования и создать групповую задачу для установки Kaspersky Embedded Systems Security 2.2 на компьютеры этой группы.

Вы можете создать задачу удаленной установки Kaspersky Embedded Systems Security 2.2 для набора компьютеров, не объединенных в одну группу администрирования. При ее создании вам нужно сформировать список отдельных компьютеров, на которые требуется установить Kaspersky Embedded Systems Security 2.2.

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

## Права для установки или удаления Kaspersky Embedded Systems Security 2.2

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 вы хотите установить Kaspersky Embedded Systems Security 2.2, 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 2.2 с помощью задачи удаленной установки. Перед установкой Агента администрирования убедитесь, что учетная запись, которую вы укажете в задаче, входит в группу администраторов на каждом из компьютеров.

- Все компьютеры, на которые вы хотите установить Kaspersky Embedded Systems Security 2.2, находятся в одном домене с Сервером администрирования и Сервер администрирования зарегистрирован под учетной записью Администратор домена (**Domain Admin**) (если эта учетная запись обладает правами администратора на компьютерах домена).

По умолчанию задача удаленной установки методом **Форсированная установка** выполняется под учетной записью, с правами которой работает Сервер администрирования.

В групповых задачах, а также в тех 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;
- правами на ресурс **Admin$**;
- правом **Вход в качестве службы**.

# Установка Kaspersky Embedded Systems Security 2.2 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 2.2 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 в комплекте поставки Kaspersky Embedded Systems Security 2.2).
- 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 2.2 с помощью задачи удаленной установки.

Вы также можете предварительно 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 2.2 с помощью задачи удаленной установки, выполните следующие действия:*

1. Запустите Консоль администрирования Kaspersky Security Center.
2. В Kaspersky Security Center разверните узел **Удаленная установка** и во вложенном узле **Инсталляционные пакеты** выберите вариант **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
3. Введите имя инсталляционного пакета.
4. Выберите файл ess.kud из комплекта поставки Kaspersky Embedded Systems Security 2.2 в качестве файла инсталляционного пакета.

   Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.
5. Если вы прочитали Лицензионное соглашение и Политику 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.

6. Чтобы изменить набор устанавливаемых компонентов Kaspersky Embedded Systems Security 2.2 (см. раздел "Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security 2.2" на стр. 50) и параметры установки по умолчанию (см. раздел "Параметры установки и удаления и их ключи командной строки для службы установщика Windows " на стр. 31) в инсталляционном пакете, выполните следующие действия:

   a. В Kaspersky Security Center разверните узел **Удаленная установка**.

   b. Во вложенном узле **Инсталляционные пакеты** в рабочей области откройте контекстное меню созданного инсталляционного пакета Kaspersky Embedded Systems Security 2.2 и выберите команду **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 2.2, 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. Учесть исключения, рекомендованные «Лабораторией Касперского».

   d. В диалоговом окне **Свойства: <название инсталляционного пакета>** нажмите на кнопку **ОК**.

7. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Kaspersky Embedded Systems Security 2.2 на выбранные компьютеры (группу администрирования). Настройте параметры задачи.

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

8. Запустите созданную задачу удаленной установки Kaspersky Embedded Systems Security 2.2.

Программа Kaspersky Embedded Systems Security 2.2 будет установлена на указанные в задаче компьютеры.

## Действия после установки Kaspersky Embedded Systems Security 2.2

После установки Kaspersky Embedded Systems Security 2.2 рекомендуется обновить базы Kaspersky Embedded Systems Security 2.2 на компьютерах, а также выполнить Проверку важных областей компьютеров, если до установки Kaspersky Embedded Systems Security 2.2 на компьютерах не были установлены антивирусные программы с включенной функцией постоянной защиты.

Если компьютеры, на которых установлен Kaspersky Embedded Systems Security 2.2, 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 2.2. Установить в качестве источника обновлений Сервер администрирования Kaspersky Security Center.
2. Создать групповую задачу проверки по требованию со статусом Задача проверки важных областей. Программа Kaspersky Security Center будет оценивать состояние безопасности каждого компьютера группы по результатам выполнения этой задачи, а не по результатам системной задачи Проверка важных областей.
3. Создать новую политику для группы компьютеров. В свойствах созданной политики на закладке **Системные задачи** выключить запуск по расписанию системных задач проверки по требованию и задач обновления баз программы на компьютерах группы администрирования.

Вы можете также настроить уведомления администратора о событиях Kaspersky Embedded Systems Security 2.2.

## 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 **Удаленная установка** и во вложенном узле **Инсталляционные пакеты** создайте новый инсталляционный пакет на основе файла client\setup.exe. Создавая новый инсталляционный пакет:

   - В окне **Выбор дистрибутива программы для установки** укажите файл client\setup.exe из папки комплекта поставки Kaspersky Embedded Systems Security 2.2 и установите флажок **Копировать обновления из репозитория в инсталляционный пакет**.
   - Если требуется, в поле **Параметры запуска исполняемого файла (необязательно)** измените состав устанавливаемых компонентов набора с помощью ключа ADDLOCAL и измените папку назначения.

     Например, чтобы установить в папке C:\KasperskyConsole только Консоль программы, не устанавливая файлы справки и документации, выполните следующую команду:

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

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

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

3. Запустите созданную задачу удаленной установки.

Консоль программы будет установлена на указанные в задаче компьютеры.

## Удаление Kaspersky Embedded Systems Security 2.2 через Kaspersky Security Center

Если доступ к управлению Kaspersky Embedded Systems Security 2.2 на компьютерах сети защищен паролем, введите пароль при создании задачи группового удаления программ. Если защита паролем не управляется политикой Kaspersky Security Center централизованно, программа Kaspersky Embedded Systems Security 2.2 будет успешно удалена на компьютерах, где доступ к управлению программой защищен паролем, совпавшим с введенным значением. Kaspersky Embedded Systems Security 2.2 на других компьютерах удален не будет.

► *Чтобы удалить Kaspersky Embedded Systems Security 2.2 в Консоли администрирования Kaspersky Security Center, выполните следующие действия:*

1. В Консоли администрирования Kaspersky Security Center создайте и запустите задачу удаления программ.
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 2.2 только с параметрами удаления по умолчанию (см. раздел "Параметры установки и удаления и их ключи командной строки для службы установщика Windows" на стр. 31).

# Установка и удаление программы через групповые политики Active Directory

Этот раздел содержит описание установки и удаления Kaspersky Embedded Systems Security 2.2 через групповые политики Active Directory, а также информацию о действиях после установки Kaspersky Embedded Systems Security 2.2 через групповые политики Active Directory.

### В этом разделе

# Установка Kaspersky Embedded Systems Security 2.2 через групповые политики Active Directory

Вы можете установить Kaspersky Embedded Systems Security 2.2 на нескольких компьютерах через групповую политику Active Directory. Консоль программы можно установить аналогичным образом.

Компьютеры, на которых вы хотите установить Kaspersky Embedded Systems Security 2.2 или Консоль программы, должны быть в одном домене и в одной организационной единице.

Операционные системы компьютеров, на которых вы хотите установить Kaspersky Embedded Systems Security 2.2 с помощью политики, должны быть одной разрядности (32-разрядные или 64-разрядные).

Вы должны обладать правами администратора домена.

Чтобы установить Kaspersky Embedded Systems Security 2.2, используйте инсталляционные пакеты ess_x86(x64).msi. Чтобы установить Консоль программы, используйте инсталляционные пакеты esstools.msi.

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

► *Чтобы установить Kaspersky Embedded Systems Security 2.2 (Консоль программы), выполните следующие действия:*

1. Сохраните msi-файл инсталляционного пакета, соответствующий разрядности установленной версии операционной системы Microsoft Windows, в папке общего доступа на контроллере домена.
2. На контроллере домена создайте новую политику для группы, к которой принадлежат компьютеры.
3. С помощью **Редактора объектов групповых политик** создайте новый инсталляционный пакет в узле **Конфигурация компьютеров**. Укажите путь к msi-файлу инсталляционного пакета Kaspersky Embedded Systems Security 2.2 (Консоли программы) в формате UNC (Universal Naming Convention).
4. Установите флажок установщика Windows **Всегда устанавливать с повышенными правами** как в узле **Конфигурация компьютеров**, так и в узле **Конфигурация пользователей** выбранной группы.
5. Примените изменения с помощью команды `gpupdate / force`.

Kaspersky Embedded Systems Security 2.2 будет установлен на компьютерах группы после их перезагрузки, перед входом в Microsoft Windows.

# Действия после установки Kaspersky Embedded Systems Security 2.2

После установки Kaspersky Embedded Systems Security 2.2 на защищаемых компьютерах 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 2.2" на стр. 47).

Вы можете также настроить уведомления администратора о событиях Kaspersky Embedded Systems Security 2.2.

## Удаление Kaspersky Embedded Systems Security 2.2 через групповые политики Active Directory

Если вы установили Kaspersky Embedded Systems Security 2.2 или Консоль программы на компьютерах группы, используя групповую политику Active Directory, вы можете использовать эту политику, чтобы удалить Kaspersky Embedded Systems Security 2.2 или Консоль программы.

Вы можете выполнить удаление 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 2.2 через групповые политики Active Directory невозможно.

► *Чтобы удалить Kaspersky Embedded Systems Security 2.2 (Консоль программы), выполните следующие действия:*

1. На контроллере домена выберите организационную единицу, с компьютеров которой вы хотите удалить Kaspersky Embedded Systems Security 2.2 или Консоль программы.
2. Выберите политику, созданную для установки Kaspersky Embedded Systems Security 2.2, 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 2.2 (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 2.2 будет удалена с компьютеров после их перезагрузки, перед входом в Microsoft Windows.

# Проверка функций Kaspersky Embedded Systems Security 2.2. Использование тестового вируса EICAR

Этот раздел содержит описание тестового вируса EICAR и процедуру проверки функций Kaspersky Embedded Systems Security 2.2 "Постоянная защита" и "Проверка по требованию" с его помощью.

### 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 вирусом и не содержит программного кода, который может нанести вред вашему компьютеру, но антивирусные программы большинства производителей идентифицируют в нем 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 папке на диске компьютера убедитесь, что постоянная защита файлов в этой папке отключена.

Файл eicar.com содержит текстовую строку. При проверке файла Kaspersky Embedded Systems Security 2.2 обнаруживает в этой текстовой строке тестовую угрозу, присваивает файлу статус **Зараженный** и удаляет его. Информация об обнаруженной в файле угрозе появляется в Консоли программы и в журнале выполнении задачи.

Вы также можете использовать файл eicar.com, чтобы проверить, как Kaspersky Embedded Systems Security 2.2 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 под новым именем, например, eicar_cure.com.

Для того чтобы Kaspersky Embedded Systems Security 2.2 обработал файл eicar.com с префиксом, в блоке параметров безопасности **Защита объектов** установите значение **Все объекты** для задач Kaspersky Embedded Systems Security 2.2 "Постоянная защита файлов и задач проверки по требованию".

*Таблица 14. Префиксы в файлах EICAR*

| Префикс | Статус файла после проверки и действие Kaspersky Embedded Systems Security 2.2 |
|---|---|
| Без префикса | Kaspersky Embedded Systems Security 2.2 присваивает объекту статус **Зараженный** и удаляет его. |
| SUSP– | Kaspersky Embedded Systems Security 2.2 присваивает объекту статус **Возможно зараженный** (обнаружен с помощью эвристического анализатора) и удаляет его (возможно зараженные объекты не подвергаются лечению). |
| WARN– | Kaspersky Embedded Systems Security 2.2 присваивает объекту статус **Возможно зараженный** (код объекта частично совпадает с известным вредоносным кодом) и удаляет его (возможно зараженные объекты не подвергаются лечению). |
| CURE– | Kaspersky Embedded Systems Security 2.2 присваивает объекту статус **Зараженный** 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 2.2 вы можете убедиться, что Kaspersky Embedded Systems Security 2.2 обнаруживает объекты, содержащие вредоносный код. Для проверки вы можете использовать тестовый вирус EICAR (см. раздел "О тестовом вирусе EICAR" на стр. 66).

► *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 папке общего доступа на локальном диске любого из компьютеров сети.

   Перед сохранением файла в папке убедитесь, что Постоянная защита файлов в этой папке отключена.

2. Если вы хотите проверить работу уведомлений пользователей сети, убедитесь, что и на защищаемом компьютере и на компьютере, на котором сохранен файл eicar.com, включена Служба сообщений Microsoft Windows.
3. Откройте Консоль программы.
4. Скопируйте сохраненный файл eicar.com на локальный диск защищаемого компьютера одним из следующих способов:
   - Чтобы проверить работу уведомлений через окно Службы 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**.
  - На компьютере, с которого вы скопировали файл, появилось следующее сообщение Службы сообщений Microsoft Windows: `Kaspersky Embedded Systems Security 2.2 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 папке общего доступа на локальном диске любого из компьютеров сети.

   Перед сохранением файла в папке убедитесь, что Постоянная защита файлов в этой папке отключена.

2. Откройте 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 жестких компьютера.
- В Консоли программы журналу выполнения задачи присвоен статус **Критический**; в журнале выполнения задачи Проверка 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 2.2 через локальную Консоль программы и с помощью Плагина управления. Действия с локальной Консолью программы описаны в *Руководстве пользователя Kaspersky Embedded Systems Security 2.2*. Действия с Плагином управления осуществляются в интерфейсе Консоли администрирования Kaspersky Security Center. Подробная информация об интерфейсе Kaspersky Security Center содержится 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 2.2.
- 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 вам 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 для приобретенной коммерческой лицензии.

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

Kaspersky Embedded Systems Security 2.2 предоставляет два типа коммерческих лицензий:

- Стандартная лицензия Kaspersky Embedded Systems Security.
- Расширенная лицензия Kaspersky Embedded Systems Security Compliance Edition, включающая 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 2.2). Чтобы продолжить использование Kaspersky Embedded Systems Security 2.2 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, который передается вам 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 коде активации

*Код активации* – уникальная последовательность из 20 символов (букв и цифр). Код активации нужно указать, чтобы добавить ключ для активации Kaspersky Embedded Systems Security 2.2. Вы получаете код активации на адрес электронной почты, указанный при приобретении Kaspersky Embedded Systems Security 2.2.

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 ключе

*Ключ* – 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 применив файл 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 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, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Embedded Systems Security 2.2.

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

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

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

- Обратитесь в Службу технической поддержки https://support.kaspersky.ru/.
- Получите файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации.

# О предоставлении данных

Лицензионное соглашение для Kaspersky Embedded Systems Security 2.2, 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 типы данных 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, уникальный идентификатор задачи обновления.
- Для использования функциональности перенаправления на статьи Базы знаний при возникновении ошибок в работе программы (служба Redirector): имя, локализацию и полный номер версии программы, включая номер сборки, тип перенаправляющей ссылки, а также идентификатор возникшей ошибки.
- Для контроля получения согласий на обработку данных – информация о статусе согласия с условиями лицензионных соглашений 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 в мастере установки Kaspersky Embedded Systems Security 2.2 на шаге подтверждения согласия с условиями Лицензионного соглашения отображается полный текст Лицензионного соглашения;
- в любой момент помощью файла в формате TXT (license.txt), содержащим полный текст Лицензионного соглашения: файл предоставляется в комплекте поставки Kaspersky Embedded Systems Security 2.2, совместно с файлами установки программы.

### Локальная обработка данных

В процессе выполнения основных функций программы, описанных в настоящем Руководстве, Kaspersky Embedded Systems Security 2.2 локально обрабатывает и хранит ряд данных на защищаемом компьютере:

- информацию о проверяемых файлах и обнаруженных объектах, например, имена и атрибуты обработанных файлов и полные пути к ним на проверяемом носителе, 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;

- 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 2.2 обрабатывает и хранит данные в рамках основной функциональности программы, в том числе для регистрации событий по работе программы и получения диагностических данных. Защита локально обрабатываемых данных выполняется в соответствии с настроенными и применяющимися параметрами программы.

Kaspersky Embedded Systems Security 2.2 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 на носителе, 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.

По умолчанию все данные, сохраненные программой в ходе работы локально, удаляются после деинсталляции Kaspersky Embedded Systems Security 2.2. Исключение составляют файлы с диагностическими данными программы (файлы трассировок, файл дампа), а также записи о работе программы в Журнале событий Windows – вам необходимо самостоятельно удалить эти файлы. Вы можете найти детальную информацию по работе с файлами, содержащими диагностические данные программы, в соответствующих разделах настоящего Руководства.

При деинсталляции программы вы также можете сохранять содержимое резервного хранилища и карантина.

# Активация программы с помощью ключа

Вы можете активировать Kaspersky Embedded Systems Security 2.2, применив ключ.

Если в Kaspersky Embedded Systems Security 2.2 уже добавлен активный ключ, и вы добавите другой ключ в качестве активного, то новый ключ заменит ранее добавленный ключ. Ранее добавленный активный ключ будет удален.

Если в Kaspersky Embedded Systems Security 2.2 уже добавлен дополнительный ключ, и вы добавите другой ключ в качестве дополнительного, то новый ключ заменит ранее добавленный ключ. Ранее добавленный дополнительный ключ будет удален.

Если в Kaspersky Embedded Systems Security 2.2 уже добавлены активный ключ и дополнительный ключ, и вы добавите новый ключ в качестве активного, новый ключ заменит ранее добавленный активный ключ, дополнительный ключ не будет удален.

► *Чтобы активировать Kaspersky Embedded Systems Security 2.2, 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 **ОК**.

Выбранный ключ будет применен. Информация о добавленном ключе отобразится в панели результатов узла **Лицензирование**.

# Просмотр информации о действующей лицензии

## Просмотр информации о лицензии

Информация о действующей лицензии отображается в панели результатов узла **Kaspersky Embedded Systems Security** Консоли программы. Статус ключа может принимать следующие значения:

- **Выполняется проверка статуса лицензии** – Kaspersky Embedded Systems Security 2.2 проверяет добавленный файл ключа или примененный код активации и ожидает ответа о текущем статусе ключа.
- **Дата окончания срока действия лицензии** – программа активирована до указанных даты и времени. Статус ключа выделен желтым цветом в следующих случаях:
  - 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.
- **Программа не активирована** – программа не активирована, так как не добавлен ключ или код активации. Статус выделен красным цветом.
- **Срок действия лицензии истек** – программа не активирована, так как истек период действия лицензии. Статус выделен красным цветом.
- **Нарушено Лицензионное соглашение** – программа Kaspersky Embedded Systems Security 2.2 не активирована, поскольку нарушены условия Лицензионного соглашения (см. раздел "О Лицензионном соглашении" на стр. 69). Статус выделен красным цветом.
- **Ключ помещен в черный список** – добавленный файл ключа 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 15. 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. Информация в графе Статус активации в панели управления узла Лицензирование может принимать следующие значения:<br>• **Применено** – если вы активировали программу с помощью кода активации или ключа.<br>• **Активация** – если вы применили код активации для активации программы и процесс активации еще не закончен. Статус принимает значение Применено по завершении активации программы и после обновления содержимого панели результатов узла.<br>• **Ошибка активации** – если не удалось активировать программу. Вы можете посмотреть причину неудачного завершения активации в журнале выполнения задач. |
| **Ключ** | Номер ключа, с помощью которого вы активировали программу. |
| **Тип лицензии** | Тип лицензии: коммерческая. |
| **Дата окончания срока действия** | Дата окончания срока действия лицензии по активному ключу. |
| **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 2.2 (см. таблицу ниже).

*Таблица 16. Подробная информация о лицензии в окне Свойства: <Статус кода активации или ключа>*

| Поле | Описание |
|---|---|
| **Закладка Общие** | |
| **Ключ** | Номер ключа, с помощью которого вы активировали программу. |
| **Дата добавления ключа** | Дата добавления ключа в программу. |
| **Тип лицензии** | Тип лицензии: коммерческая. |
| **Истекает через (сут)** | Число суток, оставшихся до даты окончания срока действия лицензии по активному ключу. |
| **Дата окончания срока действия** | Дата окончания срока действия лицензии по активному ключу. Если вы активируете программу по неограниченной подписке, в поле указывается значение *Не ограничена*. Если Kaspersky Embedded Systems Security 2.2 не удается определить дату окончания действия лицензии, указывается значение *Неизвестна*. |

| Поле | Описание |
|---|---|
| **Программа** | Название программы, для которой добавлен ключ или код активации. |
| **Ограничение на использование ключа** | Предусмотренное ограничение на использование ключа (если имеется). |
| **Осуществление технической поддержки** | Информация о том, оказывает ли "Лаборатория Касперского" или ее партнер техническую поддержку заказчику по условиям предоставления лицензии. |
| **Закладка Дополнительно** | |
| **Информация о лицензии** | Номер и тип действующей 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 заказчике лицензии: имя заказчика и название организации, для которой приобретена лицензия. |

# Функциональные ограничения даты окончания срока действия лицензии

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

- Все задачи останавливаются, за исключением задач Постоянная защита файлов, Проверка по требованию и Проверка целостности программы.
- Запуск любой задачи, кроме задач Постоянная защита файлов, Проверка по требованию и Проверка целостности программы, отклоняется. Эти задачи продолжат работать с использованием старых антивирусных баз.
- Функции задачи Защита от эксплойтов ограничены:
  - Процессы защищаются до их перезапуска.
  - Новые процессы нельзя добавить в область защиты.

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

# Продление срока действия лицензии

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

Вы можете продлить срок действия лицензии, не дожидаясь его окончания, с помощью добавления дополнительного ключа. Это позволяет не прерывать защиту сервера на период после окончания срока действия используемой лицензии и до активации программы по новой лицензии.

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

1. Приобретите новый код активации программы или файл ключа.
2. В дереве Консоли программы выберите узел **Лицензирование**.
3. В панели результатов узла **Лицензирование** выполните одно из следующих действий:
   - Если вы хотите 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**.
   - Если вы хотите 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 необходимо подключение к интернету.
4. Нажмите на кнопку **OK**.

Дополнительный ключ будет добавлен и автоматически станет активным по истечении срока действия лицензии на Kaspersky Embedded Systems Security 2.2.

# Удаление ключа

Вы можете удалить добавленный ключ из программы.

Если в Kaspersky Embedded Systems Security 2.2 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.

# Запуск и остановка Плагина управления Kaspersky Embedded Systems Security 2.2

Этот раздел содержит информацию о запуске и остановке Плагина управления Kaspersky Embedded Systems Security 2.2 и службы Kaspersky Security.

## Запуск Плагина управления Kaspersky Embedded Systems Security 2.2

Для запуска Плагина управления Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center дополнительных действий не требуется. После установки Плагина управления на компьютер администратора, запуск происходит одновременно с Kaspersky Security Center. Подробная информация о запуске Kaspersky Security Center содержится в *Справке Kaspersky Security Center*.

## 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 активности на компьютерах, проверки по требованию и обновления.

По умолчанию при запуске Kaspersky Embedded Systems Security 2.2 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 перезапустите 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 2.2, 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.

# Права доступа к функциям Kaspersky Embedded Systems Security 2.2

Этот раздел содержит информацию о правах на управление Kaspersky Embedded Systems Security 2.2 и службами Windows, которые регистрирует программа, а также инструкции по настройке этих прав.

## В этом разделе



# О правах на управление Kaspersky Embedded Systems Security 2.2

По умолчанию доступ ко всем функциям Kaspersky Embedded Systems Security 2.2 имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере, пользователи группы ESS Administrators, созданной на защищаемом компьютере при установке Kaspersky Embedded Systems Security 2.2, а также системная группа SYSTEM.

Пользователи, которые имеют доступ к функции **Изменение прав** Kaspersky Embedded Systems Security 2.2, могут предоставлять доступ к функциям Kaspersky Embedded Systems Security 2.2 другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Пользователи, не зарегистрированные в списке пользователей Kaspersky Embedded Systems Security 2.2, не могут открыть Консоль программы.

Вы можете выбрать для пользователя или группы пользователей один из следующих стандартных уровней доступа к функциям Kaspersky Embedded Systems Security 2.2:

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры работы Kaspersky Embedded Systems Security 2.2, параметры работы компонентов Kaspersky Embedded Systems Security 2.2, права пользователей Kaspersky Embedded Systems Security 2.2, а также просматривать статистику работы Kaspersky Embedded Systems Security 2.2.
- **Изменение** – доступ ко всем функциям программы, кроме изменения прав пользователей: возможность просматривать и изменять общие параметры работы Kaspersky Embedded Systems Security 2.2, параметры работы компонентов Kaspersky Embedded Systems Security 2.2.
- **Чтение** – возможность просматривать общие параметры работы Kaspersky Embedded Systems Security 2.2, параметры работы компонентов Kaspersky Embedded Systems Security 2.2, статистику работы Kaspersky Embedded Systems Security 2.2 и права пользователей Kaspersky Embedded Systems Security 2.2.

