



# Kaspersky Embedded Systems Security

*Руководство администратора*

*Версия программы: 2.1*

Уважаемый пользователь!

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

Внимание! Права на этот документ являются собственностью АО "Лаборатория Касперского" (далее также "Лаборатория Касперского") и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения "Лаборатории Касперского".

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, "Лаборатория Касперского" ответственности не несет.

В этом документе используются зарегистрированные товарные знаки и знаки обслуживания, которые являются собственностью соответствующих правообладателей.

Дата редакции документа: 27.03.2018

© АО "Лаборатория Касперского", 2018.

<http://www.kaspersky.ru>  
<http://support.kaspersky.ru>

# Содержание

Об этом документе .....	11
В этом документе .....	11
Условные обозначения .....	15
Источники информации о Kaspersky Embedded Systems Security 2.1 .....	17
Источники для самостоятельного поиска информации .....	17
Обсуждение программ "Лаборатории Касперского" на форуме .....	18
Kaspersky Embedded Systems Security 2.1 .....	19
О Kaspersky Embedded Systems Security 2.1 .....	19
Что нового .....	23
Комплект поставки .....	24
Требования к устройству, на которое устанавливается Kaspersky Embedded Systems Security 2.1 .....	28
Установка и удаление программы .....	31
Программные компоненты Kaspersky Embedded Systems Security 2.1 и их коды для службы Windows Installer .....	32
Программные компоненты Kaspersky Embedded Systems Security 2.1 .....	32
Программные компоненты набора "Средства администрирования" .....	38
Изменения в системе после установки Kaspersky Embedded Systems Security 2.1 .....	39
Процессы Kaspersky Embedded Systems Security 2.1 .....	45
Параметры установки и удаления и их ключи для службы Windows Installer .....	46
Журнал установки и удаления Kaspersky Embedded Systems Security 2.1 .....	54
Планирование установки .....	55
Выбор средств администрирования .....	56
Выбор способа установки .....	57
Установка и удаление программы с помощью мастера .....	59
Установка с помощью мастера установки .....	60
Установка Kaspersky Embedded Systems Security 2.1 .....	61
Установка Консоли Kaspersky Embedded Systems Security 2.1 .....	64
Дополнительная настройка после установки Консоли Kaspersky Embedded Systems Security 2.1 на другом компьютере .....	65
Действия после установки Kaspersky Embedded Systems Security 2.1 .....	71

Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security 2.1 .....	75
Удаление с помощью мастера установки .....	77
Удаление Kaspersky Embedded Systems Security 2.1 .....	78
Удаление Консоли Kaspersky Embedded Systems Security 2.1 .....	79
Установка и удаление программы из командной строки .....	81
Об установке и удалении Kaspersky Embedded Systems Security 2.1 из командной строки .....	81
Примеры команд для установки Kaspersky Embedded Systems Security 2.1...	82
Действия после установки Kaspersky Embedded Systems Security 2.1 .....	84
Добавление и удаление компонентов. Примеры команд .....	85
Удаление Kaspersky Embedded Systems Security 2.1. Примеры команд .....	86
Коды возврата.....	87
Установка и удаление программы через Kaspersky Security Center .....	89
Общие сведения об установке через Kaspersky Security Center.....	89
Права для установки или удаления Kaspersky Embedded Systems Security 2.1 .....	90
Процедура установки Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center .....	91
Действия после установки Kaspersky Embedded Systems Security 2.1 .....	93
Установка Консоли Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center .....	94
Удаление Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center.....	96
Установка и удаление программы через групповые политики Active Directory ...	97
Установка Kaspersky Embedded Systems Security 2.1 через групповые политики Active Directory .....	97
Действия после установки Kaspersky Embedded Systems Security 2.1 .....	99
Удаление Kaspersky Embedded Systems Security 2.1 через групповые политики Active Directory .....	99
Проверка функций Kaspersky Embedded Systems Security 2.1. Использование тестового вируса EICAR .....	100
О тестовом вирусе EICAR.....	100
Проверка функций Kaspersky Embedded Systems Security 2.1 Постоянная защита и Проверка по требованию .....	102
Миграция параметров из Kaspersky Embedded Systems Security 1.1 .....	105

Интерфейс программы .....	106
Лицензирование программы .....	107
О Лицензионном соглашении .....	107
О лицензии .....	108
О лицензионном сертификате .....	109
О ключе.....	110
О коде активации .....	110
О файле ключа.....	111
О предоставлении данных .....	111
Активация программы с помощью ключа.....	113
Просмотр информации о действующей лицензии .....	114
Продление срока действия лицензии .....	118
Удаление ключа .....	119
Запуск и остановка Kaspersky Embedded Systems Security 2.1 .....	120
Запуск плагина управления Kaspersky Security Center .....	120
Запуск и остановка службы Kaspersky Security Service .....	120
Права доступа к функциям Kaspersky Embedded Systems Security 2.1 .....	122
О правах на управление Kaspersky Embedded Systems Security 2.1 .....	122
О правах на управление службой Kaspersky Security Service .....	125
О правах доступа к службе Kaspersky Security Management.....	128
Настройка прав доступа на управление Kaspersky Embedded Systems Security 2.1 и службой Kaspersky Security Service .....	129
Защита доступа к функциям Kaspersky Embedded Systems Security 2.1 с помощью пароля.....	132
Разрешение сетевых соединений для службы Kaspersky Security Management Service.....	135
Создание и настройка политик .....	136
О политиках.....	136
Создание политики.....	137
Настройка политики.....	140
Настройка запуска по расписанию локальных системных задач.....	148
Создание и настройка задач в Kaspersky Security Center.....	151
О создании задач в Kaspersky Security Center.....	151
Создание задачи в Kaspersky Security Center .....	152

Настройка локальных задач в окне Параметры программы в Kaspersky Security Center .....	159
Настройка групповых задач в Kaspersky Security Center .....	161
Задачи генерации правил контроля устройств и контроля запуска программ .....	172
Задача Активация программы .....	175
Задачи обновления программы .....	176
Задача Проверка по требованию .....	179
Присвоение задаче проверки по требованию статуса "Задача проверки важных областей" .....	180
Задача Проверка целостности модулей программы .....	182
Настройка параметров диагностики сбоев в Kaspersky Security Center .....	183
Работа с расписанием задач .....	186
Настройка параметров расписания запуска задач .....	187
Включение и выключение запуска по расписанию .....	190
Управление параметрами программы .....	191
О способах управления Kaspersky Embedded Systems Security 2.1 из Kaspersky Security Center .....	191
О настройке общих параметров программы в Kaspersky Security Center .....	193
Настройка масштабируемости и интерфейса в Kaspersky Security Center ...	193
Настройка параметров безопасности в Kaspersky Security Center .....	196
Настройка параметров соединения в Kaspersky Security Center .....	199
О настройке дополнительных возможностей программы .....	201
Настройка параметров доверенной зоны в Kaspersky Security Center .....	202
Проверка съёмных дисков .....	206
Настройка прав доступа в Kaspersky Security Center .....	209
Настройка параметров карантина и резервного хранилища в Kaspersky Security Center .....	210
О настройке журналов и уведомлений .....	213
Настройка параметров журналов и уведомлений в Kaspersky Security Center .....	214
Настройка параметров интеграции с SIEM .....	216
Настройка параметров журналов и уведомлений в Kaspersky Security Center .....	221
Настройка взаимодействия с Сервером администрирования .....	223