Можно также выполнять расширенную настройку прав доступа (см. раздел "Настройка прав доступа для Kaspersky Embedded Systems Security 2.2 и службы Kaspersky Security" на стр. 84): предоставлять или ограничивать доступ к отдельным функциям Kaspersky Embedded Systems Security 2.2.

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы будет установлен уровень доступа **Особые разрешения**.

*Таблица 17. Права доступа к функциям Kaspersky Embedded Systems Security 2.2*

| Права доступа | Описание |
|---|---|
| Управление задачами | Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Embedded Systems Security 2.2. |
| Создание и удаление задач | Возможность создавать и удалять задачи проверки по требованию. |
| Изменение параметров | Возможности:<br>• Импортировать в конфигурационный файл параметры работы Kaspersky Embedded Systems Security 2.2.<br>• Редактировать настройки программы. |
| Чтение параметров | Возможности:<br>• просматривать общие параметры работы Kaspersky Embedded Systems Security 2.2 и параметры задач;<br>• экспортировать в конфигурационный файл параметры работы Kaspersky Embedded Systems Security 2.2;<br>• просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений. |
| Управление хранилищами | Возможности:<br>• помещать объекты на карантин;<br>• удалять объекты из карантина и резервного хранилища;<br>• 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 2.2. |
| Лицензирование программы | Возможность активировать и деактивировать Kaspersky Embedded Systems Security 2.2. |
| Удаление программы | Возможность удалить Kaspersky Embedded Systems Security 2.2. |
| Чтение прав | Возможность просматривать список пользователей Kaspersky Embedded Systems Security 2.2 и права доступа каждого пользователя. |
| Изменение прав | Возможности:<br>• изменять список пользователей, имеющих доступ к управлению программой;<br>• изменять права доступа пользователей к функциям Kaspersky Embedded Systems Security 2.2. |

# О правах на управление службой Kaspersky Security

При установке Kaspersky Embedded Systems Security 2.2 регистрирует в Windows службу Kaspersky Security (KAVFS), так как программа включает в себя функциональные компоненты, запускаемые при старте 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, а также системные группы SERVICE и INTERACTIVE с правами на чтение и системная группа SYSTEM с правами на чтение и исполнение.

Вы не можете удалить учетную запись пользователя SYSTEM или изменять права этой учетной записи. Если права учетной записи пользователя SYSTEM были изменены, при сохранении изменений для этой учетной записи восстанавливаются максимальные права.

Пользователи, имеющие доступ уровня Изменение прав к функциям (см. раздел "О правах на управление Kaspersky Embedded Systems Security 2.2" на стр. 79), 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 2.2 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: давать или ограничивать права на управление Kaspersky Embedded Systems Security 2.2 (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 18. Разграничение прав доступа к функциям Kaspersky Embedded Systems Security 2.2*

| Функция | Описание |
|---|---|
| Чтение настроек службы | Возможность просматривать общие параметры работы 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 службы у Kaspersky Security. |

| Функция | Описание |
|---|---|
| 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. |
| 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:<br>• добавлять и удалять пользователей службы Kaspersky Security;<br>• изменять права доступа пользователей к службе Kaspersky Security. |
| Удаление службы | Возможность разрегистрации службы Kaspersky Security в Диспетчере управления службами Microsoft Windows. |
| Пользовательские запросы к службе | Возможность создавать и отправлять пользовательские запросы к службе Kaspersky Security. |

### Регистрация службы Kaspersky Security как доверенной 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 2.2 и используется для регистрации службы Kaspersky Security в качестве PPL во время запуска операционной системы. Когда служба Kaspersky Security (kavfs.exe) запускается как системный защищенный процесс, незащищенные процессы в системе не могут внедрять потоки, записывать в виртуальную память защищаемых процессов и останавливать службу.

При запуске процесса в качестве PPL пользователь не может управлять им, независимо от прав. Регистрация службы Kaspersky Security как PPL с помощью драйвера ELAM поддерживается операционной системой Microsoft Windows 10 и более поздних версий. Если программа Kaspersky Embedded Systems Security 2.2 установлена на компьютер под управлением операционной системы, поддерживающей PPL, управление правами пользователей для службы Kaspersky Security (KAVFS) будет недоступно.

Служба Kaspersky Security запускает все дочерние процессы как PPL.

► *Чтобы установить Kaspersky Embedded Systems Security 2.2 как защищаемый процесс, выполните следующую команду:*

```
msiexec /i ks4ws_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Для настройки применения PPL вы можете использовать командую строку.

# О правах доступа к службе Kaspersky Security Management

Вы можете просмотреть список служб Kaspersky Embedded Systems Security 2.2.

При установке Kaspersky Embedded Systems Security 2.2 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 2.2, 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 2.2.

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 2.2.

Вы можете подключиться к Kaspersky Embedded Systems Security 2.2 с локальной учетной записью, если на защищаемом компьютере зарегистрирована учетная запись с таким же именем и таким же паролем.

# Настройка прав доступа для Kaspersky Embedded Systems Security 2.2 и службы Kaspersky Security

Вы можете изменить список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Embedded Systems Security 2.2 и управлению службой Kaspersky Security, а также изменять права доступа этих пользователей и групп пользователей.

► *Чтобы добавить в список или удалить из списка пользователя или группу, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Дополнительные возможности** выполните одно из следующих действий:
   - Выберите пункт **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют права управления функциями Kaspersky Embedded Systems Security 2.2.
   - Выберите пункт **Права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют права управления службой Kaspersky Security.

     Откроется окно **Разрешения для группы "Kaspersky Embedded Systems Security 2.2"**.
4. В открывшемся окне выполните следующие действия:
   - Чтобы добавить пользователя или группу в список, нажмите кнопку **Добавить** и выберите пользователя или группу, которым вы хотите предоставить права.
   - Чтобы удалить пользователя или группу из списка, выберите пользователя или группу, доступ для которых вы хотите ограничить, и нажмите кнопку **Удалить**.
5. Нажмите кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Embedded Systems Security 2.2 или службой Kaspersky Security, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Дополнительные возможности** выполните одно из следующих действий:
   - Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security 2.2.
   - Выберите пункт **Изменить права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Embedded Systems Security**.
4. В открывшемся окне в списке **Группы или пользователи** выберите пользователя или группу пользователей, права которых вы хотите изменить.
5. В блоке **Разрешения для группы "<Пользователь (Группа)>"** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
   - **Полный контроль**: полный набор прав на управление Kaspersky Embedded Systems Security 2.2 или службой Kaspersky Security Service.
   - **Чтение**:
     - Следующие разрешения на управление Kaspersky Embedded Systems Security 2.2: **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 2.2, кроме **Изменение прав**;
     - Следующие разрешения на управление службой Kaspersky Security: **Изменение параметров службы, Чтение прав**.
   - **Исполнение**: следующие разрешения на управление службой Kaspersky Security Service: **Запуск службы**, **Остановка службы**, **Остановка/возобновление службы**, **Чтение прав**, **Определенные пользователем запросы к службе**.

6. 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 2.2** выберите нужного пользователя или 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 группе.
   e. Нажмите на кнопку **OK**.
   f. В окне **Дополнительные параметры безопасности для Kaspersky Embedded Systems Security 2.2** нажмите на кнопку **OK**.
7. В окне **Разрешения для Kaspersky Embedded Systems Security** нажмите на кнопку **Применить**.

Настроенные права на управление Kaspersky Embedded Systems Security 2.2 или службой Kaspersky Security будут сохранены.

# Защита доступа к функциям Kaspersky Embedded Systems Security 2.2 с помощью пароля

Вы можете ограничивать доступ к управлению программой и регистрируемыми службами с помощью настройки прав пользователей (см. раздел "Права доступа к функциям Kaspersky Embedded Systems Security 2.2" на стр. 79). Вы также можете дополнительно защитить доступ к выполнению критичных операций, установив защиту паролем в параметрах Kaspersky Embedded Systems Security 2.2.

Kaspersky Embedded Systems Security 2.2 запрашивает пароль при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- удаление Kaspersky Embedded Systems Security 2.2;
- изменение компонентного состава Kaspersky Embedded Systems Security 2.2;
- выполнение команд командной строки.

Kaspersky Embedded Systems Security 2.2 не отображает заданный пароль в читаемом виде в интерфейсе программы. Kaspersky Embedded Systems Security 2.2 хранит заданный пароль в виде контрольной суммы, рассчитанной при задании пароля.

Вы можете экспортировать и импортировать параметры программы, защищенные паролем. Конфигурационный файл, созданный в результате экспорта защищенных параметров программы, содержит контрольную сумму пароля и значение модификатора, используемого для удлинения строки пароля.

Не изменяйте значение контрольной суммы или модификатора в конфигурационном файле. Импорт защищенных паролем параметров, измененных вручную, может привести к полному блокированию доступа к управлению программой.

► *Чтобы защитить доступ к функциям Kaspersky Embedded Systems Security 2.2, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Разверните группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Если вы хотите настроить параметры политики для группы компьютеров, выберите закладку **Политики** и откройте **<Название политики> > Свойства**.
   - Если вы хотите настроить параметры программы для отдельного компьютера, перейдите к параметрам, которые требуется настроить, в окне **Параметры программы** в Kaspersky Security Center (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. 103).
3. В блоке **Безопасность** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры безопасности**.
4. В блоке **Параметры применения пароля** установите флажок **Использовать защиту паролем**.

   Поля **Пароль** и **Подтверждение пароля** станут активными.
5. В поле **Пароль** введите значение, которое вы хотите использовать для защиты доступа к функциям Kaspersky Embedded Systems Security 2.2.
6. В поле **Подтверждение пароля** введите пароль повторно.
7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены. Kaspersky Embedded Systems Security 2.2 будет запрашивать пароль при доступе к защищаемым функциям.

Установленный пароль невозможно восстановить. Утеря пароля ведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого компьютера.

Вы можете изменить или сбросить заданный пароль в параметрах программы в любой момент.

► *Чтобы сбросить пароль,*

снимите флажок **Использовать защиту паролем** в свойствах политики или программы.

Защита паролем будет отключена. Kaspersky Embedded Systems Security 2.2 удалит контрольную сумму старого пароля из параметров программы.

# Разрешение сетевых соединений для службы Kaspersky Security Management

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы разрешить сетевые соединения для службы Kaspersky Security Management на защищаемом компьютере, выполните следующие действия:*

1. На защищаемом компьютере под управлением Microsoft Windows выберите **Пуск > Панель управления > Безопасность > Брандмауэр Windows**.
2. В окне **Параметры брандмауэра Windows** выберите пункт **Изменить параметры**.
3. На закладке **Исключения** в списке стандартных исключений установите флажки: **COM + Сетевой доступ**, **Инструментарий управления Windows (WMI)** и **Удаленное администрирование**.
4. Нажмите на кнопку **Добавить программу**.
5. В окне **Добавление программы** выберите файл kavfsgt.exe. Этот файл хранится в папке, которую вы указали в качестве папки назначения при установке Консоли программы.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК** в окне **Параметры брандмауэра Windows**.

Сетевые соединения для службы Kaspersky Security Management на защищаемом компьютере будут разрешены.

# Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Embedded Systems Security 2.2 на нескольких компьютерах.

## В этом разделе



# О политиках

Вы можете создавать единые политики Kaspersky Security Center для управления защитой нескольких компьютеров, на которых установлена программа Kaspersky Embedded Systems Security 2.2.

Политика применяет указанные в ней значения параметров, функции и задачи Kaspersky Embedded Systems Security 2.2 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 2.2. 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 2.2 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 2.2 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.

## 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: <Название политики>** созданной политики вы можете настроить параметры задачи постоянной защиты компьютера, общие параметры Kaspersky Embedded Systems Security 2.2, параметры карантина и резервного хранилища, уровень детализации для журналов выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Embedded Systems Security 2.2.

► *Чтобы создать политику для группы компьютеров, на которых установлена и запущена программа Kaspersky Embedded Systems Security 2.2, 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 2.2 и нажмите на кнопку **Далее**.
4. В окне **Ввод названия групповой политики** укажите имя 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 **Обзор** и выберите политику, которую требуется применить.
   c. 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.

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

  Чтобы запустить задачу Использование KSN, требуется принять Положение о KSN в окне Обработка данных (см. раздел "Настройка обработки данных" на стр. 170).

- Чтобы изменить заданные по умолчанию параметры компонента Защита от эксплойтов, нажмите на кнопку **Настройка** в блоке **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 новой созданной политики.
9. В окне мастера **Завершение работы** 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 2.2.

## Настройка политики

В окне **Свойства: <Название политики>** существующей политики вы можете настроить общие параметры Kaspersky Embedded Systems Security 2.2, 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 2.2, 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, затем 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 требуется, чтобы политика применялась на всех компьютерах, входящих в выбранную группу администрирования.
   - **Неактивная политика**, если не требуется, чтобы политика применялась на всех компьютерах, входящих в выбранную группу администрирования.

   Вариант **Политика для автономных пользователей** недоступен при работе с Kaspersky Embedded Systems Security 2.2.
5. В разделах **Оповещение о событиях**, **Параметры программы**, **Журналы и уведомления**, **Дополнительные возможности**, **История ревизий** можно настроить общие 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.

Инструкции по настройке параметров задач и функций программы через Консоль программы содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

### Разделы параметров политики Kaspersky Embedded Systems Security 2.2

**Общие**

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

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

**Уведомления о событиях**

В разделе **Оповещение о событиях** вы можете настроить параметры для следующих категорий событий:

- *Критические события;*
- *Отказ функционирования;*
- *Предупреждение;*
- *Информационные события.*

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 19. Параметры в разделе Параметры программы*

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

**Дополнительные возможности**

*Таблица 20. Параметры в разделе Дополнительные возможности*

| Блок | Параметры |
|---|---|
| **Доверенная зона** | В блоке **Доверенная зона** по кнопке **Настройка** можно настроить следующие параметры применения доверенной зоны:<br>• сформировать список исключений доверенной зоны;<br>• включить или выключить проверку операций резервного копирования файлов;<br>• сформировать список доверенных процессов. |

| | |
|---|---|
| **Проверка съемных дисков** | Нажмите на кнопку **Настройка**, чтобы настроить параметры проверки съемных дисков, подключаемых по USB. |
| **Права пользователей на управление программой** | В этом разделе можно настроить права пользователей и групп пользователей на управление Kaspersky Embedded Systems Security 2.2. |
| **Права пользователей на управление службой Kaspersky Security** | В этом разделе можно настроить права пользователей и групп пользователей на управление службой Kaspersky Security. |
| **Хранилища** | В блоке **Хранилища** по кнопке **Настройка** вы можете настроить следующие параметры карантина, резервного хранилища и хранилища заблокированных узлов:<br>• указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище;<br>• настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства;<br>• указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина;<br>• настроить передачу информации об объектах резервного хранилища и карантина на Сервер администрирования; |

**Постоянная защита компьютера**

*Таблица 21. Параметры в разделе Постоянная защита компьютера*

| Блок | Параметры |
|---|---|
| **Постоянная защита файлов** | В блоке **Постоянная защита файлов** по кнопке **Настройка** можно настроить следующие параметры задачи:<br>• указать режим защиты объектов;<br>• настроить применение эвристического анализатора;<br>• настроить применение доверенной зоны;<br>• указать область защиты;<br>• задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную;<br>• настроить параметры запуска задачи. |
| **Использование KSN** | В блоке **Использование KSN** по кнопке **Настройка** вы можете настроить следующие параметры задачи:<br>• указать действия над объектами, недоверенными в KSN;<br>• настроить передачу данных и использование Kaspersky Security Center в качестве прокси-сервера KSN.<br>Нажмите на кнопку **Обработка данных**, чтобы принять или отклонить Положение о KSN, а также настроить параметры для надежной передачи данных. |

| Блок | Параметры |
|---|---|
| **Защита от эксплойтов** | В блоке **Защита от эксплойтов** по кнопке **Настройка** можно настроить следующие параметры задачи:<br>• выбрать режим защиты памяти процессов;<br>• указать действия для снижения рисков эксплуатации уязвимостей;<br>• дополнить и изменить список защищаемых процессов. |

**Контроль активности на компьютерах**

*Таблица 22. Параметры в разделе Контроль активности на компьютерах*

| Блок | Параметры |
|---|---|
| **Контроль запуска программ** | В блоке **Контроль запуска программ** по кнопке **Настройка** можно настроить следующие параметры задачи:<br>• выбрать режим работы задачи;<br>• настроить параметры контроля повторных запусков программ;<br>• указать область применения правил контроля запуска программ;<br>• настроить использование KSN;<br>• настроить параметры запуска задачи. |
| **Контроль устройств** | В блоке **Контроль устройств** по кнопке **Настройка** можно настроить следующие параметры задачи:<br>• выбрать режим работы задачи;<br>• настроить параметры запуска задачи. |

**Контроль активности в сети**

*Таблица 23. Параметры в разделе Контроль активности в сети*

| Блок | Параметры |
|---|---|
| **Управление сетевым экраном** | В блоке **Управление сетевым экраном** по кнопке **Настройка** можно настроить следующие параметры задачи:<br>• настроить правила сетевого экрана;<br>• настроить параметры запуска задачи. |

**Диагностика системы**

*Таблица 24. Параметры в разделе Диагностика системы*

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

**Журналы и уведомления**

*Таблица 25. Параметры в разделе Журналы и уведомления*

| Блок | Параметры |
|---|---|
| **Журналы выполнения задач** | В блоке **Журналы выполнения задач** по кнопке **Настройка** можно настроить следующие параметры:<br>• указать уровень важности регистрируемых событий для выбранных компонентов программы;<br>• указать параметры хранения журналов выполнения задач.<br>• указать параметры интеграции SIEM-системы с Kaspersky Security Center. |
| **Уведомления о событиях** | В блоке **Уведомления о событиях** по кнопке **Настройка** можно настроить следующие параметры:<br>• указать параметры уведомления пользователя для события *Обнаружен объект*;<br>• указать параметры уведомления администратора для любого выбранного события из списка событий в блоке **Настройка уведомлений**. |
| **Взаимодействие с Сервером администрирования** | В блоке **Взаимодействие с Сервером администрирования** по кнопке **Настройка** можно выбрать типы объектов, информацию о которых Kaspersky Embedded Systems Security 2.2 будет передавать на Сервер администрирования. |

**История ревизий**

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

# 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 2.2 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 запуске операционной системы, Проверка целостности модулей 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 2.2, 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 2.2 для группы компьютеров, 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 указанных задач.

   Установка или снятие флажков не влияет на параметры запуска локальных пользовательских задач указанного типа.
4. Убедитесь, что политика (см. раздел "О политиках" на стр. 89), которую вы настраиваете, активна и применена к группе компьютеров.
5. Нажмите на кнопку **OK**.

Настроенные параметры запуска по расписанию для выбранных задач будут применены.

# Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security 2.2, 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. 96) 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

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в Консоли программы. Инструкции по настройке параметров задач и функций программы в Консоли содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

► *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. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, для которой вы хотите создать задачу.
     b. В панели результатов перейдите на закладку **Задачи** и выберите пункт **Создать задачу**.
   - Для создания задачи для произвольного набора компьютеров в дереве Консоли администрирования Kaspersky Security Center в узле **Выборки устройств** выберите пункт **Создать задачу**.

   Откроется окно мастера создания задачи.
2. В окне **Выбор типа задачи** под заголовком **Kaspersky Embedded Systems Security 2.2** выберите тип создаваемой задачи.
3. Если вы выбрали любой тип задачи, кроме типов Откат обновлений баз или Активация программы, откроется окно **Параметры**. В зависимости от типа создаваемой задачи выполните одно из следующих действий:
   - *Если вы создаете задачу проверки по требованию*:
     a. В окне **Область проверки** сформируйте область проверки.

        По умолчанию область проверки включает критические области компьютера. Проверяемые области отображаются в таблице помеченными 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 области проверки, откройте контекстное меню на каждой из строк и выберите **Удалить область**.
- Чтобы включить в область проверки стандартную область, диск, папку, сетевой объект или файл, откройте контекстное меню в таблице **Область проверки** и выберите пункт Добавить область. В окне **Добавление в область проверки** выберите стандартную область в списке **Стандартная область**, укажите диск компьютера, папку, сетевой объект или файл на данном компьютере или другом компьютере в сети и нажмите на кнопку **ОК**.
- Чтобы исключить из проверки вложенные папки или файлы, выберите добавленную папку (диск) в окне **Область проверки** мастера, откройте контекстное меню и выберите пункт **Настроить**, затем в окне Уровень безопасности нажмите кнопку **Настройка** и в окне **Настройка проверки по требованию** на закладке **Общие** снимите флажки **Вложенные папки** и **Вложенные файлы**.
- Чтобы изменить параметры безопасности области проверки, откройте контекстное меню на области, параметры которой вы хотите изменить, и выберите **Настроить**. В окне **Настройка проверки по требованию** выберите один из стандартных уровней безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры безопасности вручную. Настройка параметров безопасности выполняется так же, как в Консоли Kaspersky Embedded Systems Security 2.2.
- Чтобы исключить из добавленной области проверки вложенные объекты, откройте контекстное меню в таблице **Область проверки**, выберите пункт **Добавить исключение** и укажите объекты, которые вы хотите исключить: выберите стандартную область в списке Стандартная область, укажите диск компьютера, папку, сетевой объект или файл на защищаемом или другом компьютере в сети и нажмите на кнопку **ОК**.
- Области, являющиеся исключениями из проверки, отображаются в таблице помеченными значком ☐.

b. В окне **Параметры** выполните следующие действия.

Установите флажок **Применять доверенную зону**, если в задаче вы хотите исключить из области проверки объекты, описанные в доверенной зоне Kaspersky Embedded Systems Security 2.2.

Если вы планируете использовать создаваемую задачу в качестве задачи проверки важных областей, в окне **Параметры** установите флажок **Выполнять задачу в фоновом режиме**. Программа Kaspersky Security Center оценивает состояние безопасности компьютеров по результатам выполнения задач со статусом проверки важных областей, а не только по результатам выполнения системной задачи **Проверка важных областей**. При создании локальной задачи проверки по требованию флажок недоступен.

Чтобы присвоить рабочему процессу, в котором будет выполняться задача, базовый приоритет **Низкий**, в окне **Параметры** установите флажок **Выполнять задачу в фоновом режиме**. По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Embedded Systems Security 2.2, имеют приоритет **Средний**. Понижение приоритета процесса увеличивает время выполнения задачи, но оно также может положительно повлиять на скорость выполнения процессов других активных программ.

- *Если вы создаете одну из задач обновления*, установите 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.

- *Если вы создаете задачу Обновление модулей программы*, в окне **Настройка параметров обновления модулей программы** настройте нужные параметры обновления программных модулей:

  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 2.2 автоматически выполняла перезагрузку компьютера после завершения задачи, установите флажок **Разрешать перезагрузку операционной системы**. Чтобы отменить автоматическую перезагрузку компьютера после завершения задачи, снимите флажок **Разрешать перезагрузку операционной системы**.

  c. Если вы хотите получать информацию о выходе плановых обновлений модулей Kaspersky Embedded Systems Security 2.2, 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.

- *Если вы создаете задачу Копирование обновлений*, в окне **Настройка параметров копирования обновлений** укажите состав обновлений и папку локального источника обновлений, в которую обновления будут сохранены.

- *Если вы создаете задачу Активация программы*, в окне **Параметры активации** примените файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если хотите создать задачу для продления срока действия лицензии.

- *Если вы создаете задачу Формирование правил контроля устройств или задачу Формирование правил контроля запуска программ*, в окне **Настройка** укажите параметры, на основе которых будет сформирован список разрешающих правил:

  a. Укажите префикс для названий правил (только для задачи формирования правил контроля запуска программ).

  b. Настройте параметры области применения разрешающих правил (только для задачи формирования правил контроля запуска программ). Нажмите на кнопку **Далее**.

c. Укажите действия, которые задача будет выполнять во время формирования разрешающих правил (только для задачи формирования правил контроля запуска программ) и по завершении.

4. Настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз). В окне **Расписание** выполните следующие действия:

   a. Чтобы включить расписание, установите флажок **Запускать задачу по расписанию**.

   b. Укажите частоту запуска задачи. Выберите одно из следующих значений из списка **Частота запуска**: **Ежечасно**, **Ежедневно**, **Еженедельно**, **При запуске программы**, **После обновления баз программы** (в групповых задачах Обновление баз программы и Обновление модулей программы вы также можете указать частоту запуска **После получения обновлений Сервером администрирования**).

      - если вы выбрали **Ежечасно**, укажите количество часов в поле **Раз в <количество> ч** в группе параметров **Параметры запуска задачи**;
      - если вы выбрали **Ежесуточно**, укажите количество дней в поле **Раз в <количество> сут** в группе параметров **Параметры запуска задачи**;
      - если вы выбрали **Еженедельно**, укажите количество недель в поле **Раз в <количество> нед.** в группе параметров **Параметры запуска задачи**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача будет запускаться по понедельникам).

   c. В поле **Время запуска** укажите время первого запуска задачи; в поле **Начать с** укажите дату начала действия расписания.

   d. Если требуется, задайте остальные параметры расписания: нажмите на кнопку **Дополнительно** и в окне **Дополнительные параметры расписания** выполните следующие действия:

      - Укажите максимальную продолжительность выполнения задачи: в блоке **Параметры остановки задачи**, в поле **Длительность** введите количество часов и минут.
      - Укажите промежуток времени в пределах суток, в течение которого выполнение задачи будет приостановлено: в блоке **Параметры остановки задачи** введите начальное и конечное значение промежутка в полях **Приостановить с** и **до**.
      - Укажите дату, начиная с которой расписание перестанет действовать: установите флажок **Отменить расписание с** и с помощью окна **Календарь** выберите дату, начиная с которой расписание перестанет действовать.
      - Включите запуск пропущенных задач: установите флажок **Запускать пропущенные задачи**.
      - Включите использование параметра распределения времени запуска: установите флажок **Распределять время запуска задач в интервале** и укажите значение параметра в минутах.

   e. Нажмите на кнопку **OK**.

5. Если создаваемая задача предназначена для набора компьютеров, выберите сеть (группу) компьютеров, на которых она будет выполняться.

6. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, с правами которой вы хотите выполнять задачу.

7. 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").

8. 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 в окне Параметры программы, 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.
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**.

> Если программа работает под управлением политики Kaspersky Security Center, и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в Консоли программы. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.2 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

# Настройка групповых задач в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в Консоли программы. Инструкции по настройке параметров задач и функций в Консоли программы содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

► *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 кода активации или ключа**, если хотите добавить код активации или ключ 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).
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 26. Параметры групповых задач Kaspersky Embedded Systems Security 2.2*

| Типы задач Kaspersky Embedded Systems Security 2.2 | Раздел в окне Свойства: <Название задачи> | Параметры задачи |
|---|---|---|
| Автоматическое формирование правил (см. раздел "Задачи формирования правил контроля устройств и контроля запуска программ" на стр. 110) | **Настройка** | При настройке параметров задачи Формирование правил контроля запуска программ вы можете:<br>• изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых разрешен автоматически сформированными правилами;<br>• учитывать или не учитывать запущенные программы. |

| Типы задач Kaspersky Embedded Systems Security 2.2 | Раздел в окне Свойства: <Название задачи> | Параметры задачи |
|---|---|---|
| | **Параметры** | Вы можете указать следующие действия при формировании разрешающих правил контроля запуска программ:<br>• **Использовать цифровой сертификат.**<br>• **Использовать заголовок и отпечаток цифрового сертификата.**<br>• **Если сертификат отсутствует, использовать.**<br>• **Использовать хеш SHA256.**<br>• **Формировать правила для пользователя или группы пользователей**<br>Вы можете настроить параметры для конфигурационных файлов со списком сформированных разрешающих правил контроля устройств и контроля запуска программ, которые Kaspersky Embedded Systems Security 2.2 создает по завершении задач. |
| | **Расписание** | Вы можете настраивать параметры запуска задачи по расписанию. |
| Активация программы (см. раздел "Задача Активация программы" на стр. 112). | **Параметры активации** | Вы можете добавить ключ для активации программы или для продления срока действия лицензии. |
| | **Расписание** | Вы можете настраивать параметры запуска задачи по расписанию. |
| Копирование обновлений (см. раздел "Задачи обновления" на стр. 113). | **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.<br>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 2.2 | Раздел в окне Свойства: <Название задачи> | Параметры задачи |
|---|---|---|
| | **Настройка параметров копирования обновлений** | Вы можете указать состав обновлений для копирования.<br>В поле **Папка для локального хранения скопированных обновлений** укажите путь к папке, в которой Kaspersky Embedded Systems Security 2.2 будет сохранять скопированные обновления. |
| | **Расписание** | Вы можете настраивать параметры запуска задачи по расписанию. |
| Обновление баз программы (см. раздел "Задачи обновления" на стр. 113) | **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.<br>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.<br>В блоке Оптимизация использования дисковой подсистемы вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему:<br>• **Снизить нагрузку на дисковую систему**<br>• **Объем оперативной памяти, используемый для оптимизации (МБ).** |
| | 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. |
| | **Расписание** | Вы можете настраивать параметры запуска задачи по расписанию. |

| Типы задач Kaspersky Embedded Systems Security 2.2 | Раздел в окне Свойства: <Название задачи> | Параметры задачи |
|---|---|---|
| Обновление модулей программы (см. раздел "Задачи обновления" на стр. 113) | **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.<br>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. |
| | **Настройка параметров обновления модулей программы** | Вы можете указать действия, которые Kaspersky Embedded Systems Security 2.2 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. |
| Проверка по требованию (см. раздел "Создание задачи проверки по требованию" | **Область проверки** | Вы можете сформировать область проверки для задачи проверки по требованию, а также перейти к настройке уровня безопасности. |
| | Окно **Настройка проверки по требованию** | Вы можете выбрать один из стандартных уровней безопасности или настроить параметры пользовательского уровня безопасности вручную. |

| Типы задач Kaspersky Embedded Systems Security 2.2 | Раздел в окне Свойства: <Название задачи> | Параметры задачи |
|---|---|---|
| на стр. 115). | **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.<br>В блоке **Интеграция с другими компонентами** вы можете настроить следующие параметры:<br>• применение Доверенной зоны в задачах проверки по требованию;<br>• применение служб KSN в задачах проверки по требованию;<br>• 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 модулей программы (на стр. 114). | **Расписание** | Вы можете настраивать параметры запуска задачи по расписанию. |

Для задачи типа Откат обновления баз программы вы можете 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

# Задачи формирования правил контроля устройств и контроля запуска программ

► *Чтобы настроить задачу Формирование правил контроля устройств или задачу Формирование правил контроля запуска программ, 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.
5. Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*
6. В разделе **Настройка** вы можете настроить следующие параметры:
   - изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых разрешен автоматически сформированными правилами;
   - учитывать или не учитывать запущенные программы.
7. 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. В дальнейшем программа будет разрешать запуск программ, которые запускаются с помощью файлов с указанными в правиле заголовком и отпечатком цифрового сертификата.

Использование этого флажка наиболее 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 для случая, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

  - **Хеш SHA256**. В качестве критерия разрешающего правила контроля запуска программ устанавливается значение контрольной суммы 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 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.

- **Использовать хеш SHA256.**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается значение контрольной суммы файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанным значением контрольной суммы.

  Этот вариант рекомендован для случаев, когда формирование правил обязательно для обеспечения соответствия максимальному уровню безопасности: в качестве уникального идентификатора файла может использоваться контрольная сумма SHA256. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Создавать правила для пользователя или группы пользователей**.

  Поле, в котором отображаются пользователь и / или группа пользователей. Программа будет контролировать запуски программ указанным пользователем и / 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 2.2 создает по завершении задач.

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

10. 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.*

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

    Настроенные параметры групповых задач будут сохранены.

## 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.
5. Подробная информация о настройке параметров в этом разделе содержится в *Справке Kaspersky Security Center.*
6. В разделе **Параметры активации программы** примените файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если хотите добавить ключ для продления срока действия лицензии.
7. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз).
8. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.
9. 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.*

10. 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 размещения 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 2.2 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 **Настройка параметров 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).
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 вы можете 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 модулей программы

► *Чтобы настроить групповую задачу Проверка целостности 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 разделе **Устройства**, выберите устройства для которых вы хотите настроить задачу проверки целостности модулей программы.

6. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз).
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.

# Создание задачи проверки по требованию

► *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 на строке с информацией о защищаемом компьютере и выберите пункт **Свойства**.
     c. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.
   - Для создания групповой задачи:
     a. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, для которой вы хотите создать задачу.
     b. В панели результатов откройте контекстное меню на закладке **Задачи** и выберите пункт **Создать > Задачу**.
   - Для создания задачи для произвольного набора компьютеров в дереве Консоли администрирования Kaspersky Security Center в узле **Выборки устройств** выберите пункт **Создать** задачу.

   Откроется окно мастера создания задачи.
2. 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").
3. В окне **Выбор типа задачи** под заголовком **Kaspersky Embedded Systems Security 2.2** выберите задачу **Проверка по требованию** и 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 области проверки, 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 **Стандартная область**, укажите диск компьютера, папку, сетевой объект или файл на данном компьютере 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 **Параметры 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. 158).
- 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 требуется исключить: выберите стандартную область в списке **Стандартная область**, укажите диск, папку, сетевой объект или файл на этом компьютере или другом компьютере в сети.
  c. Нажмите на кнопку **ОК**.

5. В окне **Параметры** настройте эвристический анализатор и интеграцию с другими компонентами:
   - Настройте использование эвристического анализатора (см. раздел "Использование эвристического анализатора" на стр. 153).

- Установите флажок **Применять доверенную зону**, если вы хотите исключить из области проверки задачи объекты, входящие в доверенную зону Kaspersky Embedded Systems Security 2.2.

  Флажок включает или выключает применение доверенной зоны в работе задачи.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.2 добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

  Если флажок снят, Kaspersky Embedded Systems Security 2.2 не учитывает файловые операции доверенных процессов при формировании области защиты в задаче Постоянная защита файлов.

  По умолчанию флажок установлен.

- Установите флажок **Использовать KSN для проверки**, если вы хотите использовать облачные службы Kaspersky Security Network для задачи.

  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 постоянной защиты файлов 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 2.2 и программ. Как следствие, скорость выполнения задачи замедляется 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 2.2 и другие программы. В этом случае скорость выполнения задачи увеличивается.

  По умолчанию флажок снят.

  По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Embedded Systems Security 2.2, 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 2.2. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

  Если флажок установлен, Сервер администрирования регистрирует событие Выполнена проверка важных областей и обновляет статус защиты компьютера по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

  Если флажок снят, задача проверки выполняется с низким приоритетом.

  Флажок установлен по умолчанию для задачи Проверка важных областей.

6. Нажмите на кнопку **Далее**.
7. В окне **Расписание** настройте расписание задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. 124).
8. Укажите учетную запись пользователя, под которой вы хотите выполнять задачу, и укажите название задачи.
9. Нажмите на кнопку **Готово**.

Будет создана новая задача проверки по требованию для выбранного компьютера или группы компьютеров.

## Настройка задач проверки по требованию

► *Чтобы настроить задачу Проверка по требованию, 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 блоке **Параметры** вы можете выполнить следующие действия:
   a. В блоке **Область проверки** установите флажки напротив тех, файловых ресурсов, которые вы хотите включить в область проверки.
   b. Нажмите кнопку **Настроить** и выберите уровень безопасности.

      Вы можете выбрать один из стандартных уровней безопасности или настроить параметры пользовательского уровня безопасности вручную.

   c. Чтобы настроить уровень безопасности вручную, в окне **Настройка проверки по требованию** нажмите на кнопку **Настройка**.
6. В разделе **Параметры** вы можете выполнить следующие действия:
   a. В блоке **Эвристический анализатор** включить или выключить использование эвристического анализатора и настроить уровень анализа с помощью ползунка.
   b. Настройте Дополнительные параметры (см. раздел "Создание задачи проверки по требованию" на стр. 115).
7. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз).

8. В разделе **Учетная запись** укажите учетную запись, с правами которой вы хотите выполнять задачу.
9. 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.*

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

    Настроенные параметры групповых задач будут сохранены.

## Присвоение задаче проверки по требованию статуса Задача проверки важных областей

По умолчанию Kaspersky Security Center присваивает компьютеру статус *Предупреждение*, если задача Проверка важных областей выполняется реже, чем определено порогом формирования события **Проверка важных областей давно не выполнялась** в Kaspersky Embedded Systems Security 2.2.

► *Чтобы настроить проверку всех компьютеров, входящих в одну группу администрирования, выполните следующие действия:*

1. Создайте групповую задачу проверки по требованию.
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.

   Вы можете установить флажок **Считать выполнение задачи проверкой важных областей** как при создании задачи проверки по требованию для группы или набора компьютеров, так и позже, в окне **Свойства: <Название задачи>**.

3. С помощью новой или существующей политики отключите запуск по расписанию системных задач проверки по требованию на компьютерах группы (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 96).

С этого момента Сервер администрирования Kaspersky Security Center будет оценивать состояние безопасности защищаемого компьютера и уведомлять вас о нем по результатам последнего выполнения задачи со статусом проверки 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.

# Проверка файлов в облачном хранилище

## Об облачных файлах

Kaspersky Embedded Systems Security 2.2 может взаимодействовать с облачными файлами Microsoft OneDrive. Программа поддерживает новую функцию "файлы OneDrive по запросу" (OneDrive Files On-Demand).

Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 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.

# Настройка параметров диагностики сбоев в Kaspersky Security Center

Если в работе Kaspersky Embedded Systems Security 2.2 возникла проблема (например, Kaspersky Embedded Systems Security 2.2 завершается аварийно) и вы хотите диагностировать ее, вы можете включить создание файлов трассировки и файла дампа процессов Kaspersky Embedded Systems Security 2.2 и отправить эти файлы на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Embedded Systems Security 2.2 не отправляет файлы трассировки и дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Embedded Systems Security 2.2 записывает информацию в файлы трассировки и файл дампа в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security 2.2. Можно настроить права доступа (см. раздел "Права доступа к функциям Kaspersky Embedded Systems Security 2.2" на стр. 79) 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. 103).
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 2.2 будет сохранять файлы трассировки.
- Настройте уровень детализации отладочной информации.

  В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Embedded Systems Security 2.2 сохраняет в файле трассировки.

  Вы можете выбрать один из следующих уровней детализации:

  - **Критические события** – Kaspersky Embedded Systems Security 2.2 сохраняет в файле трассировки только информацию о критических событиях.
  - **Ошибки** – Kaspersky Embedded Systems Security 2.2 сохраняет в файле трассировки информацию о критических событиях и ошибках.
  - **Важные события** – Kaspersky Embedded Systems Security 2.2 сохраняет в файле трассировки информацию о критических событиях, ошибках и важных событиях.
  - **Информационные события** – Kaspersky Embedded Systems Security 2.2 сохраняет в файле трассировки информацию о критических событиях, ошибках, важных событиях и информационных событиях.
  - **Вся отладочная информация** – Kaspersky Embedded Systems Security 2.2 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 27.* Коды подсистем Kaspersky Embedded Systems Security 2.2

| Код подсистемы | Название подсистемы |
|---|---|
| * | Все компоненты. |
| gui | Подсистема пользовательского интерфейса, оснастка Kaspersky Embedded Systems Security 2.2 в Microsoft Management Console. |
| ak_conn | Подсистема интеграции с Агентом администрирования Kaspersky Security Center. |
| bl | Управляющий процесс, реализует задачи управления Kaspersky Embedded Systems Security 2.2. |
| wp | Рабочий процесс; реализует задачи антивирусной защиты. |
| blgate | Процесс удаленного управления Kaspersky Embedded Systems Security 2.2. |
| 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 2.2 (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 2.2 применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Embedded Systems Security 2.2 сохраняет отладочную информацию о работе всех подсистем Kaspersky Embedded Systems Security 2.2 (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 2.2 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 2.2 по расписанию, а также настраивать параметры запуска по расписанию.

## В этом разделе

# Настройка параметров 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 задачи, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выполните следующие действия:
   - Если вы хотите настроить параметры политики, в группе компьютеров выберите **Политика** > **<Название политики>** > **<Раздел>** > **Настроить** > **Управление задачей**.
   - Если вы хотите настроить параметры программы для отдельного компьютера с помощью Kaspersky Security Center, откройте окно **Параметры задачи** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. 103) в Kaspersky Security Center.

     Откроется окно **Параметры**.
2. В открывшемся окне на закладке **Расписание** включите запуск задачи по расписанию, установив 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.
3. 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 вами количество часов, и укажите количество часов в поле **Раз в <количество> ч.**;
      - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное вами количество дней, и укажите количество дней в поле **Раз в <количество> сут.**;
      - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное вами 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 хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security 2.2;
      - **После обновления баз программы**, если 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 откроете окно **Параметры задачи** на закладке **Расписание**.

Значение **Запрещен политикой** в поле **Следующий запуск** отображается, если запуск системных задач по расписанию запрещен параметрами действующей политики Kaspersky Security Center (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. 96).

4. На закладке **Дополнительно** настройте в соответствии с вашими требованиями следующие параметры расписания.
   - 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.
5. Нажмите на кнопку **Применить**, чтобы сохранить параметры запуска задачи.

## Включение и выключение запуска 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 хотите включить запуск задачи по расписанию;
   - снимите флажок **Запускать задачу по расписанию,** если 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 кнопку **Применить**.

# Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center.

## В этом разделе



# Управление Kaspersky Embedded Systems Security 2.2 из Kaspersky Security Center

Вы можете централизованно управлять несколькими компьютерами с установленной программой Kaspersky Embedded Systems Security 2.2, включенными в группу администрирования, с помощью Плагина управления Kaspersky Embedded Systems Security 2.2. 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 2.2, для которых требуется настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования содержится в *Справке Kaspersky Security Center*.

Параметры программы на отдельном компьютере недоступны для настройки, если работа Kaspersky Embedded Systems Security 2.2 на этом компьютере контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Embedded Systems Security 2.2 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 компьютера 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, параметры задачи автоматического формирования разрешающих правил.
- **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 программы, так и параметры всех задач Kaspersky Embedded Systems Security 2.2, 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.

# О настройке общих параметров программы в Kaspersky Security Center

Вы можете настроить общие параметры Kaspersky Embedded Systems Security 2.2 из Kaspersky Security Center для группы компьютеров или для отдельного компьютера.

## В этом разделе



# Настройка масштабируемости и интерфейса в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в Консоли программы. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.2 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

► *Чтобы настроить параметры масштабируемости и интерфейса 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. 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. 91).

- 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. 103).

  Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

3. В разделе **Параметры программы** в блоке **Масштабируемость и интерфейс** нажмите на кнопку **Настройка**.
4. В окне **Масштабируемость и интерфейс** на закладке **Общие** настройте следующие параметры:
   - В блоке **Параметры масштабируемости** настройте параметры, определяющие количество используемых Kaspersky Embedded Systems Security 2.2 рабочих процессов:
     - **Определять параметры масштабируемости автоматически**.

       Kaspersky Embedded Systems Security 2.2 регулирует количество используемых процессов автоматически.
     - **Указать количество рабочих процессов вручную**.

       Kaspersky Embedded Systems Security 2.2 регулирует количество активных рабочих процессов в соответствии с указанными значениями.
       Это значение установлено по умолчанию.
       - **Максимальное количество активных процессов.**

         Максимальное количество процессов, которые использует Kaspersky Embedded Systems Security 2.2. 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**.
5. Нажмите на кнопку **OK**.

Настроенные параметры программы будут сохранены.

# Настройка параметров безопасности в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в Консоли программы. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.2 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

► *Чтобы вручную настроить параметры безопасности, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Свойства программы** в блоке **Безопасность и надежность** нажмите на кнопку **Настройка**.
4. В окне **Параметры безопасности** настройте следующие параметры:
   - В блоке **Параметры надежности** настройте параметры восстановления задач Kaspersky Embedded Systems Security 2.2 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 2.2 после сбоя в работе программы или аварийного завершения работы программы.

       Если флажок установлен, Kaspersky Embedded Systems Security 2.2 автоматически восстанавливает задачи Kaspersky Embedded Systems Security 2.2 после сбоя в работе программы или аварийного завершения работы программы.

       Если флажок снят, Kaspersky Embedded Systems Security 2.2 не восстанавливает задачи Kaspersky Embedded Systems Security 2.2 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 2.2. 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 2.2 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 2.2 не запускает задачи проверки по расписанию при переходе компьютера на источник бесперебойного питания до восстановления стандартного режима питания.

    Если флажок снят, Kaspersky Embedded Systems Security 2.2 запускает задачи проверки по расписанию вне зависимости от режима питания компьютера.

    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 2.2 останавливает выполнение запущенных задач проверки при переходе компьютера на источник бесперебойного питания.

    Если флажок снят, Kaspersky Embedded Systems Security 2.2 продолжает выполнение запущенных задач проверки при переходе компьютера на источник бесперебойного питания.

    По умолчанию флажок установлен.

  Компьютер переходит на источник бесперебойного питания, только если уровень заряда батареи опускается ниже 90%.
- В блоке **Параметры применения пароля** задайте пароль для защиты доступа к функциям Kaspersky Embedded Systems Security 2.2.

5. Нажмите на кнопку **OK**.

Настроенные параметры безопасности и надежности будут сохранены.

## Настройка параметров соединения в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в Консоли программы. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.2 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

Настроенные параметры соединения используются для подключения Kaspersky Embedded Systems Security 2.2 к серверам обновлений и активации, а также при интеграции программ со службами KSN.

► *Чтобы настроить параметры соединения, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Свойства программы** в блоке **Прокси-сервер:** нажмите на кнопку **Настройка**.

   Откроется окно **Настройка параметров соединения**.
4. 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 2.2 не использует прокси-сервер для соединения с службами KSN, а выполняет соединение напрямую.
     - **Автоматически определять параметры прокси-сервера**.