Постоянная защита.....	225
Постоянная защита файлов.....	225
О задаче Постоянная защита файлов .....	226
Настройка параметров задачи Постоянная защита файлов.....	226
Область защиты в задаче Постоянная защита файлов .....	229
Предопределенные области защиты.....	229
Выбор предустановленных уровней безопасности .....	230
Настройка параметров безопасности вручную .....	234
Использование KSN .....	242
О задаче Использование KSN .....	242
Настройка параметров задачи Использование KSN .....	244
Настройка обработки данных .....	247
Защита от эксплойтов .....	249
О защите от эксплойтов .....	249
Настройка параметров защиты памяти процессов.....	251
Добавление защищаемого процесса .....	254
Техники снижения рисков.....	256
Контроль активности на компьютерах.....	258
Управление запуском программ из Kaspersky Security Center .....	258
Использование профиля при настройке задачи Контроль запуска программ в политике Kaspersky Security Center.....	259
Настройка параметров задачи Контроль запуска программ .....	261
Настройка контроля распространения программного обеспечения .....	267
О формировании правил контроля запуска программ для всей сети через Kaspersky Security Center .....	274
Создание разрешающих правил из событий Kaspersky Security Center ...	277
Импорт правил контроля запуска программ из файла формата XML .....	278
Импорт правил из файла отчета Kaspersky Security Center о заблокированных запусках программ .....	281
Управление подключением устройств из Kaspersky Security Center .....	284
О формировании правил контроля устройств для всей сети через Kaspersky Security Center .....	284
Создание правил на основе данных системы о внешних устройствах, подключавшихся к компьютерам сети .....	287
Формирование правил с помощью задачи Генерация правил контроля устройств .....	288

Формирование разрешающих правил на основе данных системы в политике Kaspersky Security Center.....	290
Формирование правил для подключенных устройств .....	291
Импорт правил из файла отчета Kaspersky Security Center о заблокированных устройствах.....	292
Контроль активности в сети .....	295
Управление сетевым экраном .....	295
О задаче Управление сетевым экраном.....	295
О правилах сетевого экрана .....	297
Активация и деактивация правил сетевого экрана .....	299
Добавление правил сетевого экрана вручную .....	300
Удаление правил сетевого экрана .....	302
Диагностика системы.....	304
Мониторинг файловых операций.....	304
О задаче Мониторинг файловых операций .....	304
О правилах мониторинга файловых операций .....	306
Настройка параметров задачи Мониторинг файловых операций .....	310
Настройка правил мониторинга.....	314
Анализ журналов .....	318
О задаче Анализ журналов .....	318
Настройка эвристического анализатора .....	320
Настройка правил анализа журналов .....	323
Работа с Kaspersky Embedded Systems Security 2.1 из командной строки .....	326
Команды командной строки .....	326
Вызов справки о командах Kaspersky Embedded Systems Security 2.1. KAVSHELL HELP .....	330
Запуск и остановка службы Kaspersky Security Service. KAVSHELL START, KAVSHELL STOP .....	331
Проверка указанной области. KAVSHELL SCAN.....	331
Запуск задачи Проверка важных областей. KAVSHELL SCANCritical .....	338
Управление указанной задачей в асинхронном режиме. KAVSHELL TASK .....	340
Запуск и остановка задач постоянной защиты. KAVSHELL RTP .....	341
Управление задачей Контроль запуска программ. KAVSHELL APPCONTROL /CONFIG .....	342



Генерация правил контроля запуска программ. KAVSHELL APPCONTROL /GENERATE.....	344
Поддержка программного обеспечения NCR. KAVSHELL APPCONTROL /PROFILE:NCR .....	347
Наполнение списка правил контроля запуска программ из файла. KAVSHELL APPCONTROL .....	348
Наполнение списка правил контроля устройств из файла. KAVSHELL DEVCONTROL .....	350
Запуск задачи обновления баз Kaspersky Embedded Systems Security 2.1. KAVSHELL UPDATE .....	352
Откат обновления баз Kaspersky Embedded Systems Security 2.1. KAVSHELL ROLLBACK.....	357
Активация программы. KAVSHELL LICENSE .....	358
Включение, настройка и выключение создания журнала трассировки. KAVSHELL TRACE.....	359
Дефрагментация файлов журнала Kaspersky Embedded Systems Security 2.1. KAVSHELL VACUUM .....	362
Очищение базы iSwift. KAVSHELL FBRESET .....	363
Включение и выключение создания файла дампа. KAVSHELL DUMP .....	364
Импорт параметров. KAVSHELL IMPORT .....	365
Экспорт параметров. KAVSHELL EXPORT .....	366
Коды возврата командной строки.....	368
Коды возврата команд KAVSHELL START и KAVSHELL STOP .....	369
Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCritical .....	369
Коды возврата команды KAVSHELL TASK .....	370
Коды возврата команды DEVCONTROL .....	371
Коды возврата команды KAVSHELL RTP .....	372
Коды возврата команды KAVSHELL UPDATE .....	372
Коды возврата команды KAVSHELL ROLLBACK .....	373
Коды возврата команды KAVSHELL LICENSE .....	374
Коды возврата команды KAVSHELL TRACE .....	375
Коды возврата команды KAVSHELL FBRESET .....	375
Коды возврата команды KAVSHELL DUMP .....	376
Коды возврата команды KAVSHELL IMPORT .....	376
Коды возврата команды KAVSHELL EXPORT .....	377

Контроль производительности. Счетчики Kaspersky Embedded Systems Security 2.1 .....	378
Счетчики производительности для программы Системный монитор .....	378
О счетчиках производительности Kaspersky Embedded Systems Security 2.1 .....	379
Общее количество отвергнутых запросов .....	380
Общее количество пропущенных запросов .....	381
Количество запросов, не обработанных из-за нехватки системных ресурсов .....	383
Количество запросов, отданных на обработку .....	384
Среднее количество потоков диспетчера файловых перехватов .....	385
Максимальное количество потоков диспетчера файловых перехватов .....	386
Количество элементов в очереди зараженных объектов .....	387
Количество объектов, обрабатываемых за секунду .....	388
Счетчики и ловушки SNMP Kaspersky Embedded Systems Security 2.1 .....	390
О счетчиках и ловушках SNMP Kaspersky Embedded Systems Security 2.1 ..	390
Счетчики SNMP Kaspersky Embedded Systems Security 2.1 .....	390
Счетчики производительности .....	391
Общие счетчики .....	392
Счетчик обновления .....	392
Счетчики постоянной защиты .....	393
Счетчики карантина .....	395
Счетчики резервного хранилища .....	395
Ловушки SNMP .....	395
Обращение в Службу технической поддержки .....	405
Способы получения технической поддержки .....	405
Техническая поддержка через Kaspersky CompanyAccount .....	406
Использование файла трассировки и скрипта AVZ .....	407
Глоссарий .....	408
АО "Лаборатория Касперского" .....	414
Информация о стороннем коде .....	416
Уведомления о товарных знаках .....	417
Предметный указатель .....	418

---

# Об этом документе

Руководство администратора Kaspersky Embedded Systems Security 2.1 адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Embedded Systems Security 2.1 на всех защищаемых устройствах, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Embedded Systems Security 2.1.

В этом руководстве вы можете найти информацию о настройке и использовании Kaspersky Embedded Systems Security 2.1.

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

## В этом разделе

В этом документе .....	<a href="#">11</a>
Условные обозначения .....	<a href="#">15</a>

## В этом документе

Руководство администратора Kaspersky Embedded Systems Security 2.1 содержит следующие разделы:

### **Источники информации о Kaspersky Embedded Systems Security 2.1**

Этот раздел содержит описание источников информации о программе.

### **Kaspersky Embedded Systems Security 2.1**

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Embedded Systems Security 2.1, перечень аппаратных и программных требований Kaspersky Embedded Systems Security 2.1.

## **Установка и удаление Kaspersky Embedded Systems Security 2.1**

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Embedded Systems Security 2.1.

## **Интерфейс программы**

Этот раздел содержит информацию об элементах интерфейса Kaspersky Embedded Systems Security 2.1.

## **Лицензирование программы**

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

## **Запуск и остановка Kaspersky Embedded Systems Security 2.1**

Этот раздел содержит информацию о запуске плагина управления Kaspersky Embedded Systems Security 2.1, а также запуске и остановке службы Kaspersky Security Service.

## **Права доступа к функциям Kaspersky Embedded Systems Security 2.1**

Этот раздел содержит информацию о правах на управление Kaspersky Embedded Systems Security 2.1 и службами Windows®, которые регистрирует программа, а также инструкции по настройке этих прав.

## **Создание и настройка политик**

Этот раздел содержит информацию о применении политик Kaspersky Security Center для управления задачами Kaspersky Embedded Systems Security 2.1 на нескольких компьютерах.

## **Создание и настройка задач в Kaspersky Security Center**

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security 2.1, их создании, настройке параметров выполнения, запуске и остановке.

## **Управление параметрами программы**

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center.

## **Постоянная защита**

Этот раздел содержит информацию о задачах постоянной защиты: задаче Постоянная защита файлов и задаче Использование KSN. Также этот раздел содержит инструкции по настройке параметров задач постоянной защиты и по настройке параметров безопасности защищаемого компьютера.

## **Контроль активности на компьютерах**

Этот раздел содержит информацию о функциональности Kaspersky Embedded Systems Security 2.1, которая позволяет контролировать запуски программ, подключения флеш-накопителей и других внешних устройств по USB, а также контролировать работу сетевого экрана Windows.

## **Контроль активности в сети**

Этот раздел содержит информацию о задачах Управление сетевым экраном, Защита от шифрования и Блокирование доступа к сетевым файловым ресурсам, а также о работе с правилами сетевого экрана и настройке параметров задач.

## **Диагностика системы**

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

## **Контроль производительности. Счетчики Kaspersky Embedded Systems Security 2.1**

Этот раздел содержит информацию о счетчиках Kaspersky Embedded Systems Security 2.1: счетчиках производительности для программы Системный монитор, счетчиках и ловушках SNMP.

## **Работа с Kaspersky Embedded Systems Security 2.1 из командной строки**

Этот раздел содержит описание работы с Kaspersky Embedded Systems Security 2.1 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 "Лаборатория Касперского".

## **Информация о стороннем коде**

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

## **Уведомления о товарных знаках**

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

## **Предметный указатель**

Этот раздел позволяет быстро найти необходимые сведения в документе.

# Условные обозначения

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

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: ...	Примеры приведены в блоках на голубом фоне под заголовком "Пример".
Обновление – это... Возникает событие <i>Базы устарели</i> .	Курсивом выделены следующие элементы текста: <ul style="list-style-type: none"><li>• новые термины;</li><li>• названия статусов и событий программы.</li></ul>
Нажмите на клавишу <b>ENTER</b> . Нажмите комбинацию клавиш <b>ALT+F4</b> .	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.

Пример текста	Описание условного обозначения
Нажмите на кнопку <b>Включить.</b>	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
► <i>Чтобы настроить расписание задачи, выполните следующие действия:</i>	Вводные фразы инструкций выделены курсивом и значком "стрелка".
В командной строке введите текст <code>help</code>  Появится следующее сообщение:  Укажите дату в формате ДД:ММ:ГГ.	Специальным стилем выделены следующие типы текста: <ul style="list-style-type: none"> <li>• текст командной строки;</li> <li>• текст сообщений, выводимых программой на экран;</li> <li>• данные, которые требуется ввести с клавиатуры.</li> </ul>
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.



---

# Источники информации о Kaspersky Embedded Systems Security 2.1

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 .....	<a href="#">17</a>
Обсуждение программ "Лаборатории Касперского" на форуме .....	<a href="#">18</a>

## Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Embedded Systems Security 2.1 :

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

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. [405](#)).

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

## **Страница Kaspersky Embedded Systems Security 2.1 на веб-сайте "Лаборатории Касперского"**

На странице Kaspersky Embedded Systems Security 2.1 (<http://www.kaspersky.ru/enterprise-security/embedded-systems>) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Embedded Systems Security 2.1 содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

## **Страница Kaspersky Embedded Systems Security 2.1 в Базе знаний**

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

На странице Kaspersky Embedded Systems Security 2.1 в Базе знаний (<http://support.kaspersky.ru/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 2.1, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

## **Документация Kaspersky Embedded Systems Security 2.1**

В Руководстве администратора Kaspersky Embedded Systems Security 2.1 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 с 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 2.1

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Embedded Systems Security 2.1, перечень аппаратных и программных требований Kaspersky Embedded Systems Security 2.1.

## В этом разделе

О Kaspersky Embedded Systems Security 2.1 .....	<a href="#">19</a>
Что нового.....	<a href="#">23</a>
Комплект поставки .....	<a href="#">24</a>
Требования к устройству, на которое устанавливается Kaspersky Embedded Systems Security 2.1 .....	<a href="#">28</a>

## О Kaspersky Embedded Systems Security 2.1

Kaspersky Embedded Systems Security 2.1 защищает компьютеры и другие встроенные системы, работающие под управлением операционных систем Microsoft® Windows®, от вирусов и других угроз компьютерной безопасности. Пользователями Kaspersky Embedded Systems Security 2.1 являются администраторы сети организации и сотрудники, отвечающие за антивирусную защиту сети организации.

Вы можете установить Kaspersky Embedded Systems Security 2.1 на любых типах встроенных систем под управлением Windows, в том числе на следующих классах устройств:

- банковские автоматы;
- POS-терминалы.

Вы можете управлять Kaspersky Embedded Systems Security 2.1 следующими способами:

- через Консоль Kaspersky Embedded Systems Security 2.1, установленную на одном компьютере с Kaspersky Embedded Systems Security 2.1 или на другом компьютере;
- с помощью команд командной строки;
- через плагин Kaspersky Embedded Systems Security 2.1 для Kaspersky Security Center (для централизованного управления защитой группы компьютеров, на каждом из которых установлен Kaspersky Embedded Systems Security 2.1).

Вы можете просматривать счетчики производительности Kaspersky Embedded Systems Security 2.1 для программы "Системный монитор", а также счетчики и ловушки SNMP.

## Компоненты и функции Kaspersky Embedded Systems Security 2.1

В состав программы входят следующие компоненты:

- **Постоянная защита.** Kaspersky Embedded Systems Security 2.1 проверяет объекты при обращении к ним. Kaspersky Embedded Systems Security 2.1 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 2.1 однократно проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Программа проверяет файлы, оперативную память защищаемого устройства, а также объекты автозапуска.
- **Контроль запуска программ.** Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.
- **Контроль устройств.** Компонент позволяет контролировать 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 подключаемым по USB флеш-накопителем или внешним устройством другого типа.

- **Управление сетевым экраном.** Компонент предоставляет возможность управления сетевым экраном Windows: позволяет настраивать параметры и правила сетевого экрана операционной системы и блокирует любую возможность настройки параметров сетевого экрана другими способами.
- **Мониторинг файловых операций.** Kaspersky Embedded Systems Security 2.1 выявляет изменения файлов, в областях мониторинга, заданных в параметрах задачи, которые 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 и модулей программы.** Kaspersky Embedded Systems Security 2.1 загружает обновления баз и модулей программы с FTP или HTTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или других источников обновлений.
- **Карантин.** Kaspersky Embedded Systems Security 2.1 помещает объекты, которые он признает возможно зараженными, на карантин, то есть переносит объекты из исходного местоположения на *карантин*. В целях безопасности объекты на карантине хранятся в зашифрованном виде.
- **Резервное хранилище.** Kaspersky Embedded Systems Security 2.1 сохраняет зашифрованные копии объектов со статусами *зараженный* или *обнаруживаемый* и *возможно зараженный* в резервном хранилище перед тем, как выполнить лечение или удаление этих объектов.
- **Уведомления администратора и пользователей.** Вы можете настроить уведомление администратора и пользователей, которые обращаются к защищаемому компьютеру, о событиях, связанных с работой Kaspersky Embedded Systems Security 2.1 и состоянием антивирусной защиты компьютера.

- **Импорт и экспорт параметров.** Вы можете экспортировать параметры Kaspersky Embedded Systems Security 2.1 в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Embedded Systems Security 2.1 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 2.1.
- **Управление правами доступа к функциям Kaspersky Embedded Systems Security 2.1.** Вы можете настраивать права на управление Kaspersky Embedded Systems Security 2.1 и службами Windows, которые регистрирует программа, для пользователей и групп пользователей.
- **Запись событий в журнал событий программы.** Kaspersky Embedded Systems Security 2.1 записывает в журналы 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 2.1, 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 2.1 будет применять в задачах проверки по требованию и постоянной защиты файлов.
- **Защита памяти процессов.** Вы можете защищать память процессов от эксплуатации уязвимостей с помощью внедряемого в процессы Агента защиты.