       Если выбран этот вариант, Kaspersky Embedded Systems Security 2.2 автоматически определяет параметры подключения к службам KSN с использованием протокола Web Proxy Auto-Discovery Protocol (WPAD).

       Данный вариант выбран по умолчанию.
     - **Использовать параметры указанного прокси-сервера**.

       Если выбран этот вариант, для соединения с KSN Kaspersky Embedded Systems Security 2.2 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 2.2.

       Если флажок установлен, обращение к компьютерам из сети, к которой принадлежит компьютер с установленным Kaspersky Embedded Systems Security 2.2, 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**.

5. Нажмите на кнопку **OK**.

Настроенные параметры соединения будут сохранены.

# О настройке дополнительных возможностей программы

Вы можете настроить дополнительные возможности Kaspersky Embedded Systems Security 2.2 из Kaspersky Security Center для группы компьютеров или для отдельного компьютера.

## В этом разделе

# Настройка параметров доверенной зоны в Kaspersky Security Center

По умолчанию во вновь созданных политиках и задачах доверенная зона применяется.

► *Чтобы настроить параметры доверенной зоны, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в блоке параметров **Доверенная зона**.

   Откроется окно **Доверенная зона**.
4. На закладке **Исключения** укажите объекты, которые Kaspersky Embedded Systems Security 2.2 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 2.2 будет считать доверенными.
   - Если вы хотите вручную указать условия, при удовлетворении которым файл будет считаться доверенным, нажмите на кнопку **Добавить**. В открывшемся окне укажите следующие параметры:
     - **Проверяемый объект.**

       Добавляет файл, папку, диск или файл скрипта в исключения.

       Если установлен этот флажок, Kaspersky Embedded Systems Security 2.2 пропускает указанный диапазон, файл, папку, диск или файл скрипта при запуске проверки с использованием компонентов Kaspersky Embedded Systems Security 2.2, выбранных в разделе **Область применения исключения**.

       По умолчанию флажок установлен.

- **Обнаруживаемые объекты.**

  Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Вы можете найти список имен обнаруживаемых объектов на сайте Вирусной энциклопедии.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.2 пропускает при проверке указанные объекты.

  Если флажок снят, Kaspersky Embedded Systems Security 2.2 обнаруживает все объекты, указанные в программе по умолчанию.

  По умолчанию флажок снят.

- **Область применения исключения.**

  Название задачи Kaspersky Embedded Systems Security 2.2, в которой применяется правило.

- Если требуется, укажите дополнительную информацию, поясняющую исключение, в поле **Комментарий**.

5. В окне **Доверенная зона** на закладке **Доверенные процессы** укажите процессы, которые Kaspersky Embedded Systems Security 2.2 будет пропускать при проверке:

   - **Не проверять файловые операции резервного копирования.**

     Флажок включает или выключает проверку операций чтения файлов, если эти операции выполняются установленными на компьютере средствами резервного копирования.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 пропускает при проверке операции чтения файлов, выполняемые установленными на компьютере средствами резервного копирования.

     Если флажок снят, Kaspersky Embedded Systems Security 2.2 проверяет операции чтения файлов, выполняемые установленными на компьютере средствами резервного копирования.

     По умолчанию флажок установлен.

   - **Не проверять файловую активность указанных процессов.**

     Флажок включает или выключает проверку файловой активности доверенных процессов.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 пропускает при проверке файловые операции доверенных процессов.

     Если флажок снят, Kaspersky Embedded Systems Security 2.2 проверяет файловые операции доверенных процессов.

     По умолчанию флажок снят.

6. При необходимости добавьте процессы, файловую активность которых вы не хотите проверять, нажав на кнопку **Добавить** (см. раздел "Добавление доверенных процессов" на стр. 135).

7. Нажмите на кнопку **ОК** в окне **Доверенная зона**, чтобы сохранить изменения.

## Добавление доверенных процессов

► *Чтобы добавить один или несколько процессов в список доверенных, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в блоке параметров **Доверенная зона**.

   Откроется окно **Доверенная зона**.
4. На закладке **Доверенные процессы** установите флажок **Не проверять файловую активность указанных процессов**.
5. Нажмите на кнопку **Добавить**.
6. Выберите один из 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 2.2 будет использовать полный путь к файлу для определения статуса доверенности процесса.

        Если флажок не установлен, путь к файлу не будет учитываться в качестве критерия для определения статуса доверенности процесса.

        По умолчанию флажок установлен.

     b. **Использовать хеш файла для определения доверенности процесса**.

        Если флажок установлен, Kaspersky Embedded Systems Security 2.2 использует хеш выбранного файла для определения статуса доверенности процесса.

        Если флажок не установлен, хеш файла не учитывается в качестве критерия для определения 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**.

> Требуется, чтобы учетная запись, с правами которой запускается задача Постоянная защита файлов, имела права администратора на компьютере с установленной программой Kaspersky Embedded Systems Security 2.2, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, 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 и пути.**

  В открывшемся окне **Добавление процессов в список доверенных вручную** настройте следующие параметры:

  a. Укажите путь к исполняемому файлу (включая имя файла)

  b. Нажмите на кнопку **OK**.

- **Один процесс на основе свойств объекта.**

  В открывшемся окне **Добавление процессов в список доверенных** 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 2.2 будет использовать полный путь к файлу для определения статуса доверенности процесса.

     Если флажок не установлен, путь к файлу не будет учитываться в качестве критерия для определения статуса доверенности процесса.

     По умолчанию флажок установлен.

  c. **Использовать хеш файла для определения доверенности процесса**.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 использует хеш выбранного файла для определения статуса доверенности процесса.

     Если флажок не установлен, хеш файла не учитывается в качестве критерия для определения статуса доверенности процесса.

     По умолчанию флажок установлен.

  d. Нажмите на кнопку **OK**.

Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран по крайней мере один критерий доверенности.

7. В окне **Добавление доверенного процесса** 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 2.2 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 администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
2. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в блоке параметров **Доверенная зона**.

   Откроется окно **Доверенная зона**.
4. На закладке **Исключения**, прокрутите список и выберите строку со значением **not-a-virus:***, если флажок снят.
5. Нажмите на кнопку **ОК**.

Новые настройки будут применены.

## Проверка съемных дисков

Вы можете настроить проверку съемных дисков, подключаемых к защищаемому компьютеру по USB.

Kaspersky Embedded Systems Security 2.2 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 Проверка по требованию.

Kaspersky Embedded Systems Security 2.2 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 2.2 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 28. 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.<br>Kaspersky Embedded Systems Security 2.2 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:<br>• Максимальная защита<br>• Рекомендуемый<br>• Максимальное быстродействие<br>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. |

► *Чтобы настроить параметры проверки съемных дисков при подключении, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Дополнительные параметры** нажмите на кнопку **Настройка** в блоке **Проверка съемных дисков**.

   Откроется окно **Проверка съемных дисков**.
4. В блоке **Проверка при подключении** выполните следующие действия:
   - Установите флажок **Проверять съемные диски при подключении по USB**, если вы хотите, чтобы программа Kaspersky Embedded Systems Security 2.2 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.
5. Нажмите на кнопку **ОК**.

   Настроенные параметры будут сохранены и применены.

# 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.

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в Консоли программы. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.2 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

► *Чтобы настроить права доступа к управлению программой и службой Kaspersky Security, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. Откройте раздел **Дополнительные возможности** и выполните следующие действия:
   - Если вы хотите настроить права доступа к управлению Kaspersky Embedded Systems Security 2.2 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**.
4. В открывшемся окне настройте права доступа в соответствии с вашими требованиями (см. раздел "Права доступа к функциям Kaspersky Embedded Systems Security 2.2" на стр. 79).

Настроенные параметры будут сохранены.

# Настройка параметров карантина и резервного хранилища в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в Консоли программы. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.2 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

► *Чтобы настроить параметры резервного хранилища в Kaspersky Security Center, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в блоке **Хранилища**.
4. В окне **Параметры хранилищ** на закладке **Резервное хранилище** настройте следующие **параметры резервного хранилища**:
   - Если вы хотите задать папку резервного хранилища, в поле **Папка резервного хранилища** выберите нужную папку на локальном диске защищаемого компьютера или введите полный путь к ней.
   - Если вы хотите задать максимальный размер **резервного хранилища**, установите флажок **Максимальный размер резервного хранилища (МБ)** и в поле ввода укажите нужное значение параметра в мегабайтах.
   - Если вы хотите 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.
   - Если вы хотите задать папку для восстановления, в блоке Параметры восстановления объектов выберите нужную папку на локальном диске защищаемого компьютера или в поле **Папка, в которую восстанавливаются объекты** введите имя папки и полный путь к ней.

5. В окне **Параметры хранилищ** на закладке **Карантин** настройте следующие **параметры карантина**:
   - Если вы хотите изменить папку карантина, в поле **Папка карантина** укажите полный путь к папке на локальном диске защищаемого компьютера.
   - Если вы хотите указать **максимальный размер карантина**, установите флажок **Максимальный размер карантина (МБ)** и в поле ввода укажите значение параметра в мегабайтах.
   - Если вы хотите 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 из карантина, в поле **Папка, в которую восстанавливаются объекты** укажите полный путь к папке на локальном диске защищаемого компьютера.
6. Нажмите на кнопку **ОК**.

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 2.2 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 2.2 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 **События** или в окне **Параметры уведомлений** вы можете настраивать следующие типы уведомлений:

- На закладке **События** (стандартная закладка программы Kaspersky Security Center) вы можете настраивать 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.

> Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в Консоли программы. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.2 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

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 уведомления о событиях одного типа одним способом и на закладке **События**, и в окне **Параметры уведомлений,** системный администратор будет получать уведомления об этих событиях указанным способом дважды.

## В этом разделе



# Настройка параметров журналов

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в Консоли программы. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.2 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

► *Чтобы настроить параметры журналов Kaspersky Embedded Systems Security 2.2, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

3. В разделе **Журналы и уведомления** нажмите на кнопку **Настройка** в блоке **Журналы выполнения задач**.
4. В окне **Параметры журналов** настройте следующие параметры Kaspersky Embedded Systems Security 2.2 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 2.2, 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**.
5. Нажмите на кнопку **ОК**.

Настроенные параметры журналов будут сохранены.

## Журнал безопасности

Kaspersky Embedded Systems Security 2.2 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, так же как и журнал системного аудита. При этом Kaspersky Embedded Systems Security 2.2 фиксирует 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 нарушений безопасности

Kaspersky Embedded Systems Security 2.2 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 подключение к основному syslog-серверу или его использование недоступны.

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

*Таблица 29. 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<br>Порт: 514 | Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей.<br>Вы можете указать значение IP-адреса только в формате IPv4. |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен** | Не применяется | Вы можете включать и отключать применение зеркального syslog-сервера с помощью флажка. |
| Параметры подключения к дополнительному syslog-серверу | IP-адрес: 127.0.0.1<br>Порт: 514 | Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей.<br>Вы можете указать значение IP-адреса только в формате IPv4. |

► *Чтобы настроить параметры интеграции с SIEM, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Журналы и уведомления** нажмите на кнопку **Настройка** в блоке **Журналы выполнения задач**.

   Откроется окно **Параметры журналов и уведомлений**.
4. Выберите закладку **Интеграция с SIEM**.
5. 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.

6. При необходимости 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.

7. 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.

8. 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.

   - Если требуется, установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если 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.

9. Нажмите на кнопку **OK**.

Настроенные параметры интеграции с SIEM будут применены.

## Настройка параметров уведомлений

► *Чтобы настроить параметры уведомлений Kaspersky Embedded Systems Security 2.2, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Журналы и уведомления** в блоке **Уведомления о событиях** нажмите на кнопку **Настройка**.
4. В окне **Параметры уведомлений** настройте следующие параметры Kaspersky Embedded Systems Security 2.2 согласно вашим требованиям:
   - В списке **Настройка уведомлений** выберите тип уведомления, параметры которого вы хотите настроить.
   - В блоке **Уведомление пользователей** настройте способ уведомления пользователя. Если требуется, задайте текст сообщения для уведомления.
   - В блоке **Уведомление администраторов** настройте способ уведомления администратора. Если требуется, задайте текст сообщения для уведомления. Если требуется, настройте дополнительные параметры уведомлений по кнопке **Настройка**.
   - В блоке **Пороги формирования событий** укажите интервалы времени, по истечении которых Kaspersky Embedded Systems Security 2.2 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.
5. Нажмите на кнопку **OK**.
6.

## Настройка обмена информацией с Сервером администрирования

► *Чтобы выбрать типы объектов, информацию о которых Kaspersky Embedded Systems Security 2.2 будет передавать на Сервер администрирования Kaspersky Security Center, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Журналы и уведомления** в блоке **Взаимодействие с Сервером администрирования** нажмите на кнопку **Настройка**.

   Откроется окно **Сетевые списки Сервера администрирования**.
4. В окне **Сетевые списки Сервера администрирования** выберите типы объектов, информацию о которых Kaspersky Embedded Systems Security 2.2 будет передавать на Сервер администрирования Kaspersky Security Center:
   - объекты на карантине;
   - резервные копии объектов;
5. Нажмите на кнопку **OK**.

   Kaspersky Embedded Systems Security 2.2 будет передавать информацию о выбранных типах объектов на Сервер администрирования.

# 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 и параметров безопасности защищаемого компьютера.

## В этом разделе



# 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 2.2 проверяет следующие объекты защищаемого компьютера при доступе к ним:

- файлы;
- альтернативные потоки файловых систем (NTFS-streams);
- главную загрузочную запись и загрузочные секторы локальных жестких дисков и внешних устройств;
- файлы контейнеров Windows Server® 2016 и Windows Server 2019.

При записи или считывании записанного файла любой программой на компьютере Kaspersky Embedded Systems Security 2.2 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. Kaspersky Embedded Systems Security 2.2 возвращает файл программе, если он не заражен или успешно вылечен.

Kaspersky Embedded Systems Security 2.2 перехватывает файловые операции, исполняемые в контейнерах Windows Server 2016 и Windows Server 2019.

*Контейнер* – это изолированная среда, где программа может работать без прямого взаимодействия с операционной системой. Если контейнер расположен в области защиты задачи, Kaspersky Embedded Systems Security 2.2 проверяет файлы контейнера, к которому получают доступ пользователи, на наличие компьютерных угроз. При обнаружении угрозы, программа пытается вылечить контейнер. Если лечение успешно, контейнер продолжает работу. Если лечение невозможно, контейнер выключается.

Kaspersky Embedded Systems Security 2.2 также обнаруживает вредоносную активность в процессах подсистемы Windows Subsystem for Linux®. Для таких процессов задача Постоянная защита файлов применяет действие, указанное в текущих настройках.

## Настройка задачи Постоянная защита файлов

По умолчанию системная задача Постоянная защита файлов имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

*Таблица 30. Параметры задачи Постоянная защита файлов по умолчанию*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| Область защиты | Весь компьютер, исключая виртуальные диски. | Вы можете ограничить область защиты. |
| Уровень безопасности | Единый для всей области защиты; соответствует уровню безопасности **Рекомендуемый**. | Для выбранных узлов в дереве файловых ресурсов компьютера вы можете:<br>• применить другой стандартный уровень безопасности;<br>• вручную изменить уровень безопасности;<br>• сохранить набор параметров безопасности выбранного узла в шаблон для дальнейшего использования. |
| **Режим защиты объектов** | При открытии и изменении. | Вы можете выбрать режим защиты объектов – указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security 2.2 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 компьютера с помощью инфраструктуры облачных служб Kaspersky Security Network (доступно, только если принято Положение о KSN). |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| Расписание запуска задачи | При запуске программы. | Вы можете настроить запуск задачи по расписанию. |

► *Чтобы настроить параметры задачи Постоянная защита файлов, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Постоянная защита файлов** нажмите на кнопку **Настройка** в блоке **Постоянная защита файлов**.

   Откроется окно **Постоянная защита файлов**.
4. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - Режим защиты (см. раздел "Выбор режима защиты" на стр. 154);
     - Применение эвристического анализатора (на стр. 153).
     - Параметры интеграции с другими компонентами Kaspersky Embedded Systems Security 2.2.
   - На закладке **Управление задачей**:
     - Запуск задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 124).
5. Выберите закладку **Область защиты** и выполните следующие действия:
   - Нажмите на кнопку **Добавить** или **Изменить**, чтобы изменить область защиты (см. раздел "Область защиты в задаче Постоянная защита файлов" на стр. 155).
     - В открывшемся окне выберите, что вы хотите включить в область защиты задачи:
       - **Стандартная область**
       - **Диск, папка или сетевое расположение**
       - **Файл**

- Выберите один из стандартных уровней безопасности (см. раздел "Выбор стандартных уровней безопасности" на стр. 155) или настройте параметры защиты вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 158).

6. Нажмите на кнопку **ОК** в окне **Постоянная защита файлов**.

Kaspersky Embedded Systems Security 2.2 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.

## Применение эвристического анализатора

Вы можете использовать эвристический анализатор и выбрать уровень анализа для задач Kaspersky Embedded Systems Security 2.2.

► *Чтобы настроить эвристический анализатор, выполните следующие действия:*

1. Откройте параметры программы (см. раздел "Управление Kaspersky Embedded Systems Security 2.2 из Kaspersky Security Center" на стр. 126) или параметры политики (см. раздел "Настройка политики" на стр. 91), для которой вы хотите настроить использование эвристического анализатора.
2. 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. 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.

# Выбор режима защиты объектов

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. Блок **Режим защиты объектов** позволяет определить, при каком типе доступа к объектам Kaspersky Embedded Systems Security 2.2 их проверяет.

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. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
2. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в блоке **Постоянная защита файлов**.

   Откроется окно **Постоянная защита файлов**.
4. В открывшемся окне на закладке **Общие** выберите режим защиты объектов, который вы хотите установить:
   - **Интеллектуальный режим**

     Kaspersky Embedded Systems Security 2.2 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 2.2 повторно проверяет объект только после его последнего сохранения этим процессом.
   - **При открытии и изменении**

     Kaspersky Embedded Systems Security 2.2 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 2.2 проверяет все объекты при их открытии как на чтение, так и на выполнение или изменение.
   - **При выполнении**

     Kaspersky Embedded Systems Security 2.2 проверяет файл только при открытии на выполнение.
5. Нажмите на кнопку **OK**.

Выбранный режим защиты объектов будет установлен.

# Область защиты в задаче Постоянная защита файлов

Этот раздел содержит информацию о формировании и использовании области защиты в задаче Постоянная защита файлов и дальнейшей работе с ней.

## В этом разделе



## Стандартные области защиты

Файловые ресурсы защищаемого компьютера отображаются в параметрах задачи **Постоянная защита файлов** на закладке **Область 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 2.2 предусмотрены следующие стандартные области защиты:

- **Локальные жесткие диски**. Kaspersky Embedded Systems Security 2.2 защищает файлы на жестких дисках компьютера.
- **Съемные диски**. Kaspersky Embedded Systems Security 2.2 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 2.2 защищает файлы, которые записываются в сетевые папки или считываются из них программами, выполняемыми на компьютере. Kaspersky Embedded Systems Security 2.2 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).

## Выбор стандартных уровней безопасности

Для узлов / элементов, выбранных в дереве / списке сетевых файловых ресурсов, можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**. Каждый из этих уровней имеет свой набор значений параметров безопасности (см. таблицу ниже).

### Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, помимо использования Kaspersky Embedded Systems Security 2.2 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 защимых 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 вы предъявляете повышенные требования к компьютерной безопасности в сети организации.

*Таблица 31. 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 |
| **Проверять загрузочные секторы дисков и MBR** | Да | Да | Да |

| Параметры | Уровень безопасности | | |
|---|---|---|---|
| **Защита составных объектов** | • Упакованные объекты*<br>* Только новые и измененные | • SFX-архивы*<br>• Упакованные объекты*<br>• Вложенные OLE-объекты*<br>* Только новые и измененные | • SFX-архивы*<br>• Упакованные объекты*<br>• Вложенные OLE-объекты*<br>*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**, **Использовать эвристический анализатор** не входят в набор параметров стандартных уровней безопасности. Если, выбрав один из стандартных уровней безопасности, вы измените состояние параметров безопасности **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор**, выбранный вами стандартный уровень безопасности не изменится.

► *Чтобы выбрать один из стандартных уровней безопасности, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в блоке **Постоянная защита файлов**.

   Откроется окно **Постоянная защита файлов**.
4. На закладке **Область защиты**, выберите узел, параметры безопасности которого вы хотите настроить, и нажмите на кнопку **Настроить**.

Откроется окно **Настройка параметров постоянной защиты файлов**.

5. Выберите требуемый уровень безопасности в раскрывающемся списке:
   - **Максимальная защита**
   - **Рекомендуемый**
   - **Максимальное быстродействие**
6. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены.

Kaspersky Embedded Systems Security 2.2 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.

## Настройка параметров безопасности вручную

По умолчанию в задаче Постоянная защита файлов применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют значениям стандартного уровня безопасности **Рекомендуемый** (см. раздел "Выбор стандартных уровней безопасности" на стр. 155).

Вы можете изменять заданные по умолчанию значения параметров безопасности, настроив их как едиными для всей области защиты, так и различными для разных узлов в дереве или списке файловых ресурсов компьютера.

При работе с деревом 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.

► *Чтобы вручную настроить параметры безопасности выбранного узла, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в блоке **Постоянная защита файлов**.

   Откроется окно **Постоянная защита файлов**.

4. На закладке **Область защиты**, выберите узел, параметры безопасности которого вы хотите настроить, и нажмите кнопку **Настроить**.

   Откроется окно **Настройка параметров постоянной защиты файлов**.

5. На закладке **Уровень безопасности** вы можете выбрать любой существующий уровень или нажать кнопку **Настройка**, чтобы создать пользовательскую конфигурацию.
6. Вы можете настроить пользовательские параметры безопасности для выбранного узла в соответствии с вашими требованиями.
   - Общие параметры (см. раздел "Настройка общих параметров задачи" на стр. 159)
   - Действия (см. раздел "Настройка действий" на стр. 162)
   - Производительность (см. раздел "Настройка производительности" на стр. 164)
7. Нажмите кнопку **Сохранить** в окне **Настройка области защиты**.

Новые параметры области защиты будут сохранены.

## Настройка общих параметров задачи

► *Чтобы настроить общие параметры безопасности задачи Постоянная защита файлов, выполните следующие действия.*

1. Откройте окно **Параметры Постоянной защиты файлов** (см. раздел "Настройка параметров безопасности вручную" на стр. 158).
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 2.2 проверяет все объекты.
   - **Объекты, проверяемые по формату.**

     Kaspersky Embedded Systems Security 2.2 проверяет только потенциально заражаемые файлы на основании формата файла.

     Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security 2.2.
   - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах.**

     Kaspersky Embedded Systems Security 2.2 проверяет только потенциально заражаемые файлы на основании формата файла.

     Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Embedded Systems Security 2.2.
   - **Объекты, проверяемые по указанному списку расширений.**

     Kaspersky Embedded Systems Security 2.2 проверяет файлы на основании расширения файла. Список расширений файлов, которые нужно проверять, вы можете задать вручную по кнопке **Изменить** в окне **Список расширений**.
   - **Проверять загрузочные секторы дисков и MBR**

     Включение защиты загрузочных секторов дисков и главных загрузочных записей.
     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 проверяет загрузочные секторы и основную загрузочную запись 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 **Производительность** установите или снимите флажок **Защищать только новые и измененные файлы**.

   Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security 2.2 новыми или измененными с момента последней проверки.

   Если флажок установлен, Kaspersky Embedded Systems Security 2.2 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 уровней безопасности **Максимальное быстродействие** и **Рекомендуемый**. Если установлен уровень безопасности **Максимальная защита**, 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 2.2 проверяет архивы.

     Если флажок снят, Kaspersky Embedded Systems Security 2.2 пропускает архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня безопасности.

   - **Все / Только новые SFX-архивы.**

     Проверка самораспаковывающихся архивов.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 проверяет SFX-архивы.

     Если флажок снят, Kaspersky Embedded Systems Security 2.2 пропускает SFX-архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня безопасности.

     Параметр активен, 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 2.2 проверяет файлы почтовых баз.

  Если флажок снят, Kaspersky Embedded Systems Security 2.2 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 2.2 проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Embedded Systems Security 2.2 при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **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 2.2 проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Embedded Systems Security 2.2 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 2.2 проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Embedded Systems Security 2.2 пропускает встроенные в файл объекты при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

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 **Параметры Постоянной защиты файлов** (см. раздел "Настройка параметров безопасности вручную" на стр. 158).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**.

     Когда выбран этот режим, Kaspersky Embedded Systems Security 2.2 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** необходимо настроить отдельно для каждой области защиты. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security 2.2 автоматически изменит уровень безопасности на **Пользовательский**.
   - **Блокировать доступ**.

     Если выбран этот вариант, Kaspersky Embedded Systems Security 2.2 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. Удалить, если не удалось вылечить**
     - **Удалять**
     - **Рекомендуемое**
4. Выберите действие над возможно зараженными объектами:
   - **Только сообщать**.

     Когда выбран этот режим, Kaspersky Embedded Systems Security 2.2 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** необходимо настроить отдельно для каждой области защиты. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выбрали этот режим, Kaspersky Embedded Systems Security 2.2 автоматически изменит уровень безопасности на **Пользовательский**.

- **Блокировать доступ**.

  Если выбран этот вариант, Kaspersky Embedded Systems Security 2.2 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, вы можете выбрать основное и дополнительное действие для каждого типа объектов, нажав на кнопку **Настройка** рядом с флажком.

      Если флажок снят, Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 не выполняет выбранное действие, если родительский объект неизменяем.

   По умолчанию установлен флажок для уровня безопасности **Максимальная защита** и сняты флажки **Рекомендуемый** и **Максимальное быстродействие**.

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 **Параметры Постоянной защиты файлов** (см. раздел "Настройка параметров безопасности вручную" на стр. 158).
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 2.2 пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security 2.2 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 http://www.securelist.ru.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Embedded Systems Security 2.2 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.

- **Не проверять составные объекты размером более (МБ)**

  Исключение из проверки составных объектов больше указанного размера.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.2 пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

  Если флажок снят, Kaspersky Embedded Systems Security 2.2 проверяет составные объекты, не учитывая размер.

  По умолчанию флажок установлен для уровней безопасности **Рекомендуемый** и **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 2.2 проверяет только новые файлы и файлы, изменившиеся с момента последней проверки системных объектов NTFS.

  Если флажок снят, Kaspersky Embedded Systems Security 2.2 проверяет системные файлы NTFS независимо от их даты создания и изменения.

  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 2.2 проверяет только новые и измененные файлы.

  Если флажок снят, Kaspersky Embedded Systems Security 2.2 проверяет файлы независимо от даты их создания и изменения.

  По умолчанию флажок установлен.

5. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

# 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 2.2 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 2.2 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 2.2. 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 2.2:

- 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 *Справочной системе Kaspersky Security Center*.

Если вы используете Локальный KSN на защищаемом компьютере, в окне **Обработка данных** (см. раздел "Настройка обработки данных" на стр. 170) 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 работы 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 2.2: обработка всех связанных с KSN данных останавливается.

## Настройка параметров задачи Использование KSN

Вы можете изменять параметры задачи Использование KSN, заданные по умолчанию (см. таблицу ниже).

*Таблица 32. Параметры задачи Использование KSN по умолчанию*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Действия над объектами, недоверенными в KSN** | Удалить | Вы можете указывать действия, которые Kaspersky Embedded Systems Security 2.2 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 2.2 рассчитывает MD5-хеш для файлов любого размера. |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| Положение о KSN | Флажок **Я принимаю условия Положения о Kaspersky Security Network** снят. | Решите, хотите ли вы использовать KSN после установки. Вы можете изменять 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. |
| **Я принимаю условия Положения о Kaspersky Managed Protection** | Флажок снят | Вы можете включать и выключать применение сервиса KMP. Служба доступна, только если во время приобретения программы был подписан дополнительный договор. |
| 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. |

► *Чтобы настроить параметры задачи Использование KSN, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в блоке **Использование KSN**.

   Откроется окно **Использование KSN**.

4. На закладке **Общие** настройте следующие параметры задачи:

   - В блоке **Действия над объектами, недоверенными в KSN** укажите действие, которое Kaspersky Embedded Systems Security 2.2 необходимо совершить при обнаружении объекта, имеющего репутацию недоверенного в KSN:

     - **Удалить**

       Kaspersky Embedded Systems Security 2.2 удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.

       Этот вариант выбран по умолчанию.

     - **Фиксировать информацию в отчете**

       Kaspersky Embedded Systems Security 2.2 фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Embedded Systems Security 2.2 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 2.2 не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение.

       Если флажок снят, Kaspersky Embedded Systems Security 2.2 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 2.2 будет рассчитывать контрольную сумму.

   - 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*.

5. 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 компьютера.

Программа будет запускать задачу Использование KSN по расписанию.

6. Перед запуском задачи настройте обработку данных (см. раздел "Настройка обработки данных" на стр. 170).
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 выполнения задачи.

## Настройка обработки данных

► *Чтобы настроить типы данных, которые будут обрабатываться службами KSN, и принять Положение о KSN, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Постоянная защита компьютера** нажмите на кнопку **Обработка данных** в блоке **Использование KSN**.

   Откроется окно **Обработка данных**.
4. На закладке **Службы и статистика KSN** 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 2.2 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 2.2 не отправляет

контрольные суммы файлов в KSN.

Обратите внимание, что запросы файловой репутации могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов KSN "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 2.2 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 2.2 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 2.2.

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 2.2 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, только если установлен флажок **Я принимаю условия Положения о Kaspersky Security Network**.

По умолчанию Kaspersky Embedded Systems Security 2.2 отправляет контрольные суммы файлов и дополнительную статистику после принятия Положения о KSN.

*Таблица 33. 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 |
|---|---|---|
| ☑ | • отправляются запросы репутации<br>• действия с флажком доступны | • отправляется дополнительная статистика<br>• действия с флажком доступны |
| ☑ | • не отправляются запросы репутации<br>• действия с флажком недоступны | • не отправляется дополнительная статистика<br>• действия с флажком недоступны |
| ☐ | • не отправляются запросы репутации<br>• действия с флажком доступны | • не отправляется дополнительная статистика<br>• действия с флажком доступны |
| ☐ | • не отправляются запросы репутации<br>• действия с флажком недоступны | • не отправляется дополнительная статистика<br>• действия с флажком недоступны |

# 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 2.2 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 2.2, 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 2.2 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.

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 2.2 не выполняет завершение такого процесса независимо от режима, указанного в параметрах компонента Защита от эксплойтов.

- **Только сообщать о компрометации процесса**: применяйте данный режим, чтобы получать данные о фактах эксплуатации уязвимостей в защищаемых процессах с помощью событий в журнале нарушений безопасности.

  Если выбран данный режим, Kaspersky Embedded Systems Security 2.2 регистрирует все попытки эксплуатации уязвимостей посредством создания событий.

## Настройка параметров защиты памяти процессов

► *Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, 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. 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. 91).
   - 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. 103).

   > Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

3. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в блоке **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.

4. В блоке **Защита памяти процессов** настройте следующие параметры:

   - **Защищать процессы от эксплуатации уязвимостей**.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

     Если флажок снят, Kaspersky Embedded Systems Security 2.2 не защищает процессы на компьютере от эксплуатации уязвимостей.

     По умолчанию флажок снят.

   - **Завершать скомпрометированные процессы**.

     Если выбран данный режим, Kaspersky Embedded Systems Security 2.2 завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.

   - **Только сообщать о скомпрометированном процессе**.

     Если выбран данный режим, Kaspersky Embedded Systems Security 2.2 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 2.2 обнаруживает факт эксплуатации уязвимости критического процесса, компонент принудительно переходит в режим **Только сообщать о компрометации процесса**.

5. В блоке **Действия по защите** настройте следующие параметры:

   - **Сообщать о скомпрометированных процессах посредством службы терминалов.**

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 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 2.2 не будет выводить на экран терминальное окно при обнаружении факта попытки эксплуатации уязвимости или завершения скомпрометированного процесса. Терминальное окно отображается независимо от статуса работы 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 2.2 снижает риски эксплуатации уязвимостей уже запущенных процессов независимо от того, запущена ли служба Kaspersky Security. Kaspersky Embedded Systems Security 2.2 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 2.2 не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

  По умолчанию флажок установлен.

6. Нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security 2.2 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. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
2. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в блоке **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.
4. На закладке **Защищаемые процессы**, нажмите на кнопку **Обзор**.

Откроется окно проводника Windows.

5. Выберите процесс, который вы хотите добавить в список.
6. Нажмите на кнопку **Открыть**.

   Имя процесса будет отображено в строке.
7. Нажмите на кнопку **Добавить**.

   Указанный процесс добавится в список защищаемых процессов.
8. Выберите добавленный процесс и нажмите на кнопку **Указать техники снижения рисков**.

   Откроется окно **Техники защиты от эксплойтов**.
9. Выберите один из вариантов применения техник снижения рисков:
   - **Применять все доступные техники защиты от эксплойта**

     Если выбран этот вариант, редактирование списка недоступно, Все доступные для процесса техники будут применяться по умолчанию.
   - **Применять указанные техники защиты от эксплойта**

     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**.
10. 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 сайты
      - Сайты с ограниченным доступом
      - Компьютер

      Данные параметры применимы только для Internet Explorer®.
11. Нажмите на кнопку **ОК**.

Процесс будет добавлен в область защиты задачи.

## Техники защиты от эксплойтов

*Таблица 34. 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 Exeption 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. |
| 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. |

# Контроль активности на компьютерах

Этот раздел содержит информацию о функциональности Kaspersky Embedded Systems Security 2.2, которая позволяет контролировать запуски программ, подключения внешних устройств по USB, а также работу брандмауэра Windows.

## В этом разделе



# Управление запуском программ из Kaspersky Security Center

Вы можете запрещать или разрешать запуск программ на всех компьютерах в сети организации, формируя единые списки правил контроля запуска программ на стороне Kaspersky Security Center для групп компьютеров.

## В этом разделе



# Использование профиля при настройке задачи Контроль запуска программ в политике Kaspersky Security Center

Правила контроля запуска программ, настроенные в политике, применяются ко всем компьютерам группы администрирования. Если в одну группу администрирования входят компьютеры разных типов, для контроля запуска программ на каждом компьютере могут потребоваться индивидуальные списки правил. Для того чтобы разграничить применение политики к компьютерам внутри одной группы администрирования, можно использовать *профили политики*.

Рекомендуется применять профили политики для настройки правил контроля запуска программ на компьютерах разных типов внутри одной группы администрирования, управляемой единой политикой.

Это позволяет оптимизировать защиту компьютеров, так как заданные правила контролируют запуски только тех программ, которые характерны для данного типа компьютеров.

Профили политики применяются к компьютерам группы администрирования в соответствии с назначенными для них *тегами*. Вы можете настроить профиль политики для всех компьютеров группы, имеющих общий тег.

Подробная информация о тегах и профилях политики, а также инструкции по работе с ними содержатся в *Справке Kaspersky Security Center*.

► *Чтобы применить профиль политики в задаче Контроль запуска программ, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Разверните группу администрирования, для которой хотите настроить применение профилей политики.
2. Назначьте теги для каждого компьютера в группе администрирования в соответствии с типом этого компьютера. Для этого выполните следующие действия:
   - В панели результатов выбранной группы администрирования откройте закладку **Устройства** и выберите компьютер, для которого требуется назначить теги. В окне **Свойства: <Имя компьютера>** выберите раздел **Теги** и сформируйте список тегов. Нажмите на кнопку **OK**.
3. Создайте профиль политики и настройте его применение для защиты компьютеров в группе администрирования. Для этого выполните следующие действия:
   - В панели результатов выбранной группы администрирования откройте закладку **Политики** и выберите политику, для которой хотите настроить применение профилей. В окне **Свойства: <Имя политики>** выбранной политики откройте раздел **Профили политики** и нажмите на кнопку **Добавить**, чтобы создать новый профиль. Откроется окно **Свойства: <Имя профиля>**. Выполните следующие действия:
     a. В разделе **Правила активации** настройте область применения профиля и укажите условия, при которых профиль будет активирован.
     b. В разделе **Контроль запуска программ** настройте списки правил контроля запуска программ для редактируемого профиля.
     c. Нажмите на кнопку **OK**.
4. В окне **Свойства: <Имя политики>** нажмите на кнопку **OK**.

Настроенный профиль будет применен в политике для задачи Контроль запуска программ.

## Настройка параметров задачи Контроль запуска программ

Вы можете изменять значения параметров задачи Контроль запуска программ, заданных по умолчанию (см. таблицу ниже).

*Таблица 35. Параметры задачи Контроль запуска программ по умолчанию*

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| **Режим работы задачи** | **Только статистика**. Задача фиксирует события блокировки и запуска программ в соответствии с заданными правилами в журнале выполнения задачи. Фактическая блокировка запуска программ не выполняется. | Вы можете выбрать режим **Активный** для защиты компьютера после того, как будет сформирован окончательный список правил. |
| **Управление правилами** | **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. | Вы можете указывать типы файлов, запуск которых будет контролироваться правилами. |
| **Использование KSN** | Данные о репутации программ в KSN не используются. | Вы можете использовать данные о репутации программ в KSN при работе задачи Контроль запуска программ. |
| **Автоматически разрешать распространение для программ и пакетов из списка** | Не применяется. | Вы можете разрешать распространение программного обеспечения с помощью указанных в настройках пакетов установки и программ. По умолчанию разрешено только распространение программ с помощью Windows Installer. |
| **Разрешение распространения программ через Windows Installer** | Применяется. | Вы можете разрешить установку или обновление любого программного обеспечения, если операции выполняются через Windows Installer. |
| **Запретить запуск командных интерпретаторов без команд к исполнению** | Не применяется. | Вы можете запрещать запуск командных интерпретаторов без исполняемых команд. |
| **Запуск задачи** | Первый запуск не определен. | Задача Контроль запуска программ не запускается автоматически при старте Kaspersky Embedded Systems Security 2.2. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию. |

► *Чтобы настроить параметры задачи Контроль запуска программ, 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. 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. 91).
   - 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. 103).

   > Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Контроль активности на компьютерах** нажмите на кнопку **Настройка** в блоке **Контроль запуска программ**.

   Откроется окно **Контроль запуска программ**.
4. 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 2.2 контролирует запуск программ с помощью заданных правил.
     - **Только статистика**. Kaspersky Embedded Systems Security 2.2 не контролирует запуск программ с помощью заданных правил, а только фиксирует в журнале выполнения задач информацию о запусках программ. Запуск всех программ разрешен. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации, зарегистрированной в журнале выполнения задачи.

     По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.
   - Снимите или установите флажок **Повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках**.

     Флажок включает или выключает контроль повторного запуска программ на основе записей кеша о прецедентах.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 запрещает или разрешает выполнение повторно запущенной программы на основе решения, которое было принято при первом запуске программы задачей контроля запуска программ. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом событии сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки на наличие разрешающих правил.

Если флажок снят, Kaspersky Embedded Systems Security 2.2 проверяет программу при каждой попытке ее запуска.

По умолчанию флажок установлен.

- Снимите или установите флажок **Запретить запуск интерпретаторов команд при отсутствии команд**.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.2 запрещает запуск интерпретатора командной строки, даже если запуск интерпретатора разрешен. Запуск командной строки без команд разрешается только при выполнении обоих условий:

  - Запуск интерпретатора командной строки разрешен.
  - Выполняемая команда разрешена.

  Если флажок снят, Kaspersky Embedded Systems Security 2.2 учитывает только разрешающие правила для запуска командной строки. Запуск блокируется, если не применено разрешающее правило, или выполняемый процесс не имеет статуса доверенного в KSN. Если разрешающее правило применено, или у процесса есть статус доверенного в KSN, запуск командной строки разрешается как с командой, так и без нее.

  Kaspersky Embedded Systems Security 2.2 работает со следующими интерпретаторами:

  - cmd.exe;
  - powershell.exe;
  - python.exe;
  - perl.exe.

5. В блоке **Правила** настройте параметры применения правил:

   a. Нажмите кнопку **Список правил**, чтобы добавить разрешающие правила контроля запуска задач.

   Kaspersky Embedded Systems Security 2.2 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, заданный 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 2.2 применяет два стандартных правила, которые разрешают запуск скриптов, MSI-пакетов и файлов запуска по сертификату.

6. В блоке **Область применения правил** задайте следующие параметры:

   - **Использовать правила для исполняемых файлов**.

     Флажок включает / выключает контроль запуска исполняемых файлов программ.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 разрешает или запрещает запуск исполняемых файлов программ с помощью заданных правил, в параметрах которых указана область применения Исполняемые файлы.

     Если флажок снят, Kaspersky Embedded Systems Security 2.2 не контролирует запуск исполняемых файлов программ с помощью заданных правил. Запуск исполняемых файлов программ разрешен.

     По умолчанию флажок установлен.

   - **Контролировать загрузку DLL-модулей**.

     Флажок включает/выключает контроль загрузки DLL-модулей.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 разрешает или запрещает загрузку DLL-модулей с помощью заданных правил, в параметрах которых указана область применения "Исполняемые файлы".

     Если флажок снят, Kaspersky Embedded Systems Security 2.2 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 контроль запуска скриптов и пакетов MSI.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 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 2.2 не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

     По умолчанию флажок установлен.

7. В блоке **Использование KSN** настройте следующие параметры запуска программ:

   - **Не разрешать запуск программ, недоверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

     Если флажок установлен, Kaspersky Embedded Systems Security 2.2 запрещает запуск программ, имеющих статус недоверенных в KSN. При этом разрешающие правила контроля запуска программ, под которые подпадают недоверенные в KSN программы, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