# Что нового

В новой версии Kaspersky Embedded Systems Security в полном объеме сохранены функциональные возможности программы Kaspersky Embedded Systems Security 2.0, а также учтены критические исправления и закрыты уязвимости, обнаруженные в предыдущих версиях программы.

Версия Kaspersky Embedded Systems Security 2.1 учитывает следующие критические исправления вышедших публичных и частных патчей:

- Оптимизирован алгоритм расчета данных о запускаемых DLL-файлах (при включённой функции контроля DLL-файлов):
  - Изменена процедура проверки подписи файлов, для которых выполняется перехват и проверка запуска.
  - Программа больше не рассчитывает все метаданные и контрольные суммы для запускаемых модулей, если эти данные не будут использованы в качестве критерия срабатывания или для записи в отчет (например, если запись событий, под которые подпадает запуск такого файла, отключена, или если запуск файла обрабатывается по кешу, то есть требует учета только пути к файлу).

Исправление значительно уменьшает время загрузки операционной системы и снижает нагрузку на маломощные устройства.

- Исправлена ошибка обработки запусков файлов с цифровой подписью файла каталога (.cat) для компонента Контроль запуска программ на операционных системах Microsoft Windows 10 и выше. Kaspersky Embedded Systems Security корректно применяет разрешающие и запрещающие правила по сертификату для файлов с подписью CAT-типа после применения исправления.
- Улучшен контроль USB-подключений:
  - Повышена стабильность работы компонента Проверка съемных дисков на компьютерах с операционной системой Microsoft Windows XP SP2.
  - Исправлен формат событий, регистрируемых программой в Kaspersky Security Center при подключении внешних устройств по шине USB к защищаемому

компьютеру. После применения исправления программа отправляет полные данные о подключенном внешнем устройстве в рамках событий на Сервер администрирования.

- Исправлены причины избыточного потребления ресурсов Агентом администрирования при установке программы в конфигурации “no-av-bases”.
- Оптимизирована обработка поврежденных файлов отчетов программы при запуске службы Kaspersky Security (KAVFS): наличие поврежденных файлов отчетов больше не приводит к ошибкам запуска службы KAVFS.
- Оптимизирован алгоритм расчета свободной оперативной памяти перед развертыванием обновленных антивирусных баз: после применения исправления программа точнее рассчитывает свободную память, доступную под проверочный запуск новых компонентов защиты.
- Улучшен алгоритм обнаружения и валидации компонента Filter Manager в среде развертывания (для операционных систем Microsoft Windows XP SP2).

В версии Kaspersky Embedded Systems Security 2.1 закрыт ряд критических уязвимостей, в том числе уязвимость драйвера, эксплуатация которой позволяла максимально повысить привилегии исполнения для процесса, запущенного от имени непривилегированного пользователя. Описание уязвимости: <https://support.kaspersky.ru/13893>.

Версия Kaspersky Embedded Systems Security 2.1 соответствует Общему регламенту по защите данных (General Data Protection Regulation). Условия, ответственность и порядок передачи и обработки данных определены в Лицензионном соглашении и Положении о KSN, а также во всех документах, ссылки на которые содержат Лицензионное соглашение и Положение о KSN.

## Комплект поставки

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

- запустить мастер установки Kaspersky Embedded Systems Security 2.1;



- запустить мастер установки Консоли Kaspersky Embedded Systems Security 2.1;
- запустить мастер установки плагина управления Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center;
- прочитать Руководство администратора;
- прочитать Руководство пользователя;
- перейти на страницу Kaspersky Embedded Systems Security 2.1 на веб-сайте "Лаборатории Касперского";
- перейти на веб-сайт Службы технической поддержки;
- прочитать информацию о текущем выпуске Kaspersky Embedded Systems Security 2.1.

Папка \console содержит файлы для установки Консоли Kaspersky Embedded Systems Security 2.1 (набор компонентов "Средства администрирования Kaspersky Embedded Systems Security 2.1").

Папка \product содержит:

- файлы для установки компонентов Kaspersky Embedded Systems Security 2.1 на компьютере под управлением 32-разрядной или 64-разрядной операционной системы Microsoft® Windows;
- файл для установки плагина управления Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center;
- файл архива антивирусных баз, актуальных на момент выпуска программы;
- файл с текстом Лицензионного соглашения и Политики конфиденциальности.

Папка \product\_no\_avbases содержит файлы установки компонентов и плагина Kaspersky Embedded Systems Security 2.1 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 2.1

Файл	Назначение
autorun.inf	Файл автозапуска мастера установки Kaspersky Embedded Systems Security 2.1 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 выпуске.
setup.exe	Файл запуска программы-приветствия; запускает setup.hta.
\console\esstools_x86(x64).msi	Пакет установки службы Windows Installer; устанавливает на компьютере Консоль Kaspersky Embedded Systems Security 2.1.
\console\setup.exe	Файл запуска мастера установки для набора компонентов "Средства администрирования" (в него входит Консоль Kaspersky Embedded Systems Security 2.1); 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 2.1 на защищаемом компьютере; запускает файл пакета установки ess.msi с указанными в мастере параметрами установки.

Файл	Назначение
product\less_x86(x64).msi	Пакет установки службы Windows Installer; устанавливает Kaspersky Embedded Systems Security 2.1 на защищаемом компьютере.
\product\less.kud	Файл в формате Kaspersky Unicode Definition с описанием инсталляционного пакета для удаленной установки Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center.
\product\klcfginst.exe	Программа установки плагина управления Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center. Установите плагин управления на каждом компьютере, на котором установлена Консоль администрирования Kaspersky Security Center, если вы планируете управлять Kaspersky Embedded Systems Security 2.1 через нее.
\product\license.txt	Текст Лицензионного соглашения и Политики конфиденциальности.
\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.

# Требования к устройству, на которое устанавливается Kaspersky Embedded Systems Security 2.1

Перед установкой Kaspersky Embedded Systems Security 2.1 требуется удалить с компьютера другие антивирусные программы.

## Аппаратные требования к устройству

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;
- всех программных компонентов – 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 устройству

Вы можете установить Kaspersky Embedded Systems Security 2.1 на устройстве под управлением 32-разрядной или 64-разрядной операционной системы Microsoft Windows.

Для установки и работы Kaspersky Embedded Systems Security 2.1 на устройстве под управлением операционной системы Windows XP требуется наличие Microsoft Windows Installer 3.1.

Для установки и работы Kaspersky Embedded Systems Security 2.1 на устройстве под управлением встроенных операционных систем требуется наличие компонентов Filter Manager и Administration Support Tools.

Вы можете установить Kaspersky Embedded Systems Security 2.1 на устройстве под управлением одной из следующих 32-разрядных операционных систем Microsoft Windows:

- Windows XP Embedded SP3.
- Windows XP Pro SP2 / SP3.
- Windows Embedded POSReady 2009.
- Windows Embedded Standard 7 SP1.
- Windows Embedded Enterprise 7 SP1.
- Windows Embedded POSReady 7.
- Windows 7 Pro / Enterprise SP1.
- Windows Embedded 8.1 Industry Pro / Enterprise.
- Windows Embedded 8.1 Pro.
- Windows Embedded 8.0 Standard.
- Windows 8 Pro / Enterprise.

- Windows 8.1 Pro / Enterprise.
- Windows 10 Pro / Enterprise.
- Windows 10 Redstone 1 Pro / Enterprise.
- Windows 10 Redstone 2 Pro / Enterprise.
- Windows 10 IoT Enterprise.