Если флажок снят, Kaspersky Embedded Systems Security 2.2 не учитывает репутацию недоверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые подпадают программы.

По умолчанию флажок снят.

- **Разрешать запуск программ, доверенных в KSN**.

  Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

  Если флажок установлен, Kaspersky Embedded Systems Security 2.2 разрешает запуск программ, имеющих статус доверенных в KSN. При этом 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 2.2 не учитывает репутацию доверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые подпадают программы.

  По умолчанию флажок снят.

- Пользователи и / или группы пользователей, которым разрешен запуск доверенных в KSN программ.

8. На закладке **Контроль пакетов установки** настройте параметры контроля пакетов установки (см. раздел "Настройка контроля пакетов установки" на стр. 188).
9. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 124).
10. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Kaspersky Embedded Systems Security 2.2 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.

## О Контроле пакетов установки

Формирование правил контроля запуска программ может усложниться, если вам требуется учесть контроль пакетов установки на защищаемом компьютере. Например, для компьютеров, на которых выполняется периодическое автоматическое обновление установленных программ. В этом случае требуется обновлять списки разрешающих правил при каждом обновлении программного обеспечения, чтобы в параметрах задачи Контроль запуска программ учитывались запуски новых файлов, созданных в процессе обновления. Для упрощения контроля запуска файлов в сценариях распространения программного обеспечения вы можете использовать соответствующий модуль в задаче Контроль запуска программ.

*Пакет установки* (далее также "пакет") представляет собой программу, устанавливаемую на компьютере. 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 пакетов в этот список программа разрешает распаковку доверенных пакетов и автоматический запуск программного обеспечения, созданного и измененного доверенным пакетом. 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 2.2 контролирует только полный цикл распространения программного обеспечения. Программа не сможет корректно обработать запуски файлов, измененных доверенным пакетом, если при первом запуске такого пакета Контроль пакетов установки выключен или не установлен компонент Контроль запуска программ.

Контроль пакетов установки невозможен, если в настройках задачи Контроль запуска программ не установлен флажок **Использовать правила для исполняемых файлов**.

### Кеш контроля пакетов установки

Kaspersky Embedded Systems Security 2.2 определяет связь между файлами, созданными при распространении программного обеспечения, и доверенными пакетами с помощью динамического формирования *кеша контроля пакетов установки* (далее "кеш распространения"). При первом запуске доверенного пакета Kaspersky Embedded Systems Security 2.2 обнаруживает все файлы, созданные при распространении программного обеспечения с помощью этого пакета, и сохраняет их контрольные суммы и полные пути в кеше распространения. В дальнейшем запуски всех файлов, сохраненных в кеше распространения, разрешаются автоматически.

Вы не можете просматривать, очищать, а также вручную изменять кеш распространения через пользовательский интерфейс. Kaspersky Embedded Systems Security 2.2 самостоятельно наполняет его, а также контролирует его актуальность.

Вы можете экспортировать кеш распространения в конфигурационный файл (в формате XML), а также очищать кеш распространения 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 2.2 обновляет кеш распространения раз в сутки. Если значение полного пути или контрольной суммы ранее разрешенного файла изменены, программа удаляет запись о таком файле из кеша распространения. При активном режиме работы задачи Контроль запуска программ, дальнейшие запуски такого файла будут заблокированы.

### Обработка извлеченных файлов

Признак доверенности для всех файлов, извлеченных из доверенного пакета, наследуется при первом запуске пакета. Если вы снимете флажок после первого запуска, наследование признака сохранится для всех извлеченных из этого пакета файлов. Чтобы отменить исходное наследование признака извлеченными файлами, нужно очистить кеш распространения и снять флажок **Разрешить запуск всех 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, для признака доверенности нет ограничений на уровень вложенности.

Признак доверенности извлеченных файлов сохраняется и после перезагрузки операционной системы.

Обработка файлов настраивается в параметрах Контроля пакетов установки (см. раздел "Настройка Контроля пакетов установки" на стр. 188) с помощью флажка **Разрешать исполнение всей цепочке файлов, извлеченных из этого пакета установки**.

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 или запустить, даже если они содержат другие вложенные файлы. Это соблюдается для всех уровней вложенности.

Если пакет test.msi добавлен в список исключений, а флажок **Разрешить запуск всех 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.

### Взаимодействие с основным 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 для таких пакетов и файлов отсутствуют правила в основном списке правил контроля запуска программ.

### Использование KSN-заключений

Недоверенные KSN-заключения имеют больший приоритет, чем исключение Контроля пакетов установки: распаковка доверенного пакета установки или запуск созданных и измененных им файлов будут заблокированы, если для таких файлов получено недоверенное заключение от KSN.

## Настройка Контроля пакетов установки

► *Чтобы добавить доверенный пакет установки, 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. 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. 91).
   - 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. 103).

   Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Контроль активности на компьютерах** нажмите на кнопку **Настройка** в блоке **Контроль запуска программ**.

   Откроется окно **Контроль запуска программ**.
4. На выбранной закладке установите флажок **Автоматически разрешать распространение 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, запущенных с помощью доверенных пакетов установки. Список программ и пакетов для 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 установлен флажок **Использовать правила для исполняемых файлов** в параметрах задачи **Контроль запуска программ**.
5. Если требуется, снимите флажок **Всегда разрешать распространение программ с помощью установщика Windows**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью установщика Windows.

   Если флажок установлен, программа всегда разрешает запуск файлов, установленных с помощью установщика Windows.

   Если флажок снят, использование установщика Windows для запуска программы не является критерием для разрешения такой программы.

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 установщика Windows** рекомендуется снимать только в случае крайней необходимости. Отключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также блокированию запуска файлов, извлеченных из пакета установки.

6. 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 2.2 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).

   Система контролирует запуск объектов со следующими расширениями:

   - exe;
   - msi.

   По умолчанию флажок снят.

Программа контролирует процесс распространения программного обеспечения от доставки пакета на компьютер до установки/обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки программы на компьютер.

7. Чтобы отредактировать список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в раскрывшемся меню выберите один из доступных способов:

   - **Добавить один вручную**.

     a. Нажмите на кнопку **Обзор** и выберите исполняемый файл или пакет установки.

        Блок **Критерии доверенности** автоматически заполнится данными о выбранном файле.

     b. Снимите или установите флажок **Разрешить запуск всех 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.**

          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.

- **Использовать хеш SHA256**.

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается значение контрольной суммы файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанным значением контрольной суммы.

  Этот вариант рекомендован для случаев, когда формирование правил обязательно для обеспечения соответствия максимальному уровню безопасности: в качестве уникального идентификатора файла может использоваться контрольная сумма SHA256. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.

  Данный вариант выбран по умолчанию.

- **Добавить несколько по хешу**.

  Вы можете выбрать неограниченное число исполняемых файлов и пакетов установки и добавить их в список одновременно. Kaspersky Embedded Systems Security 2.2 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 сохраненного конфигурационного файла. Для распознавания в Kaspersky Embedded Systems Security 2.2 файл должен удовлетворять следующим параметрам:

  - иметь текстовое расширение;
  - 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.

8. 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.

9. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены.

# Переход в режим разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и имеют доверенный статус в KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить режим только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило разрешения по умолчанию, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Контроль активности на компьютерах** нажмите на кнопку **Настройка** в блоке **Контроль запуска программ**.
4. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля запуска программ**.
5. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите **Добавить одно правило**.

   Откроется окно **Параметры правила**.
6. В поле **Название** введите название правила.
7. В раскрывающемся списке **Тип** выберите вариант **Разрешающее**.
8. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов программ.
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
9. В блоке **Критерий срабатывания правила** выберите **Путь к файлу**.
10. Введите следующую маску: **?:**
11. В окне **Параметры правила** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security 2.2 применяет режим разрешения по умолчанию.

# О формировании правил контроля запуска программ для всей сети через Kaspersky Security Center

Вы можете создать списки правил контроля запуска программ с помощью задач и политик Kaspersky Security Center сразу для всех компьютеров и групп компьютеров в сети организации. Этот вариант рекомендуется, если в сети организации нет эталонной машины и вы не можете сформировать общий список правил с помощью задачи автоматического формирования разрешающих правил по программам, установленным на такой эталонной машине.

По умолчанию компонент Контроль запуска программ устанавливается с двумя разрешающими правилами:

- Разрешающие правила для скриптов и MSI, имеющих доверенный сертификат в операционной системе.
- Разрешающие правила исполняемых файлов, имеющих доверенный сертификат 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.

  При использовании 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. Далее вы можете вручную импортировать сформированные списки правил в задачу Контроль запуска программ в политике Kaspersky Security Center. Вы также можете настроить автоматическое добавление созданных правил в список правил контроля запуска программ по завершении групповой задачи формирования правил контроля запуска программ.

  Рекомендуется использовать этот сценарий, если необходимо сформировать списки правил контроля запуска программ в короткие сроки. Запуск задачи Формирование правил контроля запуска программ по расписанию рекомендуется настраивать только в том случае, если область применения разрешающих правил включает папки, содержащие заведомо безопасные файлы.

  > При применении политики контроля 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 автоматического формирования правил для контроля компьютеров на 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.

  При использовании этого сценария Kaspersky Embedded Systems Security 2.2 не блокирует запуски программ, но фиксирует все запуски и блокировки запусков программ на всех компьютерах сети за период работы задачи Контроль запуска программ в режиме **Только статистика** в разделе **События** Kaspersky Security Center. Затем Kaspersky Security Center создает на основе журнала выполнения задачи единый список событий блокирования программ.

  Необходимо настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнялись все возможные сценарии работы защищаемых компьютеров и групп компьютеров и хотя бы одна их перезагрузка. Далее при добавлении правил в задачу контроля запуска программ вы можете импортировать данные о запусках программ из сохраненного файла отчета о событиях Kaspersky Security Center (в формате TXT) и сформировать на основе этих данных разрешающие правила контроля запуска таких программ.

Рекомендуется использовать этот сценарий, если сеть организации включает большое количество компьютеров разных типов с различным набором установленных программ (см. раздел "Использование профиля при настройке задачи Контроль запуска программ в политике Kaspersky Security Center" на стр. 179).

- На основе событий о блокировании 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 выполнять обновление списка правил при изменении состава программ, установленных на компьютерах в сети (например, при установке обновлений или переустановке операционной системы). Рекомендуется формировать обновленный список правил с помощью задачи Формирование правил контроля запуска программ или политики Контроль запуска программ в режиме **Только статистика**, выполняемых на компьютерах тестовой группы администрирования. Тестовая группа администрирования включает компьютеры, необходимые для тестового запуска новых программ перед их установкой на компьютеры сети.

Перед тем как добавить разрешающие правила, выберите один из доступных режимов применения правил (см. раздел "Настройка параметров задачи Контроль запуска программ" на стр. 181). В списке правил политики Kaspersky Security Center отображаются только те правила, которые заданы в этой политике, вне зависимости от режима применения правил. В списке локальных правил отображаются все применяющиеся правила: и локальные, и добавленные через политику.

## В этом разделе



## Создание разрешающих правил из событий Kaspersky Security Center

► *Чтобы сформировать разрешающие правила для программ с помощью опции Создать разрешающие правила программ из событий Kaspersky Security Center в параметрах политики Контроль запуска программ, выполните следующие действия:*

1. В 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. В контекстном меню политики, параметры которой вы хотите настроить, выберите пункт **Свойства**.

   Откроется окно **Свойства: <Имя политики>**.
4. В разделе **Контроль активности на компьютерах** нажмите на кнопку **Настройка** в блоке **Контроль запуска программ**.

5. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля запуска программ**.

6. Нажмите кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Создать разрешающие правила программ из событий Kaspersky Security Center**.

7. Выберите принцип добавления правил к списку уже заданных правил контроля запуска программ:

   - **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 окно **Формирование правил контроля запуска программ**.

8. Настройте следующие параметры запроса:

   - **Адрес Сервера администрирования**
   - **Порт**
   - **Пользователь**
   - **Пароль**

9. Выберите типы событий, которые должны стать основой для задачи формирования:

   - **Режим Только статистика: запуск программы запрещен**.
   - **Запуск программы запрещен**.

10. Выберите период из раскрывающегося списка **Запрашивать события, созданные в течение периода**.

11. Нажмите на кнопку **Создать правила**.

12. Нажмите кнопку **Сохранить** в окне **Правила контроля запуска программ**.

    Список правил в политике 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 2.2 добавит выбранные правила из событий блокирования к уже заданным правилам. Правила с повторяющимся хешем не добавляются, так как все правила в списке должны быть уникальными.

## Импорт правил контроля запуска программ из файла формата XML

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 автоматического формирования разрешающих правил программа экспортирует созданные разрешающие правила в файлы формата XML в указанную общую сетевую папку.

Каждый файл со списком правил создается на основе анализа запуска файлов и программ на каждом отдельном компьютере в сети организации. Списки содержат разрешающие правила для запуска файлов и программ, тип которых соответствует параметрам, указанным в групповой задачи автоматического формирования правил.

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.2 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в Консоли программы. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.2 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.2*.

► *Чтобы задать разрешающие правила запуска программ для группы компьютеров на основе автоматически сформированного списка разрешающих правил, выполните следующие действия:*

1. На закладке **Задачи** в панели управления настраиваемой группы компьютеров создайте групповую задачу Формирование правил контроля запуска программ или выберите созданную ранее задачу.
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. Также вы можете изменять состав папок, запуск программ из которых будет разрешен: исключать из области действия задачи папки, указанные по умолчанию, и добавлять новые папки вручную.
   - В блоке **Параметры** укажите действия задачи во время ее выполнения и по ее завершении. Укажите критерий, на основе которого будут сформированы правила, 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 2.2 не будет создавать разрешающие правила по программам, запускаемым 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.

   По завершении задачи автоматически сформированные списки разрешающих правил будут сохранены в указанной общей сетевой папке в файлах формата XML.

При применении политики контроля 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 автоматического формирования правил для контроля компьютеров на тестовой группе компьютеров или на эталонной машине.

4. Добавьте сформированные списки разрешающих правил в задачу Контроль запуска программ. Для этого в свойствах настраиваемой 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 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 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.

   d. В открывшемся стандартном окне Windows выберите файлы формата XML, 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 свойствах политики Контроль запуска программ выберите режим выполнения задачи **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.

## Импорт правил из файла отчета Kaspersky Security Center о заблокированных запусках программ

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 отследить, запуск каких программ будет блокироваться.

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 запуска программ для группы компьютеров на основе отчета о заблокированных программах из Kaspersky Security Center, выполните следующие действия:*

1. В свойствах политики в параметрах задачи Контроль запуска программ установите режим работы **Только статистика**.
2. В свойствах политики в разделе **Настройка событий** убедитесь, что:
   - На закладке **Критические события** для события Запуск программы запрещен установлено время хранения события, превышающее планируемое время работы задачи в режиме **Только статистика** (значение по умолчанию: 30 дней).
   - На закладке **Предупреждение** для события *Только статистика: запуск программы запрещен* установлено время хранения события, превышающее планируемое время работы задачи в режиме **Только статистика** (значение по умолчанию: 30 дней).

   По завершении периода, указанного в графе **Время хранения**, информация о регистрируемых 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 установленное время хранения указанных событий.
3. По завершении задачи экспортируйте зарегистрированные события в файл формата TXT.
   a. Для этого в свойствах задачи Контроль запуска программ разверните узел **Журналы и уведомления**.
   b. Во вложенном узле **События** создайте выборку событий по характеристике *Запрещен*, чтобы просмотреть, запуск каких программ будет блокироваться задачей контроля запуска программ.
   c. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных устройствах в файл формата TXT.

   Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех программах, запуск которых вы хотите разрешить.
4. 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 уже заданных правил контроля запуска программ:
      - **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.

d. В открывшемся стандартном окне 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.

# Управление подключением устройств из Kaspersky Security Center

Вы можете разрешать или запрещать подключение флеш-накопителей и других запоминающих устройств ко всем компьютерам в сети, формируя единые списки контроля компьютеров для групп компьютеров на стороне Kaspersky Security Center.

## В этом разделе



## О задаче Контроль устройств

Kaspersky Embedded Systems Security 2.2 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-подключаемыми флеш-накопителями или внешним устройством другого типа. Запоминающее устройство – это подключаемое к компьютеру внешнее устройство, предназначенное для записи и хранения данных.

Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 внешнему устройству один из двух статусов:

- *Доверенное*. Устройство, обмен данными с которым разрешен. Путь к экземпляру такого устройства подпадает под область применения хотя бы одного разрешающего правила.
- *Недоверенное*. Устройство, обмен данными с которым запрещен. Путь к экземпляру такого устройства не подпадает под область определения 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 2.2 идентифицирует регистрируемое в системе внешнее 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 2.2 в момент создания разрешающих правил автоматически.

Задача Контроль устройств может выполняться в одном из двух режимов:

- **Активный**. Kaspersky Embedded Systems Security 2.2 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 ином случае принцип блокирования по умолчанию не будет применен к устройству.

- **Только статистика**. Kaspersky Embedded Systems Security 2.2 не контролирует подключение флеш-накопителей и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях 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, зарегистрированной во время выполнения задачи.

# О формировании правил контроля устройств для всей сети через 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 2.2 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 списки правил в свойства политики Контроль устройств. В отличие от задачи на локальном компьютере, в политике вы не можете настроить автоматическое добавление созданных правил в список правил контроля устройств по завершении групповой задачи автоматического генерации разрешающих правил.

  Рекомендуется использовать этот сценарий для формирования списка разрешающих правил перед первым запуском политики Контроль устройств в режиме активного применения правил.

  > При применении политики контроля устройств 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 автоматического формирования правил для контроля компьютеров на тестовой группе компьютеров или на эталонной машине.

- 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 2.2 не блокирует подключения запоминающих устройств, но фиксирует в разделе **События** Kaspersky Security Center все попытки подключения и регистрации запоминающих устройств на всех компьютерах сети за период работы задачи Контроль устройств в режиме **Только статистика**. Затем Kaspersky Security Center создает на основе журнала выполнения задачи единый список событий блокирования и подключения 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, если необходимо добавить разрешающие правила для большого количества новых запоминающих устройств, а также для создания разрешающих правил для доверенных мобильных устройств, подключаемых по протоколу MTP.

- На основе реестра системы о подключавшихся запоминающих устройствах (с помощью опции Сформировать правила на основе данных системы в параметрах политики Контроль устройств).

  При использовании этого сценария Kaspersky Embedded Systems Security 2.2 формирует разрешающие правила для устройств, подключавшихся ранее или подключенных в текущий момент

к компьютеру, на котором установлена Консоль администрирования 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 опции **Сформировать правила для подключенных устройств**).

  При использовании этого сценария Kaspersky Embedded Systems Security 2.2 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 2.2 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 контроля устройств, основанных на применении данных системы о всех устройствах.

## Создание правил на основе данных системы о внешних устройствах, подключавшихся к компьютерам сети

Вы можете создавать правила (см. раздел "О формировании правил контроля устройств для всей сети через Kaspersky Security Center" на стр. 200) 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, если хотите, чтобы при формировании разрешающих правил учитывались данные о всех когда-либо подключавшихся запоминающих устройствах, сохранившиеся в системах на всех компьютерах сети.
- С помощью варианта **Создать правила на основе данных системы** в параметрах политики Контроль устройств. Используйте этот способ, если хотите, чтобы при формировании разрешающих правил учитывались данные о всех когда-либо подключавшихся запоминающих устройствах, сохранившиеся в системе компьютера с установленной Консолью администрирования Kaspersky Security Center.
- С помощью варианта **Сформировать правила для подключенных устройств** в параметрах политики Контроль устройств и 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 2.2 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 контроля устройств, основанных на применении данных системы о всех устройствах.

## В этом разделе



## 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. На закладке **Задачи** панели управления настраиваемой группы компьютеров создайте групповую задачу Формирование правил контроля устройств или выберите созданную ранее задачу.
2. В свойствах созданной групповой задачи Формирование правил контроля запуска программ или в мастере создания задачи настройте следующие параметры:
   - В разделе **Уведомления** настройте параметры сохранения отчета выполнения задачи.
   - В разделе **Параметры** укажите действия задачи по ее завершении. Укажите имя файла, в который будут экспортированы созданные правила.
   - В разделе **Расписание** настройте параметры запуска задачи по расписанию.
3. На закладке **Задачи** панели управления настраиваемой группы компьютеров в списке групповых задач выберите созданную задачу Формирование правил контроля устройств и нажмите на кнопку **Запустить** для запуска задачи.

   По завершении задачи автоматически сформированные списки разрешающих правил будут сохранены в указанной общей сетевой папке 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 папки общего доступа не предусмотрено политикой организации, рекомендуется запустить задачу автоматического формирования правил для контроля компьютеров на тестовой группе компьютеров или на эталонной машине.

4. Добавьте сформированные списки разрешающих правил в задачу контроля устройств. Для этого в свойствах настраиваемой политики в параметрах задачи Контроль устройств выполните следующие действия:
   a. На закладке **Общие** нажмите на кнопку **Список правил**.

      Откроется окно **Правила контроля устройств**.

   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 устройств:
      - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих. 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.

d. В открывшемся стандартном окне Windows выберите файлы формата XML, созданные по завершении групповой задачи Формирование правил контроля устройств.

e. Нажмите на кнопку **ОК** в окне Правила контроля устройств и в окне **Параметры задачи**.

5. Если вы хотите применять созданные правила контроля устройств, в свойствах политики **Контроль 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.

## Формирование разрешающих правил на основе данных системы в политике Kaspersky Security Center

► *Чтобы задать разрешающие правила с помощью опции **Создать правила на основе данных системы** в параметрах политики 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. В Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
3. Разверните группу администрирования, параметры политики которой вы хотите настроить и выберите в панели результатов закладку **Политики**.
4. В контекстном меню политики, параметры которой вы хотите настроить, выберите пункт **Свойства**.
5. Откроется окно **Свойства: <Имя политики>**.
6. В свойствах политики откройте окно настройки параметров задачи Контроль устройств и выполните следующие действия:

   a. На закладке **Общие** нажмите на кнопку **Список правил**.

      Откроется окно **Правила контроля устройств**.

   b. Нажмите кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Создать правила на основе данных системы**.

   c. Выберите принцип добавления правил к списку уже заданных правил контроля устройств:

      - **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.

7. Нажмите на кнопку **ОК** в окне **Правила контроля устройств** и в окне **Параметры задачи**.

Список правил в политике Контроль устройств будет дополнен новыми правилами, сформированными на основе данных системы компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

### Формирование правил для подключенных устройств

► *Чтобы задать разрешающие правила с помощью опции **Создать правила на основе данных системы** в параметрах политики Контроль устройств, выполните следующие действия:*

1. В 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. В контекстном меню политики, параметры которой вы хотите настроить, выберите пункт **Свойства**.
4. Откроется окно **Свойства: <Имя политики>**.
5. В разделе **Контроль активности на компьютерах** нажмите на кнопку **Настройка** в блоке **Контроль устройств**.
6. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля устройств**.
7. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила для подключенных устройств**.

   Откроется окно **Сформировать правила на основе данных системы**.
8. В списке обнаруженных устройств, подключенных к защищаемому компьютеру, выберите устройства, для которых требуется сформировать разрешающие правила.
9. Нажмите на кнопку **Добавить правила для выбранных устройств**.
10. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в политике Контроль устройств будет дополнен новыми правилами, сформированными на основе данных системы компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

## Импорт правил из файла отчета Kaspersky Security Center о заблокированных устройствах

Вы можете импортировать данные о заблокированных запоминающих устройствах из отчета, сформированного в Kaspersky Security Center по результатам выполнения задачи Контроль устройств в режиме **Только статистика**, 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.

При импорте из отчета данных о заблокированных устройствах в настройки политики убедитесь, что применяемый список содержит только те устройства, подключение которых вы хотите разрешить.

► *Чтобы задать разрешающие правила подключения устройств для группы компьютеров на основе отчета из Kaspersky Security Center о заблокированных устройствах, выполните следующие действия:*

1. В свойствах политики в параметрах задачи Контроль устройств установите режим работы **Только статистика**.
2. В свойствах политики в разделе **Настройка событий** убедитесь, что:
   - На закладке **Критическое событие** для события *Запоминающее устройство запрещено* установлено время хранения события, превышающее планируемое время работы задачи в режиме **Только статистика** (значение по умолчанию: 30 дней).
   - На закладке **Предупреждение** для события *Только статистика: обнаружено недоверенное запоминающее устройство* установлено время хранения события, превышающее планируемое время работы задачи в режиме **Только статистика** (значение по умолчанию: 30 дней).

     По завершении периода, указанного в графе **Время хранения**, информация о регистрируемых 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.
3. По завершении задачи экспортируйте зарегистрированные события в файл формата TXT. Для этого разверните узел **Журналы и уведомления** и во вложенном узле **События** создайте выборку событий по характеристике *Запрещено*, чтобы просмотреть, подключение каких устройств будет блокироваться задачей контроля устройств. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных устройствах 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.
4. Импортируйте данные о заблокированных попытках подключения устройств в политику контроля устройств. Для этого в свойствах политики в параметрах задачи Контроль устройств выполните следующие действия:
   a. На закладке **Общие** нажмите на кнопку **Список правил**.

      Откроется окно **Правила контроля устройств**.
   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать данные о заблокированных устройствах из отчета Kaspersky Security Center**.
   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 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.

d. В открывшемся стандартном окне Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных устройствах.

e. Нажмите на кнопку **ОК** в окне **Правила контроля устройств** и в окне **Параметры задачи**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных устройствах, будут добавлены к списку правил в политике контроля устройств.

# Контроль активности в сети

Этот раздел содержит информацию о задаче Управление сетевым экраном.

## 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 2.2 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 2.2. В ходе выполнения задачи Управление сетевым экраном Kaspersky Embedded Systems Security 2.2 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 2.2.

Если при установке Kaspersky Embedded Systems Security 2.2 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 2.2 обнаруживает несовпадение параметров сетевого экрана Windows и параметров задачи Управление сетевым экраном, программа форсированно передает параметры задачи сетевому экрану операционной системы.

При ежеминутном опросе сетевого экрана Windows Kaspersky Embedded Systems Security 2.2 контролирует следующие статусы:

- статус работы сетевого экрана Windows;
- статус правил, добавленных после установки Kaspersky Embedded Systems Security 2.2 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 2.2 создает группу правил Kaspersky Security Group в оснастке **Брандмауэр Windows**. Эта группа объединяет все правила, созданные на стороне Kaspersky Embedded Systems Security 2.2 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 2.2.

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 форсировано сообщаются сетевому экрану Windows при выполнении задачи.

При первом запуске задачи Kaspersky Embedded Systems Security 2.2 считывает и копирует все разрешающие правила для входящего трафика, заданные в параметрах сетевого экрана Windows, в параметры задачи Управление сетевым экраном. При дальнейшей работе программа действует в соответствии со следующими алгоритмами:

- если в параметрах сетевого экрана Windows создается новое правило (вручную или автоматически при установке новой программы), Kaspersky Embedded Systems Security 2.2 удаляет такое правило;
- если в параметрах сетевого экрана Windows удаляется существующее правило, Kaspersky Embedded Systems Security 2.2 восстанавливает такое правило;
- если в параметрах сетевого экрана Windows изменяются параметры существующего правила, Kaspersky Embedded Systems Security 2.2 отменяет изменения;

- если в параметрах задачи Управление сетевым экраном создается новое правило, Kaspersky Embedded Systems Security 2.2 форсированно передает это правило сетевому крану Windows;
- если в параметрах задачи Управление сетевым экраном удаляется существующее правило, Kaspersky Embedded Systems Security 2.2 форсированно удаляет такое правило в параметрах сетевого экрана Windows;

Kaspersky Embedded Systems Security 2.2 не работает с запрещающими правилами, а также с правилами, контролирующими исходящий трафик. В момент запуска задачи Управление сетевым экраном Kaspersky Embedded Systems Security 2.2 удаляет все правила этих типов в параметрах сетевого экрана 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 2.2, 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.

## Активация и выключение правил сетевого экрана

► *Чтобы активировать или выключить существующее правило фильтрации входящего трафика, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в блоке **Управление сетевым экраном**.
4. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.
5. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.
6. 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.
7. 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

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. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
2. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в блоке **Управление сетевым экраном**.
4. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.
5. 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**.
6. 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.

7. В окне **Настроить правило для приложения** или **Настроить правило для порта** нажмите на кнопку **ОК**.
8. 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 администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
2. 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. 91).
   - 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. 103).

> Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

3. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в блоке **Управление сетевым экраном**.
4. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.
5. В зависимости от типа правила, которое вы хотите удалить, выберите закладку **Приложения** или закладку **Порты**.
6. В списке правил выберите правило, которое вы хотите удалить.
7. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.
8. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи Управление сетевым экраном будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

# Диагностика системы

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

## В этом разделе



# 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 поля действия задачи, например, из-за приостановки выполнения задачи или физического отсутствия запоминающего устройства на защищаемом компьютере. Kaspersky Embedded Systems Security 2.2 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 Мониторинга файловых операций, требуется 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. 220). 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 2.2 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 2.2 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 2.2 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 2.2 не может получить данные о пользователе вследствие прерывания задачи или сбоя драйвера синхронизации данных или USN-журнала. Если Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см.таблицу ниже).

*Таблица 36. 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 |

| ID файловой операции | Маркер файловой операции | Поддерживаемые файловые системы |
|---|---|---|
| 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 |
| 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 |

## Настройка параметров задачи Мониторинг файловых операций

Вы можете изменять параметры задачи Мониторинг файловых операций, заданные по умолчанию (см.таблицу ниже).

*Таблица 37. Параметры задачи Мониторинг файловых операций по умолчанию*

| 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/или группы пользователей, действия которых в указанных каталогах 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. |
| **Учитывать исключенную область мониторинга** | 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 2.2 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 для характеристики файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Embedded Systems Security 2.2 формирует событие аудита. |
| Расписание запуска задачи | Первый запуск не определен | Вы можете настроить параметры запуска задачи по расписанию. |

► *Чтобы настроить параметры задачи Мониторинг файловых операций, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Диагностика системы** в блоке **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг файловых операций**.
4. В открывшемся окне на закладке **Параметры мониторинга файловых операций** настройте параметры области мониторинга:
   a. Снимите или установите флажок **Фиксировать события 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 2.2 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. 220), которые будет контролировать задача.
5. На закладке **Управление задачей** запустите задачу на базе расписания (см. раздел "Работа с расписанием задач" на стр. 123).
6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

## Настройка правил мониторинга

По умолчанию область мониторинга не задана; задача не контролирует выполнение файловых операций ни в одной директории.

► *Чтобы добавить область мониторинга, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Диагностика системы** в блоке **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

   Откроется окно **Свойства: Мониторинг файловых операций**.
4. В блоке **Область мониторинга** нажмите на кнопку **Добавить**.

   Откроется окно **Область мониторинга**.
5. 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> вне зависимости от их расположения;
     - <*\name.ext> - все файлы с именем name и расширением <ext> вне зависимости от их расположения;
     - <\dir*> - все файлы в директории <\dir>;
     - <\dir*\name.ext> - все файлы с именем name и расширением <ext> в директории <\dir> и всех ее поддиректориях.

   При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Embedded Systems Security 2.2 не добавит указанную область мониторинга.

6. На закладке **Доверенные пользователи**, нажмите на кнопку **Добавить**.

   Откроется стандартное окно Microsoft Windows **Выбор: "Пользователи" или "Группы"**.

7. 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 2.2 считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 215), и формирует для них события с уровнем важности Критический.

8. Выберите закладку **Маркеры файловых операций**.

9. 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. 215) установите флажки напротив тех операций, которые вы хотите контролировать.

   По умолчанию Kaspersky Embedded Systems Security 2.2 контролирует все доступные файловые операции, выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

10. Если вы хотите, чтобы программа Kaspersky Embedded Systems Security 2.2 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 2.2 рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

       Если файловая операция обнаруживается сразу по нескольким маркерам, рассчитывается только финальная контрольная сумма файла после всех последовательных изменений.

       Если флажок снят, Kaspersky Embedded Systems Security 2.2 не рассчитывает контрольную сумму измененных файлов.

       Программа не выполняет расчет контрольной суммы в следующих случаях:

       - если в результате файловой операции файл стал недоступен (например, изменены права 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 вариантов:

       - **Хеш MD5**
       - **Хеш SHA256**

11. Если вы хотите контролировать не все файловые операции, в списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 215) установите флажки напротив тех операций, которые вы хотите контролировать.
12. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:
    a. Выберите закладку **Исключения**.
    b. Установите флажок **Учитывать исключенные области мониторинга**.

       Флажок включает или 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 2.2 будет пропускать области мониторинга, заданные в списке исключений.

       Если флажок снят, Kaspersky Embedded Systems Security 2.2 будет фиксировать 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.
13. В окне **Область мониторинга** нажмите на кнопку **ОК**.

    Указанные параметры правил будут применяться к выбранной области мониторинга задачи Мониторинг файловых операций.

# 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 2.2 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 2.2 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 данных 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 2.2 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 2.2 фиксирует событие с уровнем важности Критическое событие в журнале выполнения задачи Анализ журналов.

По умолчанию задача Анализ журналов не учитывает 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.

## Настройка стандартных правил задачи

► *Чтобы настроить параметры стандартных правил для задачи Анализ журналов, 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. 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. 91).
   - 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. 103).

     Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Мониторинг целостности системы** в блоке **Анализ журналов** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры анализа журналов**.
4. Перейдите на закладку **Стандартные правила**.
5. Снимите или установите флажок **Использовать стандартные правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security 2.2 применяет эвристический анализатор для обнаружения аномальной активности на защищаемом компьютере.

   Если этот флажок не установлен, то эвристический анализатор выключен, Kaspersky Embedded Systems Security 2.2 использует стандартные или пользовательские правила для обнаружения аномальной активности.

   По умолчанию флажок установлен.

   Для работы 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, нажмите на кнопку **Дополнительные параметры**.

   Откроется окно **Анализ журналов**.

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 атипичной аутентификации** укажите начало и конец временного интервала, при выполнении попытки входа в который Kaspersky Embedded Systems Security 2.2 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 **ОК**.

       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**.
13. Указанный IP-адрес добавится в список доверенных.
14. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 124).
15. Нажмите на кнопку **ОК**.

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 администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
2. 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. 91).
   - 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. 103).

   Если устройство работает под управлением активной политики Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
3. В разделе **Мониторинг целостности системы** в блоке **Анализ журналов** нажмите на кнопку **Настройка**.

   Откроется окно **Анализ журналов**.
4. На закладке **Правила анализа журналов** снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security 2.2 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, вы не можете добавлять или изменять пользовательские правила. Kaspersky Embedded Systems Security 2.2 применяет параметры правил по умолчанию.

   По умолчанию флажок установлен. Активно только правило Обнаружено всплывающее окно приложения.

   Вы можете контролировать применение стандартных правил в списке правил. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.
5. Чтобы добавить новое пользовательское правило, нажмите на кнопку **Добавить**.

   Откроется окно **Правило анализатора журналов**.

6. В блоке **Общие** введите следующие данные нового правила:
   - **Название**
   - **Источник**

     Выберите журнал, события которого будут использоваться для анализа. Для выбора доступны следующие виды журналов событий Windows:

     - Программа;
     - Безопасность;
     - Система.

     Вы можете добавить новый пользовательский журнал, указав имя журнала в поле **Источник**.
7. 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.

# Отчеты 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 2.2 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. 103).
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 (см. раздел "Управление запуском программ из Kaspersky Security Center" на стр. 179) можно сформировать два типа отчетов: отчет о запрещенных программах (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 серверах 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. 181).
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. 181).
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 Kaspersky Embedded Systems Security 2.2 из командной строки

Этот раздел содержит описание работы с Kaspersky Embedded Systems Security 2.2 из командной строки.

## В этом разделе



## Команды командной строки

Вы можете выполнять основные команды управления Kaspersky Embedded Systems Security 2.2 из командной строки защищаемого компьютера, если при установке Kaspersky Embedded Systems Security 2.2 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 2.2.

Некоторые из команд Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 (см. таблицу ниже).

Таблица 38. Документация Kaspersky Embedded Systems Security 2.2

| Команда | Описание |
|---|---|
| KAVSHELL APPCONTROL (см. раздел "Наполнение списка правил контроля запуска программ из файла. KAVSHELL APPCONTROL" на стр. 244). | 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. 241). | Управляет режимами работы задачи Контроль запуска программ. |
| KAVSHELL APPCONTROL /GENERATE (см. раздел "Формирование правил контроля запуска программ. KAVSHELL APPCONTROL /GENERATE" на стр. 242). | Запускает задачу автоматического формирования разрешающих правил контроля запуска программ. |
| KAVSHELL VACUUM (см. раздел "Дефрагментация файлов журнала событий Kaspersky Embedded Systems Security 2.2.KAVSHELL VACUUM" на стр. 253). | Дефрагментирует файлы журнала выполнения Kaspersky Embedded Systems Security 2.2. |
| KAVSHELL PASSWORD | Управляет параметрами защиты паролем. |
| KAVSHELL HELP (см. раздел "Вызов справки о командах Kaspersky Embedded Systems Security 2.2.KAVSHELL HELP" на стр. 233). | Вызывает справку о командах Kaspersky Embedded Systems Security 2.2. |
| KAVSHELL START (см. раздел "Запуск и остановка службы Kaspersky Security. KAVSHELL START, KAVSHELL STOP" на стр. 234) | Запускает службу Kaspersky Embedded Systems Security 2.2. |
| KAVSHELL STOP (см. раздел "Запуск и остановка службы Kaspersky Security. KAVSHELL START, KAVSHELL STOP" на стр. 234). | Останавливает службу Kaspersky Embedded Systems Security 2.2. |
| KAVSHELL SCAN (см. раздел "Проверка выбранной области.KAVSHELL SCAN" на стр. 234). | Создает и запускает временную задачу проверки по требованию с областью проверки и параметрами безопасности, заданными ключами команды. |
| KAVSHELL SCANCRITICAL (см. раздел "Запуск задачи Проверка важных областей.KAVSHELL SCANCRITICAL" на стр. 238). | Запускает системную задачу Проверка важных областей. |
| KAVSHELL TASK (см. раздел "Управление указанной задачей в асинхронном режиме.KAVSHELL TASK" на стр. 239). | 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 файлов.KAVSHELL RTP" на стр. 240). | Запускает или останавливает все задачи постоянной защиты. |

| Команда | Описание |
|---|---|
| KAVSHELL VACUUM (см. раздел "Запуск задачи Обновление баз Kaspersky Embedded Systems Security 2.2.KAVSHELL UPDATE" на стр. 246). | Запускает задачу обновления баз Kaspersky Embedded Systems Security 2.2 с параметрами, указанными с помощью ключей команды. |
| KAVSHELL ROLLBACK (см. раздел "Откат обновления баз Kaspersky Embedded Systems Security 2.2.KAVSHELL ROLLBACK" на стр. 249). | Откатывает базы до предыдущей версии. |
| KAVSHELL LICENSE (см. раздел "Активация программы KAVSHELL LICENSE" на стр. 250). | Управление ключами. |
| KAVSHELL TRACE (см. раздел "Включение, настройка и выключение журнала трассировки.KAVSHELL TRACE" на стр. 251). | Включает или выключает запись журнала трассировки, управляет параметрами журнала трассировки. |
| KAVSHELL DUMP (см. раздел "Включение и выключение файла дампа.KAVSHELL DUMP" на стр. 254). | Включает или выключает создание файлов дампов памяти процессов Kaspersky Embedded Systems Security 2.2 при аварийном завершении процессов. |
| KAVSHELL IMPORT (см. раздел "Импорт параметров.KAVSHELL IMPORT" на стр. 255). | Импортирует общие параметры Kaspersky Embedded Systems Security 2.2, параметры его функций и задач из предварительно созданного конфигурационного файла. |
| KAVSHELL EXPORT (см. раздел "Экспорт параметров.KAVSHELL EXPORT" на стр. 256). | Экспортирует все параметры Kaspersky Embedded Systems Security 2.2 и существующих задач в конфигурационный файл. |
| KAVSHELL DEVCONTROL (см. раздел "Наполнение списка правил контроля устройств.KAVSHELL DEVCONTROL" на стр. 245). | Дополняет список сформированных правил контроля устройств в соответствии с выбранным принципом добавления. |

## Отображение справки о командах Kaspersky Embedded Systems Security 2.2. KAVSHELL HELP

Чтобы получить список всех команд Kaspersky Embedded Systems Security 2.2, 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. 239).

### 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>]
```