Вы можете установить Kaspersky Embedded Systems Security 2.1 на устройстве под управлением одной из следующих 64-разрядных операционных систем Microsoft Windows:

- Windows XP Pro SP2 / SP3.
- Windows Embedded Standard 7 SP1.
- Windows Embedded Enterprise 7 SP1.
- Windows Embedded POSReady 7.
- Windows 7 Pro / Enterprise SP1.
- Windows Embedded 8.1 Industry Pro / Enterprise.
- Windows Embedded 8.1 Pro.
- Windows Embedded 8.0 Standard.
- Windows 8 Pro / Enterprise.
- Windows 8.1 Pro / Enterprise.
- Windows 10 Pro / Enterprise.
- Windows 10 Redstone 1 Pro / Enterprise.
- Windows 10 Redstone 2 Pro / Enterprise.
- Windows 10 IoT Enterprise.

---

# Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Embedded Systems Security 2.1.

## В этом разделе

Программные компоненты Kaspersky Embedded Systems Security 2.1 и их коды для службы Windows Installer .....	<a href="#">32</a>
Изменения в системе после установки Kaspersky Embedded Systems Security 2.1 ...	<a href="#">39</a>
Процессы Kaspersky Embedded Systems Security 2.1.....	<a href="#">45</a>
Параметры установки и удаления и их ключи для службы Windows Installer .....	<a href="#">46</a>
Журнал установки и удаления Kaspersky Embedded Systems Security 2.1 .....	<a href="#">54</a>
Планирование установки .....	<a href="#">60</a>
Установка и удаление программы с помощью мастера.....	<a href="#">60</a>
Установка и удаление программы из командной строки.....	<a href="#">81</a>
Установка и удаление программы через Kaspersky Security Center.....	<a href="#">89</a>
Установка и удаление программы через групповые политики Active Directory.....	<a href="#">97</a>
Проверка функций Kaspersky Embedded Systems Security 2.1. Использование тестового вируса EICAR.....	<a href="#">100</a>
Миграция параметров из Kaspersky Embedded Systems Security 1.1 .....	<a href="#">105</a>

# Программные компоненты Kaspersky Embedded Systems Security 2.1 и их коды для службы Windows Installer

По умолчанию файлы \product\ess\_x86(x64).msi устанавливают все программные компоненты Kaspersky Embedded Systems Security 2.1. 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 программных компонентов Kaspersky Embedded Systems Security 2.1 для службы Windows Installer. Вы можете использовать эти коды, чтобы задать список устанавливаемых компонентов при установке Kaspersky Embedded Systems Security 2.1 из командной строки.

## В этом разделе

Программные компоненты Kaspersky Embedded Systems Security 2.1 .....	<a href="#">32</a>
Программные компоненты набора "Средства администрирования" .....	<a href="#">37</a>

# Программные компоненты Kaspersky Embedded Systems Security 2.1

В следующей таблице содержатся коды и описание программных компонентов Kaspersky Embedded Systems Security 2.1.



Таблица 3. Описание программных компонентов Kaspersky Embedded Systems Security 2.1

Компонент	Код	Выполняет функции
Основная функциональность	Core	Этот компонент включает в себя набор базовых функций программы и обеспечивает их работу.
Контроль запуска программ	AppCtrl	<p>Этот компонент отслеживает попытки запуска программ пользователями и разрешает или запрещает запуск программ в соответствии с заданными правилами контроля запуска программ.</p> <p>Компонент реализуется в задаче Контроль запуска программ.</p>
Контроль устройств	DevCtrl	<p>Этот компонент отслеживает попытки подключения запоминающих USB устройств и запрещает или разрешает их использование в соответствии с заданными правилами контроля устройств.</p> <p>Компонент реализуется в задаче Контроль устройств.</p>
Антивирусная защита	AVProtection	<p>Этот компонент обеспечивает антивирусную защиту и включает в себя следующие компоненты:</p> <ul style="list-style-type: none"> <li>• Проверка по требованию;</li> <li>• Постоянная защита файлов.</li> </ul>

Компонент	Код	Выполняет функции
Проверка по требованию	Ods	<p>Этот компонент устанавливает системные файлы Kaspersky Embedded Systems Security 2.1 и файлы, реализующие задачи проверки по требованию (проверка объектов защищаемого сервера, выполняемая по требованию).</p> <p>Если, устанавливая Kaspersky Embedded Systems Security 2.1 из командной строки, вы укажете другие компоненты Kaspersky Embedded Systems Security 2.1, не указывая компонент Core, компонент Core будет установлен автоматически.</p>
Постоянная защита файлов	Oas	<p>Этот компонент обеспечивает антивирусную проверку файлов на защищаемом сервере при обращении к этим файлам.</p> <p>Компонент реализует задачу Постоянная защита файлов.</p>
Использование Kaspersky Security Network	Ksn	<p>Этот компонент реализует защиту на основе облачных технологий "Лаборатории Касперского".</p> <p>Компонент реализует задачу Использование KSN (отправка запросов и получение заключений от службы Kaspersky Security Network).</p>

Компонент	Код	Выполняет функции
Мониторинг файловых операций	Fim	Этот компонент позволяет фиксировать операции производимые над файлами в выбранной области мониторинга.  Компонент реализуется в задаче Мониторинг файловых операций.
Защита от эксплойтов	AntiExploit	Этот компонент обеспечивает управление параметрами защиты процессов в памяти защищаемого компьютера.
Служба Kaspersky Security Broker Host	BrokerService	Этот компонент позволяет применять службу Kaspersky Security Broker Host, которая используется программой для сообщения параметров защиты внешним агентам защиты, а также для получения данных о событиях безопасности от внешних агентов защиты.
Управление сетевым экраном	Firewall	Этот компонент предоставляет возможность управления сетевым экраном Windows через графический интерфейс Kaspersky Embedded Systems Security 2.1.  Компонент реализуется в задаче Управление сетевым экраном.

Компонент	Код	Выполняет функции
Модуль интеграции с Агентом администрирования Kaspersky Security Center	AKIntegration	Обеспечивает связь Kaspersky Embedded Systems Security 2.1 с Агентом администрирования Kaspersky Security Center.  Вы можете установить этот компонент на защищаемом компьютере, если вы планируете управлять программой через Kaspersky Security Center.
Инвентаризация журналов	LogInspector	Компонент позволяет осуществлять 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 2.1 и находить возможные узкие места при совместной работе Kaspersky Embedded Systems Security 2.1 с другими программами.

Компонент	Код	Выполняет функции
Поддержка SNMP-протокола	SnmpSupport	Компонент публикует счетчики и ловушки Kaspersky Embedded Systems Security 2.1 через службу Simple Network Management Protocol (SNMP) Microsoft Windows. Вы можете установить этот компонент на защищаемом компьютере только в случае, если служба Microsoft SNMP установлена на этом компьютере.
Значок Kaspersky Embedded Systems Security 2.1 в области уведомлений	TrayApp	Компонент отображает значок Kaspersky Embedded Systems Security 2.1 в области уведомлений панели задач защищаемого компьютера. Значок Kaspersky Embedded Systems Security 2.1 показывает состояние защиты компьютера, позволяет открыть Консоль Kaspersky Embedded Systems Security 2.1 (если она установлена) и окно <b>О программе</b> .
Утилита командной строки	Shell	Позволяет управлять Kaspersky Embedded Systems Security 2.1 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 2.1	MmcSnapin	Компонент устанавливает оснастку Microsoft Management Console для управления через Консоль Kaspersky Embedded Systems Security 2.1.  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 2.1. Вы можете открыть файл справки из меню <b>Пуск</b> или по клавише <b>F1</b> на открытом окне Консоли Kaspersky Embedded Systems Security 2.1.
Документация	Docs	Kaspersky Embedded Systems Security 2.1 сохраняет "Руководство администратора", "Руководство пользователя" в формате PDF на защищаемом компьютере. Вы можете открыть "Руководство администратора" и "Руководство пользователя" из меню <b>Пуск</b> .

# Изменения в системе после установки Kaspersky Embedded Systems Security 2.1

При установке Kaspersky Embedded Systems Security 2.1 и Консоли Kaspersky Embedded Systems Security 2.1 (набора "Средства администрирования") служба Windows Installer выполняет на компьютере следующие изменения:

- создает папки Kaspersky Embedded Systems Security 2.1 на защищаемом компьютере и компьютере, на котором установлена Консоль Kaspersky Embedded Systems Security 2.1;
- регистрирует службы Kaspersky Embedded Systems Security 2.1;
- создает группу пользователей Kaspersky Embedded Systems Security 2.1;
- регистрирует ключи Kaspersky Embedded Systems Security 2.1 в системном реестре.

Эти изменения описаны в таблице ниже.

## Папки Kaspersky Embedded Systems Security 2.1

Таблица 5. Папки Kaspersky Embedded Systems Security 2.1 на защищаемом компьютере

Папка	Файлы Kaspersky Embedded Systems Security 2.1
<p>Папка %Kaspersky Embedded Systems Security 2.1%; по умолчанию:</p> <p>В Microsoft Windows 32-разрядной версии – %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\</p> <p>В Microsoft Windows 64-разрядной версии – %ProgramFiles(x86)%\Kaspersky Embedded Systems Security\</p>	<p>Исполняемые файлы Kaspersky Embedded Systems Security 2.1 (папка назначения, указанная при установке).</p>
<p>Папка %Kaspersky Embedded Systems Security 2.1%\mibs</p>	<p>Файлы Management Information Base (MIB); содержат описание счетчиков и ловушек, публикуемых Kaspersky Embedded Systems Security 2.1 по протоколу SNMP.</p>
<p>Папка %Kaspersky Embedded Systems Security 2.1%\x64</p>	<p>64-разрядные версии исполняемых файлов Kaspersky Embedded Systems Security 2.1 (папка создается только при установке Kaspersky Embedded Systems Security 2.1 в Microsoft Windows 64-разрядной версии).</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Data\</p>	<p>Служебные файлы Kaspersky Embedded Systems Security 2.1.</p>



Папка	Файлы Kaspersky Embedded Systems Security 2.1
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Settings\  %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Dskm\	
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Update\	Файлы с параметрами источников обновлений.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\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\2.1\Reports\	Журналы выполнения задач и журнал системного аудита.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Bases\Current\	Набор баз, используемых в текущий момент.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Bases\Backup\	Резервная копия баз; перезаписывается при каждом обновлении баз.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Bases\Temp\	Временные файлы, создаваемые во время выполнения задач обновления.

Папка	Файлы Kaspersky Embedded Systems Security 2.1
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Quarantine\	Объекты на карантине (папка по умолчанию).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Backup\	Объекты в резервном хранилище (папка по умолчанию).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Restored\	Объекты, восстановленные из резервного хранилища и карантина (папка для восстановленных объектов по умолчанию).

Таблица 6. Папки, создаваемые при установке Консоли Kaspersky Embedded Systems Security 2.1

Папка	Файлы Kaspersky Embedded Systems Security 2.1
<p>Папка %Kaspersky Embedded Systems Security 2.1%; по умолчанию:</p> <ul style="list-style-type: none"> <li>в Microsoft Windows 32-разрядной версии – %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security 2.1\;</li> <li>в Microsoft Windows 64-разрядной версии – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security 2.1\</li> </ul>	Файлы набора "Средства администрирования" (папка назначения, указанная при установке Консоли Kaspersky Embedded Systems Security 2.1).

## Службы Kaspersky Embedded Systems Security 2.1

Службы Kaspersky Embedded Systems Security 2.1 запускаются под системной учетной записью **Локальная система (SYSTEM)**.

## Службы Kaspersky Embedded Systems Security 2.1

Службы Kaspersky Embedded Systems Security 2.1 запускаются под системной учетной записью **Локальная система (SYSTEM)**.

Таблица 7. Службы Kaspersky Embedded Systems Security 2.1

Служба	Назначение
Служба Kaspersky Security Service (KAVFS)	Основная служба Kaspersky Embedded Systems Security 2.1, которая управляет задачами и рабочими процессами Kaspersky Embedded Systems Security 2.1.
Служба Kaspersky Security Management Service (KAVFSGT)	Служба, предназначенная для управления программой через Консоль Kaspersky Embedded Systems Security 2.1.
Служба Kaspersky Security Broker Service (KAVFSWH)	Служба, выполняющая роль посредника для сообщения параметров защиты внешним агентам защиты, а также для получения данных о событиях безопасности.

## Группы Kaspersky Embedded Systems Security 2.1

Таблица 8. Группы Kaspersky Embedded Systems Security 2.1

Группа	Назначение
ESS Administrators	Группа на защищаемом компьютере, пользователи которой имеют полный доступ к Службе Kaspersky Security Management Service, а также доступ ко всем функциям Kaspersky Embedded Systems Security 2.1.

## Ключи системного реестра

Таблица 9. Ключи системного реестра

Ключ	Назначение
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Параметры службы Kaspersky Embedded Systems Security 2.1.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Параметры журнала событий Kaspersky Embedded Systems Security 2.1 (Kaspersky Event Log).
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Параметры службы управления Kaspersky Embedded Systems Security 2.1.
<p>В Microsoft Windows 32-разрядной версии:</p> <p>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]</p> <p>В Microsoft Windows 64-разрядной версии:</p> <p>[[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance].</p>	Параметры счетчиков производительности.
<p>В Microsoft Windows 32-разрядной версии:</p> <p>[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.1\SnmpAgent]</p> <p>В Microsoft Windows 64-разрядной версии:</p> <p>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Kaspersky Lab\ESS\2.1\SnmpAgent]</p>	Параметры компонента "Поддержка SNMP-протокола".

Ключ	Назначение
<p>В Microsoft Windows 32-разрядной версии:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.1\CrashDump\</p> <p>В Microsoft Windows 64-разрядной версии:</p> <p>HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\ESS\2.1\CrashDump\</p>	Параметры записи файла дампа.
<p>В Microsoft Windows 32-разрядной версии:</p> <p>HKEY_LOCAL_MACHINE\Software\KasperskyLab\ESS\2.1\Trace\</p> <p>В Microsoft Windows 64-разрядной версии:</p> <p>HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\ESS\2.1\Trace\</p>	Параметры журнала трассировки.

## Процессы Kaspersky Embedded Systems Security 2.1

Kaspersky Embedded Systems Security 2.1 запускает процессы, описанные в таблице ниже.

Таблица 10. Процессы Kaspersky Embedded Systems Security 2.1

Имя файла	Назначение
kavfswp.exe	Рабочий процесс Kaspersky Embedded Systems Security 2.1
kavtray.exe	Процесс компонента Значок Kaspersky Embedded Systems Security 2.1 в области уведомлений
kavshell.exe	Процесс утилиты командной строки
kavfsrqn.exe	Процесс удаленного управления Kaspersky Embedded Systems Security 2.1
kavfs.exe	Процесс службы Kaspersky Security Service
kavfsgt.exe	Процесс службы управления Kaspersky Security Management Service
kavfswh.exe	Процесс службы контроля внешних процессов Kaspersky Security Broker Host

## Параметры установки и удаления и их ключи для службы Windows Installer

В следующих таблицах описаны параметры установки и удаления Kaspersky Embedded Systems Security 2.1 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 msixexec службы Windows Installer при установке Kaspersky Embedded Systems Security 2.1 из командной строки.

Таблица 11. Параметры установки и их ключи в Windows Installer

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Принятие условий Лицензионного соглашения	Отклонить условия Лицензионного соглашения	EULA=<значение>  <b>0</b> – вы отклоняете условия Лицензионного соглашения.  <b>1</b> – вы принимаете условия Лицензионного соглашения.	Вам нужно принять условия Лицензионного соглашения для установки Kaspersky Embedded Systems Security 2.1.
Принятие условий Политики Конфиденциальности	Отклонить условия Политики Конфиденциальности	PRIVACYPOLICY=<значение>  <b>0</b> – вы отклоняете условия Политики Конфиденциальности.  <b>1</b> – вы принимаете условия Политики Конфиденциальности.	Вам нужно принять условия Политики Конфиденциальности для установки Kaspersky Embedded Systems Security 2.1.
Принять условия Положения о KSN	Условия Положения о KSN не приняты	KSNAGREEMENT=<значение>  <b>0</b> - вы отклоняете условия Положения о KSN;  <b>1</b> - вы принимаете условия Положения о KSN	Вам нужно принять или отклонить условия Положения о KSN для установки Kaspersky Embedded Systems Security 2.1.