В состав команды KAVSHELL SCAN входят как обязательные, так и дополнительные ключи, использование которых не является обязательным (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 39. Ключи команды KAVSHELL SCAN*

| Ключ | Описание |
|---|---|
| **Область проверки**. Обязательный ключ. | |
| <файлы><br><папки><br><сетевой путь> | Область проверки – список файлов, папок, сетевых путей и стандартных областей.<br>Указывайте сетевые пути в формате UNC (Universal Naming Convention).<br>В следующем примере папка Folder4 указана без пути к ней – она находится в папке, из которой вы запускаете команду KAVSHELL:<br>KAVSHELL SCAN Folder4<br>Если имя объекта, который вы хотите проверить, содержит пробелы, требуется заключить его в кавычки.<br>Если вы выбрали папку, то Kaspersky Embedded Systems Security 2.2 проверит также все вложенные подпапки для данной папки.<br>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. |

| Ключ | Описание |
|---|---|
| /L: <имя файла со списком областей проверки> | Имя файла со списком областей проверки, включая полный путь к файлу.<br>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:<br>C:\<br>D:\Docs*.doc<br>E:\My Documents<br>/STARTUP<br>/SHARED |
| **Проверяемые объекты** (File types). Если вы не укажете никаких значений этого ключа, Kaspersky Embedded Systems Security 2.2 будет проверять объекты по формату. | |
| /FA | Проверять все объекты |
| /FC | Проверять объекты по формату (по умолчанию). Kaspersky Embedded Systems Security 2.2 проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам. |
| /FE | Проверять объекты по расширению. Kaspersky Embedded Systems Security 2.2 проверяет только объекты с расширениями, которые входят в список расширений, свойственных заражаемым объектам. |
| /NEWONLY | Проверять только новые и измененные файлы.<br>Если вы не укажете этот ключ, Kaspersky Embedded Systems Security 2.2 будет проверять все объекты. |
| /AI: **Действия над зараженными и другими обнаруженными объектами**. Если вы не зададите никаких значений этого ключа, Kaspersky Embedded Systems Security 2.2 будет выполнять действие **Пропускать**. | |
| DISINFECT | Лечить, если невозможно, пропускать. |
| DISINFDEL | Лечить, если невозможно, удалять. |
| DELETE | Удалять<br>Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Embedded Systems Security 2.2 для обеспечения совместимости с предыдущими версиями. Вы можете использовать эти параметры вместо ключей команд /AI: и /AS: В этом случае Kaspersky Embedded Systems Security 2.2 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 2.2 выполнит действие **Пропускать**. | |
| QUARANTINE | Карантин |
| DELETE | Удалять |
| REPORT | Отсылать отчет (по умолчанию) |
| AUTO | Выполнять рекомендованное действие |