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Папка назначения	<p>Kaspersky Embedded Systems Security 2.1: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security 2.1</p> <p>Средства администрирования: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security 2.1 Admins Tools</p> <p>В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%.</p>	INSTALLDIR=<полный путь к папке>	<p>Папка, в которой будут сохранены файлы Kaspersky Embedded Systems Security 2.1 при его установке.</p> <p>Вы можете указать другую папку.</p>
Запуск постоянной защиты файлов при запуске Kaspersky Embedded Systems Security 2.1 (Включить постоянную защиту после установки программы)	Запустить	<p>RUNRTP= &lt;значение&gt;</p> <p><b>1</b> – запустить;</p> <p><b>0</b> – не запускать.</p>	<p>Включите этот параметр, чтобы запустить постоянную защиту файлов при запуске Kaspersky Embedded Systems Security 2.1 (рекомендуется).</p>



Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Исключения из проверки, рекомендуемые корпорацией Microsoft <b>(Добавить к исключениям файлы, рекомендованные Microsoft)</b>	Исключать	ADDMSEXCLUSION= <значение>  <b>1</b> – исключать;  <b>0</b> – не исключать.	В задаче Постоянная защита файлов исключает из области защиты объекты на компьютере, которые рекомендует исключать корпорация Microsoft.  Некоторые программы на компьютере могут работать нестабильно, когда антивирусная программа перехватывает или изменяет файлы, к которым эти программы обращаются. К таким программам корпорация Microsoft относит, например, некоторые программы контроллеров доменов.
Исключения из проверки, рекомендуемые "Лабораторией Касперского" <b>(Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского")</b>	Исключать	ADDKLEXCLUSION= <значение>  <b>1</b> – исключать;  <b>0</b> – не исключать.	В задаче Постоянная защита файлов исключает из области защиты объекты на компьютере, которые рекомендует исключать "Лаборатория Касперского".

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Разрешать удаленное подключение к Консоли Kaspersky Embedded Systems Security 2.1	Не разрешать	ALLOWREMOTECON = <значение>  1 – разрешать; 0 – не разрешать.	По умолчанию удаленное подключение к Консоли Kaspersky Embedded Systems Security 2.1, установленной на защищенном компьютере, не разрешено. Во время установки вы можете разрешить подключение. Kaspersky Embedded Systems Security 2.1 создаст разрешающие правила для процесса kavfsgt.exe по протоколу TCP для всех портов.
Путь к файлу ключа ( <b>Ключ</b> )	Папка комплекта поставки \product	LICENSEKEYPATH= <имя файла ключа>	По умолчанию программа установки пытается найти файл ключа с расширением .key в папке \product комплекта поставки.  Если в папке \product хранится несколько файлов ключа, программа установки выбирает файл ключа с самой поздней датой истечения срока действия.  Вы можете предварительно сохранить файл ключа в папке \product или указать

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
			<p>другой путь к файлу ключа с помощью параметра Добавление ключа.</p> <p>Вы можете добавить ключ после установки Kaspersky Embedded Systems Security 2.1 с помощью выбранного вами средства администрирования, например, через Консоль Kaspersky Embedded Systems Security 2.1. Если вы не добавите ключ программы во время его установки, после установки Kaspersky Embedded Systems Security 2.1 не будет функционировать.</p>
Путь к конфигурационному файлу	Не указан	CONFIGPATH =<имя конфигурационного файла>	<p>Kaspersky Embedded Systems Security 2.1 импортирует параметры из указанного конфигурационного файла, созданного в программе.</p> <p>Kaspersky Embedded Systems Security 2.1 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.</p> <p>Если вы не укажете конфигурационный файл, после установки программа начнет работать с параметрами по умолчанию.</p>

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Разрешение сетевых соединений для Консоли	Выключен	ADDWFEXCLUSION=<значение>  <b>1</b> – разрешать;  <b>0</b> – не разрешать.	<p>Используйте этот параметр, если вы устанавливаете Kaspersky Embedded Systems Security 2.1 не на защищаемом компьютере. С помощью Консоли, установленной на другом компьютере, вы сможете управлять защитой компьютера удаленно.</p> <p>В брандмауэре Microsoft Windows компьютера будет открыт TCP-порт 135, разрешены сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Embedded Systems Security 2.1 kavfsrchn.exe и открыт доступ к программам DCOM.</p> <p>После завершения установки добавьте пользователей, которые будут управлять программой удаленно, в группу ESS Administrators на компьютере и разрешите на нем сетевые соединения для службы Kaspersky Security Management Service (файл kavfsgt.exe).</p> <p>Вы можете прочитать о том, как произвести дополнительную настройку при установке Консоли Kaspersky Embedded Systems Security 2.1 на другом компьютере (см. стр. <a href="#">65</a>).</p>

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Отключение проверки на наличие несовместимого программного обеспечения	Проверка выполняется	SKIPINCOMPATIBLESW = <значение>  0 - выполняется проверка на несовместимое программное обеспечение;  1 - проверка на наличие несовместимого программного обеспечения не выполняется.	Используйте этот параметр, чтобы включить или отключить проверку на наличие несовместимого программного обеспечения при установке программы на устройство в фоновом режиме.  Независимо от значения данного параметра, при установке Kaspersky Embedded Systems Security 2.1, программа всегда предупреждает о других версиях программы, установленных на этом же устройстве.

Таблица 12. Параметры удаления и их ключи в Windows Installer

Параметр	Значение по умолчанию	Описание, ключи Windows Installer и их значения
Восстановление содержимого карантина	Удалить	RESTOREQTN = <значение>  0 – удалить содержимое карантина;  1 – восстановить содержимое карантина в папку, указанную параметром RESTOREPATH.
Восстановление содержимого	Удалить	RESTOREBCK = <значение>

резервного хранилища		<p><b>0</b> – удалить содержимое резервного хранилища;</p> <p><b>1</b> – восстановить содержимое резервного хранилища в папку, указанную параметром RESTOREPATH.</p>
Ввод текущего пароля для подтверждения операции удаления (при активной функции применения пароля)	Не указано	UNLOCK_PASSWORD=<заданный пароль>
Папка для восстановленных объектов	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Restored	<p>RESTOREPATH=&lt;полный путь к папке&gt;</p> <p>Восстановленные объекты будут сохранены в папке, указанной этим параметром:</p> <p>Объекты из карантина будут сохранены во вложенной папке \Quarantine.</p> <p>Объекты из резервного хранилища – во вложенной папке \Backup.</p>

## Журнал установки и удаления Kaspersky Embedded Systems Security 2.1

Если вы выполняете установку или удаление Kaspersky Embedded Systems Security 2.1 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 мастер установки.

Если вы выполняете установку или удаление Kaspersky Embedded Systems Security 2.1 из командной строки, по умолчанию журнал установки не создается.

► *Чтобы установить Kaspersky Embedded Systems Security 2.1 с созданием файла журнала ess.log 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 2.1, особенностей установки Kaspersky Embedded Systems Security 2.1 с помощью мастера установки (см. раздел "Установка и удаление программы с помощью мастера" на стр. [60](#)), из командной строки (см. раздел "Установка и удаление программы из командной строки" на стр. [81](#)), через Kaspersky Security Center (см. раздел "Установка и удаление программы через Kaspersky Security Center" на стр. [89](#)) и через групповые политики Active Directory® (см. раздел "Установка и удаление программы через групповые политики Active Directory" на стр. [97](#)).

Перед тем как начать установку Kaspersky Embedded Systems Security 2.1, спланируйте основные этапы ее проведения:

1. Выберите средства администрирования, которые вы будете использовать для управления Kaspersky Embedded Systems Security 2.1 и его настройки.
2. Определите, какие программные компоненты требуется установить (см. раздел "Программные компоненты Kaspersky Embedded Systems Security 2.1 и их коды для службы Windows Installer" на стр. [32](#)).
3. Выберите способ установки.