| Ключ | Описание |
|---|---|
| **Исключения** | |
| /E:ABMSPO | Ключ исключает составные объекты следующих типов:<br>A – SFX-архивы;<br>B – почтовые базы;<br>M – файлы почтовых форматов;<br>S – архивы (включая SFX-архивы);<br>P – упакованные объекты;<br>O – вложенные OLE-объекты. |
| /EM:<"маски"> | Исключать файлы по маске<br>Можно указать несколько масок, например: EM:″*.txt; *.png; C\Videos*.avi″. |
| /ET:<количество секунд> | Прекращать обработку объекта, если она продолжается дольше указанного количества секунд.<br>По умолчанию ограничений в продолжительности проверки нет. |
| /ES:<размер> | Исключать из проверки составные объекты, размер которых в мегабайтах превышает указанный значением <размер>.<br>По умолчанию Kaspersky Embedded Systems Security 2.2 проверяет объекты любого размера. |
| /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.<br>Доступны следующие уровни эвристического анализа:<br>1 – поверхностный;<br>2 – средний;<br>3 – глубокий.<br>Если вы опустите этот ключ, Kaspersky Embedded Systems Security 2.2 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 2.2.<br>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) | |

| Ключ | Описание |
|---|---|
| /W:<имя файла журнала выполнения задачи> | Если вы укажете этот ключ, Kaspersky Embedded Systems Security 2.2 сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа.<br>Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней.<br>В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий Kaspersky Embedded Systems Security 2.2 в консоли "Просмотр событий".<br>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.<br>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.<br>Вы можете просматривать файл журнала во время выполнения задачи.<br>Журнал отображается в узле Журналы выполнения задач Консоли программы.<br>Если Kaspersky Embedded Systems Security 2.2 не удается создать файл журнала, он не прерывает выполнение команды, но выдает сообщение об ошибке. |
| /ANSI | Ключ позволяет записывать события в журнал выполнения задач в кодировке ANSI.<br>Ключ ANSI не будет применяться, если не задан ключ W.<br>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 40. Синтаксис ключа /W команды KAVSHELL SCANCRITICAL*

| Ключ | Описание |
|---|---|

| Ключ | Описание |
|---|---|
| /W:<имя файла журнала выполнения задачи> | Если вы укажете этот ключ, Kaspersky Embedded Systems Security 2.2 сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа.<br>Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней.<br>В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий програмы в консоли "Просмотр событий".<br>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.<br>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.<br>Вы можете просматривать файл журнала во время выполнения задачи.<br>Журнал отображается в узле **Журналы выполнения задач** Консоли программы.<br>Если Kaspersky Embedded Systems Security 2.2 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 41. Ключи команды KAVSHELL TASK*

| Ключ | Описание |
|---|---|
| Без ключей | Команда возвращает список всех существующих задач Kaspersky Embedded Systems Security 2.2. 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 2.2 присваивает задачам. Чтобы просмотреть альтернативные названия задач Kaspersky Embedded Systems Security 2.2, 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. |

Коды возврата команды KAVSHELL TASK (см. раздел "Коды возврата команды KAVSHELL TASK" на стр. 258).

## 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 42. Ключи команды KAVSHELL RTP*

| Ключ | Описание |
|---|---|

| 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 43. Ключи команды `KAVSHELL APPCONTROL /GENERATE`*

| Ключ | Описание |
|---|---|
| `/mode:<applyrules\|statistics>` | Режим работы задачи Контроль запуска программ.<br>Вы можете выбрать один из следующих режимов работы задачи:<br>• active - Активный;<br>• 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. |
| `/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 44. 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. |

| Ключ | Описание |
|---|---|
| /masks: <edms> | Расширения исполняемых файлов, для которых требуется создать разрешающие правила контроля запуска программ.<br>Вы можете включить в область срабатывания создаваемых правил файлы следующих расширений:<br>• e - файлы с расширением exe;<br>• d - файлы с расширением dll;<br>• m - файлы с расширением msi;<br>• s - скрипты. |
| /runapp | Учитывать при формировании разрешающих правил программы, запущенные на защищаемом компьютере в момент выполнения задачи. |
| **Действия при автоматическом формировании правил** | |
| /rules: <ch\|cp\|h> | Указать действия, которые задача совершает во время формирования разрешающих правил контроля запуска программ:<br>• ch - использовать цифровой сертификат. Если сертификат отсутствует, использовать хеш SHA256.<br>• cp - использовать цифровой сертификат. Если сертификат отсутствует, использовать значение пути к исполняемому файлу.<br>• h - использовать хеш SHA256. |
| /strong | Использовать заголовок и отпечаток цифрового сертификата при автоматическом формировании 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 автоматического формирования правил** | |
| /export: <путь к XML-файлу> | Сохранять сформированные правила в файл формата XML. |
| /unique | Добавлять информацию о компьютере, по программам которого формируются разрешающие правила контроля запуска программ. |
| /prefix: <префикс для названий правил> | Префикс для названий создаваемых 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: :<br>• a - **Добавлять к существующим правилам** (одинаковые правила дублируются);<br>• r - **Заменять существующие правила** (новые правила добавляются вместо заданных правил);<br>• m - **Объединять с существующими правилами** (добавляются новые правила, параметры которых не совпадают с параметрами уже заданных правил). |

# Заполнение списка правил задачи Контроль 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 45. 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 46. 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 2.2. KAVSHELL UPDATE

С помощью команды KAVSHELL UPDATE вы можете запускать задачу обновления баз Kaspersky Embedded Systems Security 2.2 в синхронном режиме.

Задача обновления баз Kaspersky Embedded Systems Security 2.2, 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 2.2 на компьютерах с помощью программы Kaspersky Security Center читайте в разделе "Управление Kaspersky Embedded Systems Security 2.2 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>]
```

В состав команды KAVSHELL UPDATE входят как обязательные, так и дополнительные ключи, использование которых не является обязательным (см. таблицу ниже).

## Примеры команды KAVSHELL UPDATE

- *Чтобы запустить пользовательскую задачу обновления баз, выполните следующую команду:*

```
KAVSHELL UPDATE
```

- *Чтобы запустить задачу обновления баз, 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 команду:*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

- *Чтобы загрузить обновления баз Kaspersky Embedded Systems Security 2.2 с сервера обновлений "Лаборатории Касперского", подключитесь к источнику обновлений через прокси-сервер (адрес прокси-сервера: proxy.company.com, порт: 8080). Для доступа к компьютеру с помощью встроенной проверки подлинности Microsoft Windows (NTLM authentication) 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 47. Ключи команды KAVSHELL UPDATE*

| Ключ | Описание |
|---|---|
| **Источники обновления** (обязательный ключ). Укажите один или несколько источников. Kaspersky Embedded Systems Security 2.2 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). |
| **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 2.2 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:<br>**0** – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Kaspersky Embedded Systems Security 2.2 будет обращаться к прокси-серверу под учетной записью **Локальная система** (**SYSTEM**);<br>**1** – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Kaspersky Embedded Systems Security 2.2 будет обращаться к прокси-серверу под учетной записью, данные которой описаны ключами /PROXYUSER и /PROXYPWD;<br>**2** – проверка подлинности по имени и паролю пользователя, заданным ключами /PROXYUSER и /PROXYPWD (Basic authentication).<br>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) |

| Ключ | Описание |
|---|---|
| /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 вы укажете этот ключ, Kaspersky Embedded Systems Security 2.2 будет использовать активный режим FTP-сервера для соединения с защищаемым компьютером. Если вы не укажете этот ключ, Kaspersky Embedded Systems Security 2.2 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 2.2 использует значение по умолчанию: 10 секунд. Значение ключа должно быть целым числом. |
| /REG:<код iso3166> | Региональные параметры. Ключ "Региональные используется при получении обновлений с серверов обновлений "Лаборатории Касперского". Kaspersky Embedded Systems Security 2.2 оптимизирует загрузку обновлений на защищаемый компьютер, выбирая ближайший к нему сервер обновлений.<br>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 2.2 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 2.2.<br>Если этот ключ не задан, задаче присваивается альтернативное имя update_<kavshell_pid>, например, update_1234. В Консоли программы задаче автоматически присваивается имя Обновление баз программы (<дата и время>), например: Обновление баз программы 16.08.2007 17:41:02. |

| Ключ | Описание |
|---|---|
| /W:<имя файла журнала выполнения задачи> | Если вы укажете этот ключ, Kaspersky Embedded Systems Security 2.2 сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа.<br>Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней.<br>В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий Kaspersky Embedded Systems Security 2.2 в консоли "Просмотр событий".<br>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.<br>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.<br>Вы можете просматривать файл журнала во время выполнения задачи.<br>Журнал отображается в узле **Журналы выполнения задач** Консоли программы.<br>Если Kaspersky Embedded Systems Security 2.2 не удается создать файл журнала, он не прерывает выполнение команды и не отображает сообщение об ошибке. |

Коды возврата команды KAVSHELL UPDATE (на стр. 259).

## Откат обновления баз Kaspersky Embedded Systems Security 2.2. KAVSHELL ROLLBACK

С помощью команды `KAVSHELL ROLLBACK` вы можете выполнить системную задачу Откат обновления баз – откатить базы Kaspersky Embedded Systems Security 2.2 до предыдущих установленных обновлений. Команда выполняется синхронно.

### Синтаксис команды

```
KAVSHELL ROLLBACK
```

Коды возврата команды KAVSHELL ROLLBACK (на стр. 260).

## 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 48. 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. 258).

## Активация программы KAVSHELL LICENSE

С помощью команды `KAVSHELL LICENSE` вы можете управлять ключами и кодами активации в Kaspersky Embedded Systems Security 2.2.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<password>]`.

### Синтаксис команды KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<файл ключа | код активации> [/R] | /DEL:<ключ | код активации>]
```

### Примеры команды KAVSHELL LICENSE

► *Чтобы активировать программу, выполните команду:*

```
KAVSHELL.EXE LICENSE / ADD: <код активации или файл ключа>
```

► *Чтобы получить информацию о добавленных ключах, выполните команду:*

```
KAVSHELL LICENSE
```

► *Чтобы удалить добавленный ключ с номером 0000-000000-00000001, выполните команду:*

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

Команда KAVSHELL LICENSE может быть выполнена как без ключей, так и с их использованием (см. таблицу ниже).

*Таблица 49. Ключи команды KAVSHELL LICENSE*

| Ключ | Описание |
|---|---|
| Без ключей | Команда возвращает следующую информацию о добавленных ключах:<br>• Ключ.<br>• Тип лицензии (коммерческая).<br>• Срок действия связанной с ключом лицензии.<br>• Статус ключа (активный или дополнительный). Если указано значение *, ключ добавлен в качестве дополнительного. |
| /ADD:<имя файла ключа или код активации> | Добавляет ключ с помощью указанного файла или кода активации.<br>Указывая путь к файлу ключа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения. |
| /R | Код активации или ключ /R является дополнительным к коду активации или ключу /ADD и указывает на то, что код активации или ключ добавляется в качестве дополнительного. |
| /DEL:<ключ или код активации> | Удаляет ключ с указанным номером или указанный код активации. |

Коды возврата команды KAVSHELL LICENSE (см. раздел "Коды возврата команды KAVSHELL LICENSE" на стр. 260).

# 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 2.2, а также устанавливать уровень детализации информации в журнале.

Kaspersky Embedded Systems Security 2.2 записывает информацию в файлы трассировки и файл дампа 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 журнал трассировки ведется и вы хотите изменить его параметры, введите команду `KAVSHELL TRACE` с ключом /ON и задайте параметры журнала значениями ключей /S и /LVL (см. таблицу ниже).

*Таблица 50. 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).<br>Если вы укажете путь к несуществующей папке, журнал трассировки не будет создан. Можно указать сетевые пути в формате UNC (Universal Naming Convention), но нельзя указать пути к папкам на сетевых дисках защищаемого компьютера.<br>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".<br>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 2.2 начнет записывать информацию в новый файл; предыдущий файл журнала сохранится.<br>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.<br>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. 261).

## Дефрагментация файлов журнала событий Kaspersky Embedded Systems Security 2.2. KAVSHELL VACUUM

С помощью команды KAVSHELL VACUUM вы можете провести дефрагментацию файлов журнала событий программы. Это позволяет избежать ошибок в работе системы или Kaspersky Embedded Systems Security 2.2, связанных с хранением большого количества файлов отчетов, сформированных по событиям работы 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 2.2 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 2.2\2.2\Reports. Если вы вручную указали другой путь для хранения файлов, команда KAVSHELL VACUUM выполняет дефрагментацию файлов в папке, указанной в параметрах журнала событий Kaspersky Embedded Systems Security 2.2.

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 2.2 и запрещает запись событий в журнал. Во избежание снижения уровня защиты рекомендуется заранее планировать выполнение команды KAVSHELL VACUUM в нерабочее время.

► *Чтобы выполнить дефрагментацию файлов журнала событий Kaspersky Embedded Systems Security 2.2, выполните команду:*

```
KAVSHELL VACUUM
```

Выполнение команды доступно при запуске с правами учетной записи локального администратора.

## Очищение базы iSwift. KAVSHELL FBRESET

Kaspersky Embedded Systems Security 2.2 использует технологию iSwift, позволяющую не проверять файл повторно, если с момента последней проверки он не был изменен (**Использовать технологию iSwift**).

Kaspersky Embedded Systems Security 2.2 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 2.2. В данном файле хранится только актуальная информация о существующих в системе файлах: если какой-либо файл удален, то Kaspersky Embedded Systems Security 2.2 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 2.2 не приостанавливает защиту (в отличие от удаления файла klamfb.dat вручную).
- После очистки файла klamfb.dat Kaspersky Embedded Systems Security 2.2 может увеличить нагрузку на компьютер. При этом после очистки файла klamfb.dat антивирусная программа проверяет все файлы, к которым обращается впервые. После проверки Kaspersky Embedded Systems Security 2.2 вновь заносит информацию о проверенных объектах в файл klamfb.dat. При повторном обращении к этому же объекту технология iSwift позволит не сканировать файл повторно, если он не был изменён.

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` вы можете включать или выключать создание образов памяти (файла дампа) процессов Kaspersky Embedded Systems Security 2.2 при их аварийном завершении (см. таблицу ниже). Кроме этого вы можете в любой момент снять образы памяти выполняющихся процессов Kaspersky Embedded Systems Security 2.2.

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>
```

### 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 /P:1234
```

► *Чтобы выключить создание файла дампа, выполните команду:*

```
KAVSHELL DUMP /OFF
```

*Таблица 51. 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. Если вы укажете путь к несуществующей папке, файл дампа не будет создан. Можно указать сетевые пути в формате UNC (Universal Naming Convention), но нельзя указать пути к папкам на сетевых дисках защищаемого компьютера.<br>Указывая путь к папке с файлом дампа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения. |
| /SNAPSHOT | Снимает образ памяти указанного выполняющегося процесса Kaspersky Embedded Systems Security 2.2 и сохраняет файл дампа в папке, 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. 261).

## Импорт параметров. KAVSHELL IMPORT

С помощью команды `KAVSHELL IMPORT` вы можете импортировать параметры Kaspersky Embedded Systems Security 2.2, его функций и задач из конфигурационного файла в Kaspersky Embedded Systems Security 2.2 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>
```

### Примеры команды KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

*Таблица 52. Ключи команды KAVSHELL IMPORT*

| Ключ | Описание |
|---|---|
| <имя конфигурационного файла и путь к файлу> | Имя конфигурационного файла, из которого будут импортированы параметры.<br>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. 262).

## Экспорт параметров. KAVSHELL EXPORT

С помощью команды `KAVSHELL EXPORT` вы можете экспортировать все параметры Kaspersky Embedded Systems Security 2.2 и существующих задач в конфигурационный файл, чтобы потом импортировать их в Kaspersky Embedded Systems Security 2.2 на других компьютерах.

### Синтаксис команды KAVSHELL EXPORT

```
KAVSHELL EXPORT <имя конфигурационного файла и путь к файлу>
```

### Примеры команды KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

*Таблица 53. Ключи команды KAVSHELL EXPORT*

| Ключ | Описание |
|---|---|
| <имя конфигурационного файла и путь к файлу> | Имя конфигурационного файла, в котором будут сохранены параметры.<br>Вы можете присвоить конфигурационному файлу любое расширение.<br>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. 262).

## 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>
```

### Примеры команды KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

*Таблица 54. 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 55. 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 2.2 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 2.2 работает под учетной записью Локальная система). |
| -99 | Неизвестная ошибка |

## Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL

*Таблица 56. 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 обнаруженных 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 57. Код возврата команды KAVSHELL TASK LOG-INSPECTOR*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -6 | Неверная операция (например, служба Kaspersky Embedded Systems Security 2.2 уже запущена или уже остановлена) |
| 402 | Задача уже запущена (для ключа /STATE) |

## Коды возврата команды KAVSHELL TASK

*Таблица 58. 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) |

| Код возврата | Описание |
|---|---|
| -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 59. 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 60. 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 |

| Код возврата | Описание |
|---|---|
| -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 2.2 не прошел проверку подлинности при соединении с источником обновлений |
| -236 | Базы программы повреждены |
| -301 | Недействительный ключ |

## Коды возврата команды KAVSHELL ROLLBACK

*Таблица 61. 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 62. 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 63. 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 64. Коды возврата команды KAVSHELL FBRESET*

| Код возврата | Описание |
|---|---|
| 0 | Операция выполнена успешно |
| -99 | Неизвестная ошибка |

## Коды возврата команды KAVSHELL DUMP

*Таблица 65. 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 66. 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 |
| 501 | Операция выполнена успешно, однако во время выполнения команды возникла ошибка / замечание, например, Kaspersky Embedded Systems Security 2.2 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 2.2 более поздней или несовместимой версии) |

## Коды возврата команды KAVSHELL EXPORT

*Таблица 67. 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 2.2 не экспортировал параметры какого-либо из функциональных компонентов |

# Интеграция со сторонними системами

В этом разделе описана интеграция Kaspersky Embedded Systems Security 2.2 с функциями и технологиями сторонних производителей.

## В этом разделе



# Контроль производительности. Счетчики Kaspersky Embedded Systems Security 2.2

Этот раздел содержит информацию о счетчиках Kaspersky Embedded Systems Security 2.2: 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 2.2 во время установки.

## В этом разделе

## О счетчиках производительности Kaspersky Embedded Systems Security 2.2

В состав устанавливаемых компонентов Kaspersky Embedded Systems Security 2.2 по умолчанию включен компонент **Счетчики производительности**. Во время установки Kaspersky Embedded Systems Security 2.2 регистрирует свои счетчики производительности для программы "Системный монитор" Microsoft Windows.

С помощью счетчиков Kaspersky Embedded Systems Security 2.2 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 2.2 и сбои в его работе.

Вы можете просматривать счетчики производительности Kaspersky Embedded Systems Security 2.2, 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 2.2 в случае, если значения счетчиков их превышают.

## Общее количество отвергнутых запросов

*Таблица 68. 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 2.2; рассчитывается с момента последнего запуска Kaspersky Embedded Systems Security 2.2.<br>Программа пропускает объекты, запросы на обработку которых отвергаются рабочими процессами Kaspersky Embedded Systems Security 2.2. |
| **Назначение** | Счетчик позволяет обнаруживать следующие ситуации:<br>• снижение качества постоянной защиты из-за полной загрузки рабочих процессов Kaspersky Embedded Systems Security 2.2;<br>• 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.<br>Возможны следующие ситуации в зависимости от поведения счетчика:<br>• счетчик показывает несколько отвергнутых запросов в течение длительного времени: все рабочие процессы Kaspersky Embedded Systems Security 2.2 были полностью загружены, поэтому Kaspersky Embedded Systems Security 2.2 не удалось проверить объекты.<br>Чтобы исключить пропуск объектов, увеличьте количество процессов программы для задач постоянной защиты. Вы можете использовать параметры Kaspersky Embedded Systems Security 2.2 **Максимальное количество активных процессов** и **Число процессов для постоянной защиты**.<br>• количество отвергнутых запросов значительно превышает критический порог и быстро растет: отказал диспетчер файловых перехватов. Программа не проверяет объекты при доступе. Перезапустите Kaspersky Embedded Systems Security 2.2. |

## Общее количество пропущенных запросов

*Таблица 69. 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 2.2, но не отправивших события о завершении обработки; рассчитывается с момента последнего запуска программы.<br>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 2.2 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.<br>Если скорость проверки не удовлетворительна, перезапустите Kaspersky Embedded Systems Security 2.2, чтобы восстановить простаивающие потоки. |

## Количество запросов, не обработанных из-за нехватки системных ресурсов

*Таблица 70. 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 2.2.<br>Kaspersky Embedded Systems Security 2.2 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 2.2 нуждаются в увеличении объема оперативной памяти для обработки запросов.<br>Возможно, активные процессы других программ используют всю доступную оперативную память. |

## Количество запросов, отданных на обработку

*Таблица 71. 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 2.2 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 (Average number of file interception dispatcher streams).

*Таблица 72. Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams).*

| | |
|---|---|
| **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 2.2. |

| | |
|---|---|
| **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 2.2 пропустит объект.<br>Увеличьте количество процессов Kaspersky Embedded Systems Security 2.2 для задач постоянной защиты. Вы можете использовать параметры Kaspersky Embedded Systems Security 2.2 **Максимальное количество активных процессов Количество процессов для постоянной защиты**. |

## Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).

*Таблица 73. Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).*

| | |
|---|---|
| **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 2.2 неравномерно распределяет нагрузку на выполняющиеся процессы.<br>Перезапустите Kaspersky Embedded Systems Security 2.2. |

## Количество элементов в очереди зараженных объектов

*Таблица 74. 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:<br>• прерывание постоянной защиты из-за возможного отказа диспетчера файловых перехватов;<br>• перегруженность процессора из-за неравномерного распределения процессорного времени между другими работающими программами и Kaspersky Embedded Systems Security 2.2;<br>• вирусную эпидемию. |
| **Нормальное / пороговое значение** | Значение счетчика может быть отличным от нуля, пока Kaspersky Embedded Systems Security 2.2 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:<br>• Kaspersky Embedded Systems Security 2.2 не обрабатывает объекты (возможно, отказал диспетчер файловых перехватов);<br>Перезапустите Kaspersky Embedded Systems Security 2.2.<br>• Недостаточно процессорного времени для обработки объектов;<br>Обеспечьте выделение дополнительного процессорного времени для Kaspersky Embedded Systems Security 2.2, например, снизив нагрузку на компьютер со стороны других программ.<br>• Возникла вирусная эпидемия.<br>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 75. 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 выделяемого рабочим процессам Kaspersky Embedded Systems Security 2.2 процессорного времени или сбоя в работе Kaspersky Embedded Systems Security 2.2. |
| **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 2.2 и загрузки компьютера процессами других программ.<br>Наблюдайте средний уровень показаний счетчика в течение продолжительного времени. Если общий уровень показаний счетчика снизился, то могла произойти одна из следующих ситуаций:<br>• Рабочим процессам Kaspersky Embedded Systems Security 2.2 не хватает процессорного времени для обработки объектов.<br>Обеспечьте выделение дополнительного процессорного времени для Kaspersky Embedded Systems Security 2.2, например, снизив нагрузку на компьютер со стороны других программ.<br>• Возник сбой в работе Kaspersky Embedded Systems Security 2.2 (простаивает несколько потоков).<br>Перезапустите Kaspersky Embedded Systems Security 2.2. |

# Счетчики и ловушки SNMP Kaspersky Embedded Systems Security 2.2

Этот раздел содержит информацию о счетчикахи ловушках SNMP Kaspersky Embedded Systems Security 2.2.

## В этом разделе



## О счетчиках и ловушках SNMP Kaspersky Embedded Systems Security 2.2

Если вы включили в состав устанавливаемых компонентов Kaspersky Embedded Systems Security 2.2 компонент **Счетчики и ловушки SNMP**, вы можете просматривать счетчики и ловушки Kaspersky Embedded Systems Security 2.2 по протоколам Simple Network Management Protocol (SNMP).

Чтобы просмотреть счетчики и ловушки Kaspersky Embedded Systems Security 2.2 на рабочем месте администратора, запустите на защищаемом компьютере Службу SNMP, а на рабочем месте администратора – Службу SNMP и Службу ловушек SNMP.

## Счетчики SNMP Kaspersky Embedded Systems Security 2.2

Этот раздел содержит таблицы с описанием параметров счетчиков SNMP Kaspersky Embedded Systems Security 2.2.

## В этом разделе



## Счетчики производительности

*Таблица 76. Счетчики производительности*

| Счетчик | Определение |
|---|---|
| currentRequestsAmount | Количество запросов, отправленных на обработку (см. стр. 266). |
| currentInfectedQueueLength | Количество элементов в очереди зараженных объектов (см. раздел "Количество элементов в очереди зараженных объектов" на стр. 268). |
| currentObjectProcessingRate | Количество объектов, обрабатываемых за секунду (см. стр. 268). |
| currentWorkProcessesNumber | Количество рабочих процессов Kaspersky Embedded Systems Security 2.2 в текущий момент |

## Счетчики карантина

*Таблица 77. 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) |

## Счетчики резервного хранилища

*Таблица 78. Счетчики резервного хранилища*

| Счетчик | Определение |
|---|---|
| currentBackupStorageSize | Объем данных в папке резервного хранилища (МБ) |

## Общие счетчики

*Таблица 79. 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 2.2 с момента его последнего запуска, в сотых долях секунды |
| currentFileMonitorTaskStatus | Статус задачи Постоянная защита файлов: **Вкл.** – запущена; **Выкл.** – остановлена или приостановлена. |

## Счетчик обновления

*Таблица 80. Счетчик обновлений*

| 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 81. 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 |
| totalObjectsQuarantined | Общее количество зараженных, возможно зараженных и других объектов, которые Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 вылечил; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |
| totalObjectsNotDisinfected | Общее количество зараженных и других объектов, которые Kaspersky Embedded Systems Security 2.2 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 2.2 удалил; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |
| totalObjectsNotDeleted | Общее количество зараженных, возможно зараженных и других объектов, которые Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 пытался поместить в резервное хранилище, но это ему не удалось; рассчитывается с момента последнего запуска задачи Постоянная защита файлов |

## Ловушки SNMP

Параметры ловушек SNMP Kaspersky Embedded Systems Security 2.2 описаны в таблице ниже.

*Таблица 82. Ловушки SNMP Kaspersky Embedded Systems Security 2.2*

| Ловушка | Описание | Параметры |
|---|---|---|
| eventThreatDetected | Обнаружен объект. | eventDateAndTime<br>eventSeverity<br>computerName<br>userName<br>objectName<br>threatName<br>detectType<br>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 2.2 продолжает резервировать зараженные объекты. | eventDateAndTime<br>eventSeverity<br>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 2.2 продолжает резервировать зараженные объекты. | eventDateAndTime<br>eventSeverity<br>eventSource |
| eventQuarantineStorageSizeExceeds | Превышен максимальный размер карантина. Общий объем данных в папке карантина превысил значение, указанное параметром **Максимальный размер карантина (МБ)**. Kaspersky Embedded Systems Security 2.2 продолжает помещать возможно зараженные объекты на карантин. | eventDateAndTime<br>eventSeverity<br>eventSource |
| eventThresholdQuarantineStorageSizeExceeds | Достигнут порог свободного места в карантине. Размер свободного пространства в папке карантина, заданный параметром **Порог доступного пространства в карантине (МБ)**, уменьшился до указанного значения. Kaspersky Embedded Systems Security 2.2 продолжает помещать возможно зараженные объекты на карантин. | eventDateAndTime<br>eventSeverity<br>eventSource |

| Ловушка | Описание | Параметры |
|---|---|---|
| eventObjectNotQuarantined | Ошибка карантина. | eventSeverity<br>eventDateAndTime<br>eventSource<br>userName<br>computerName<br>objectName<br>storageObjectNotAddedEventReason |
| eventObjectNotBackuped | Ошибка сохранения копии объекта в резервном хранилище. | eventSeverity<br>eventDateAndTime<br>eventSource<br>objectName<br>userName<br>computerName<br>storageObjectNotAddedEventReason |
| eventQuarantineInternalError | Ошибка карантина. | eventSeverity<br>eventDateAndTime<br>eventSource<br>eventReason |
| eventBackupInternalError | Ошибка резервного хранилища. | eventSeverity<br>eventDateAndTime<br>eventSource<br>eventReason |
| eventAVBasesOutdated | Базы программы устарели. Рассчитывается количество дней, прошедших с момента последнего завершения задачи обновления баз (локальной, групповой задачей или задачей для наборов компьютеров). | eventSeverity<br>eventDateAndTime<br>eventSource<br>days |
| eventAVBasesTotallyOutdated | Базы программы сильно устарели. Рассчитывается количество дней, прошедших с момента последнего завершения задачи обновления баз (локальной, групповой задачей или задачей для наборов компьютеров). | eventSeverity<br>eventDateAndTime<br>eventSource<br>days |
| eventApplicationStarted | Kaspersky Embedded Systems Security 2.2 запущен. | eventSeverity<br>eventDateAndTime<br>eventSource |
| eventApplicationShutdown | Kaspersky Embedded Systems Security 2.2 остановлен. | eventSeverity<br>eventDateAndTime<br>eventSource |

| Ловушка | Описание | Параметры |
|---|---|---|
| eventCriticalAreasScanWasntPerformForALongTime | Проверка важных областей не проводилась давно. Рассчитывается количество дней с момента последнего завершения задачи, имеющей статус *Задача проверки важных областей*. | eventSeverity<br>eventDateAndTime<br>eventSource<br>days |
| eventLicenseHasExpired | Срок действия лицензии истек. | eventSeverity<br>eventDateAndTime<br>eventSource |
| eventLicenseExpiresSoon | Срок действия лицензии скоро истечет. Рассчитывается количество дней, оставшихся до окончания срока действия лицензии. | eventSeverity<br>eventDateAndTime<br>eventSource<br>days |
| eventTaskInternalError | Ошибка выполнения задачи. | eventSeverity<br>eventDateAndTime<br>eventSource<br>errorCode<br>knowledgeBaseId<br>taskName |
| eventUpdateError | Ошибка выполнения задачи обновления. | eventSeverity<br>eventDateAndTime<br>taskName<br>updaterErrorEventReason |

В таблице ниже описаны параметры ловушек и возможные значения параметров.

*Таблица 83. Значения параметров ловушек SNMP*

| Параметр | Описание и возможные значения |
|---|---|
| eventDateAndTime | Время возникновения события. |
| eventSeverity | Уровень важности события. Параметр принимает следующие значения:<br>• critical (1) – критический,<br>• warning (2) – предупреждение,<br>• 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). |

| Параметр | Описание и возможные значения |
|---|---|
| eventSource | Источник события: функциональный компонент, в работе которого возникло событие. Параметр принимает следующие значения:<br>• unknown (0) – функциональный компонент не определен;<br>• quarantine (1) – Карантин;<br>• backup (2) – Резервное хранилище;<br>• reporting (3) – Журналы выполнения задач;<br>• updates (4)– Обновление;<br>• realTimeProtection (5) – Постоянная защита файлов;<br>• onDemandScanning (6) – Проверка по требованию;<br>• product (7) – событие связано не с работой отдельных компонентов, а с работой Kaspersky Embedded Systems Security 2.2 в целом;<br>• systemAudit (8) – Журнал системного аудита. |
| eventReason | Причина возникновения события. Параметр принимает следующие значения:<br>• reasonUnknown (0) – причина не определена,<br>• 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 2.2 будет использовать папку резервного хранилища или папку карантина, установленную по умолчанию. |
| objectName | Имя объекта (например, имя файла, в котором обнаружена угроза). |
| threatName | Имя объекта согласно классификации Вирусной энциклопедии. Это имя входит в полное название обнаруженного объекта, которое Kaspersky Embedded Systems Security 2.2 возвращает при обнаружении объекта. Полное имя обнаруженного объекта можно просмотреть в журнале выполнения задач (см. раздел "Настройка параметров журналов" на стр. 143). |
| detectType | Тип обнаруженного объекта.<br>Параметр принимает следующие значения:<br>• undefined (0) – не определен;<br>• virware – классические вирусы и сетевые черви;<br>• trojware – троянские программы;<br>• malware – прочие вредоносные программы;<br>• adware – рекламные программы;<br>• pornware – порнографические программы;<br>• riskware – легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным. |

| Параметр | Описание и возможные значения |
|---|---|
| detectCertainty | Степень уверенности обнаружения угрозы. Параметр принимает следующие значения:<br>• Suspicion (возможно зараженный) – Kaspersky Embedded Systems Security 2.2 обнаружил частичное совпадение участка кода объекта с известным вредоносным кодом;<br>• Sure (зараженный) – Kaspersky Embedded Systems Security 2.2 обнаружил 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 принимает следующие значения:<br>• reasonUnknown (0) – причина не определена,<br>• reasonAccessDenied – доступ запрещен;<br>• reasonUrlsExhausted – список источников обновлений исчерпан;<br>• reasonInvalidConfig – неправильный файл конфигурации;<br>• reasonInvalidSignature – неверная подпись;<br>• reasonCantCreateFolder – невозможно создать папку;<br>• reasonFileOperError – файловая ошибка;<br>• reasonDataCorrupted – объект поврежден;<br>• reasonConnectionReset – сброс соединения;<br>• reasonTimeOut – истекло время ожидания при соединении;<br>• reasonProxyAuthError – ошибка проверки подлинности на прокси-сервере;<br>• reasonServerAuthError – ошибка проверки подлинности на сервере;<br>• reasonHostNotFound – компьютер не найден;<br>• reasonServerBusy – сервер недоступен;<br>• reasonConnectionError – ошибка соединения;<br>• reasonModuleNotFound – объект не найден;<br>• reasonBlstCheckFailed(16) – ошибка проверки черного списка ключей. Возможно, в момент обновления публиковались обновления баз; повторите обновление через несколько минут. |

| Параметр | Описание и возможные значения |
|---|---|
| storageObjectNotAddedEventReason | Причина непомещения объекта в резервное хранилище или на карантин. Параметр принимает следующие значения:<br>• reasonUnknown (0) – причина не определена,<br>• reasonStorageInternalError – ошибка базы данных; восстановите Kaspersky Embedded Systems Security 2.2.<br>• reasonStorageReadOnly – база данных доступна только для чтения; восстановите Kaspersky Embedded Systems Security 2.2.<br>• reasonStorageIOError – ошибка ввода-вывода: а) Kaspersky Embedded Systems Security 2.2 поврежден, восстановите Kaspersky Embedded Systems Security 2.2; б) диск, на котором хранятся файлы Kaspersky Embedded Systems Security 2.2, поврежден.<br>• reasonStorageCorrupted – хранилище повреждено; восстановите Kaspersky Embedded Systems Security 2.2.<br>• reasonStorageFull – база данных полна; освободите место на диске.<br>• reasonStorageOpenError – не удалось открыть файл базы данных; восстановите Kaspersky Embedded Systems Security 2.2.<br>• reasonStorageOSFeatureError – некоторые особенности операционной системы не отвечают требованиям Kaspersky Embedded Systems Security 2.2.<br>• reasonObjectNotFound – помещаемый в хранилище объект отсутствует на диске.<br>• reasonObjectAccessError – недостаточно прав для использования Backup API: учетная запись, с правами которой выполняется операция, не обладает правами Backup Operator.<br>• reasonDiskOutOfSpace – недостаточно места на диске. |

# Интеграция с WMI

Kaspersky Embedded Systems Security 2.2 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 2.2 и ее компонентов.

В момент установки Kaspersky Embedded Systems Security 2.2 регистрирует в системе собственный модуль, который обеспечивает создание пространства имен Kaspersky Embedded Systems Security 2.2 в корневом пространстве имен WMI на локальном компьютере. Пространство имен Kaspersky Embedded Systems Security 2.2 позволяет работать с классами, экземплярами классов и их свойствами в Kaspersky Embedded Systems Security 2.2.

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 таких 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 84. 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. |
| IsLicenseInstalled | The application activation state. | Статус ключа, с помощью которого активирована программа.<br>Возможные значения:<br>• False – В программе не задан ключ или код активации.<br>• 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.<br>Возможные неположительные значения:<br>• 0 - Срок действия лицензии истек<br>• -1 - Не удалось получить данные о текущем ключе или указанный ключ не может быть использован для активации программы (например, заблокирован по чёрному списку ключей). |

| Свойство экземпляра класса | Описание | Значения |
|---|---|---|
| AVBasesDatetime | The timestamp for a current anti-virus database version. | Дата и время формирования антивирусных баз, используемых в текущий момент.<br>Если установленная программа не использует антивирусные базы, поле содержит значение “Not installed”. |
| IsExploitPreventionEnabled | The Exploit Prevention component state. | Статус компонента Защита от эксплойтов.<br>Возможные значения:<br>• True - Компонент Защита от эксплойтов включен и выполняет функции защиты.<br>• 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.<br>Если ни одна из нецикличных задач не запущена, поле содержит значение «No». |
| IsAppControlRunning | The Applications Launch Control task state. | Статус выполнения задачи Контроль запуска программ.<br>• True - Задача Контроль запуска программ выполняется в текущий момент.<br>• 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.<br>Возможные значения:<br>• Active - в параметрах задачи указан **Активный** режим.<br>• Statistics Only - в параметрах задачи указан режим **Только статистика**.<br>• 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. |

| Свойство экземпляра класса | Описание | Значения |
|---|---|---|
| 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.<br>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.<br>Если ни одна цикличная задача не запущена в текущий момент, поле содержит значение “No”. |
| 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.<br>Возможные значения:<br>• Success - Соединение успешно установлено: клиент WMI может принимать данные о статусе программы.<br>• 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 2.2
- .ProductName=Kaspersky Embedded Systems Security является ключом параметра Kaspersky Embedded Systems Security 2.2.

Экземпляр класса создается в пространстве имен ROOT\Kaspersky\Security.

# 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).

## 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 2.2 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 компьютера.

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.

# 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 стране 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 |
| Вирусная лаборатория: | http://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и веб-сайтов) |
| Веб-форум "Лаборатории Касперского": | https://forum.kaspersky.ru |

# 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.

Microsoft, Active Directory, Excel, Internet Explorer, Outlook, Windows, Windows Server и Windows Vista – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

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.

# 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 устройствах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на устройствах 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).

# Предметный указатель

## Д



## З