## В этом разделе

Выбор средств администрирования.....	<a href="#">56</a>
Выбор способа установки .....	<a href="#">57</a>

# Выбор средств администрирования

Определите, какие средства администрирования вы будете использовать для настройки параметров Kaspersky Embedded Systems Security 2.1 и управления им. В качестве средств администрирования Kaspersky Embedded Systems Security 2.1 вы можете использовать Консоль Kaspersky Embedded Systems Security 2.1, утилиту командной строки и Консоль администрирования Kaspersky Security Center.

## Консоль Kaspersky Embedded Systems Security 2.1

Консоль Kaspersky Embedded Systems Security 2.1 представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console. Вы можете управлять Kaspersky Embedded Systems Security 2.1 через Консоль Kaspersky Embedded Systems Security 2.1, установленную на защищаемом компьютере или на другом компьютере в сети организации.

В одну Microsoft Management Console, открытую в авторском режиме, вы можете добавить несколько оснасток Kaspersky Embedded Systems Security 2.1, чтобы управлять из нее защитой нескольких компьютеров, на которых установлен Kaspersky Embedded Systems Security 2.1.

Консоль Kaspersky Embedded Systems Security 2.1 входит в набор компонентов "Средства администрирования".

## Утилита командной строки

Вы можете управлять Kaspersky Embedded Systems Security 2.1 из командной строки защищаемого компьютера.

Утилита командной строки входит в набор программных компонентов Kaspersky Embedded Systems Security 2.1.



## 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 2.1 через Консоль администрирования Kaspersky Security Center.

Вам потребуется установить следующие компоненты:

- **Модуль интеграции с Агентом администрирования Kaspersky Security Center.** Этот компонент входит в набор программных компонентов Kaspersky Embedded Systems Security 2.1. Он обеспечивает связь Kaspersky Embedded Systems Security 2.1 с Агентом администрирования. Установите Модуль интеграции с Агентом администрирования Kaspersky Security Center на защищаемом компьютере.
- **Агент администрирования Kaspersky Security Center.** Установите его на каждом защищаемом компьютере. Этот компонент будет обеспечивать взаимодействие между Kaspersky Embedded Systems Security 2.1, установленным на компьютере, и Консолью администрирования Kaspersky Security Center. Файл установки Агента администрирования входит в комплект поставки Kaspersky Security Center.
- **Плагин Kaspersky Embedded Systems Security 2.1.** Дополнительно на компьютер, на котором установлена Консоль администрирования Kaspersky Security Center, установите плагин управления Kaspersky Embedded Systems Security 2.1 через Сервер администрирования. Он обеспечивает интерфейс управления программой через Kaspersky Security Center. Файл установки плагина, \product\klcfginst.exe, входит в комплект поставки Kaspersky Embedded Systems Security 2.1.

## Выбор способа установки

После определения программных компонентов для установки Kaspersky Embedded Systems Security 2.1 (см. раздел "Программные компоненты Kaspersky Embedded Systems Security 2.1 и их коды для службы Windows Installer" на стр. [32](#)), вам 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 2.1, или вы будете использовать параметры установки по умолчанию (см. стр. [46](#));

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

Вы можете установить Kaspersky Embedded Systems Security 2.1 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 2.1: через групповые политики Active Directory или с помощью задачи удаленной установки Kaspersky Security Center.

Вы можете установить Kaspersky Embedded Systems Security 2.1 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 2.1 на других компьютерах (эта возможность не применяется при установке через групповые политики Active Directory).

### **Запуск мастера установки**

С помощью мастера установки вы можете установить:

- программные компоненты Kaspersky Embedded Systems Security 2.1 (см. стр. [61](#)) на защищаемом компьютере из файла `\product\setup.exe` комплекта поставки;
- Консоль Kaspersky Embedded Systems Security 2.1 из файла `\client\setup.exe` комплекта 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 2.1 с параметрами установки по умолчанию. С помощью ключей Kaspersky Embedded Systems Security 2.1 вы можете изменять параметры установки.

Вы можете установить Консоль Kaspersky Embedded Systems Security 2.1 на защищаемом компьютере и / или рабочем месте администратора.

Примеры команд для установки Kaspersky Embedded Systems Security 2.1 и Консоли Kaspersky Embedded Systems Security 2.1 приведены в разделе "Установка и удаление Kaspersky Embedded Systems Security 2.1 из командной строки" (см. стр. [81](#)).

## Централизованная установка через Kaspersky Security Center

Если вы используете программу Kaspersky Security Center для управления антивирусной защитой компьютеров сети, вы можете установить Kaspersky Embedded Systems Security 2.1 на нескольких компьютерах с помощью задачи удаленной установки Kaspersky Security Center.

Компьютеры, на которых вы хотите установить Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center (см. стр. [89](#)), 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 вы можете устанавливать Kaspersky Embedded Systems Security 2.1 на защищаемом компьютере. Вы также можете устанавливать Консоль Kaspersky Embedded Systems Security 2.1 на защищаемом компьютере или рабочем месте администратора.

Вы можете установить Kaspersky Embedded Systems Security 2.1 только с параметрами установки по умолчанию.

Компьютеры, на которых вы устанавливаете Kaspersky Embedded Systems Security 2.1 через групповые политики Active Directory, должны находиться в одном домене и в одной организационной единице. 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 2.1 и Консоли программы на защищаемом компьютере с помощью мастера установки, а также информацию о дополнительной настройке Kaspersky Embedded Systems Security 2.1 и действиях после установки программы.

## В этом разделе

Установка с помощью мастера установки .....	<a href="#">60</a>
Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security 2.1 .....	<a href="#">75</a>
Удаление с помощью мастера установки .....	<a href="#">77</a>

## Установка с помощью мастера установки

В следующих разделах содержится информация о том, как установить Kaspersky Embedded Systems Security 2.1 и Консоль Kaspersky Embedded Systems Security 2.1.

► *Чтобы установить и приступить к использованию Kaspersky Embedded Systems Security 2.1, выполните следующие действия:*

1. Установите Kaspersky Embedded Systems Security 2.1 на защищаемом компьютере.
2. На компьютерах, с которых вы планируете управлять Kaspersky Embedded Systems Security 2.1, установите Консоль Kaspersky Embedded Systems Security 2.1.
3. Если вы установили Консоль Kaspersky Embedded Systems Security 2.1 не на защищаемом компьютере, а на другом компьютере сети, выполните дополнительную настройку, чтобы пользователи Консоли могли через нее удаленно управлять Kaspersky Embedded Systems Security 2.1.
4. Выполните действия после установки Kaspersky Embedded Systems Security 2.1.

## В этом разделе

Установка Kaspersky Embedded Systems Security 2.1 .....	<a href="#">61</a>
Установка Консоли Kaspersky Embedded Systems Security 2.1 .....	<a href="#">64</a>
Дополнительная настройка после установки Консоли Kaspersky Embedded Systems Security 2.1 на другом компьютере .....	<a href="#">65</a>
Действия после установки Kaspersky Embedded Systems Security 2.1 .....	<a href="#">71</a>

# Установка Kaspersky Embedded Systems Security 2.1

Перед установкой Kaspersky Embedded Systems Security 2.1 выполните следующие действия:

- Убедитесь, что на компьютере не установлены другие антивирусные программы.
- Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, зарегистрирована в группе администраторов на защищаемом компьютере.

После выполнения описанных выше действий, перейдите к процедуре установки. Следуя инструкциям мастера установки, задайте параметры установки Kaspersky Embedded Systems Security 2.1. Вы можете прервать установку Kaspersky Embedded Systems Security 2.1 на любом шаге мастера установки. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Вы можете подробнее прочитать о параметрах установки (удаления) (см. стр. [46](#)).

► *Чтобы установить Kaspersky Embedded Systems Security 2.1 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 2.1**.
3. В открывшемся окне приветствия мастера установки Kaspersky Embedded Systems Security 2.1 нажмите на кнопку **Далее**.

Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.

4. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности.
5. Установите флажки, свидетельствующие, что вы принимаете **положения и условия настоящего Лицензионного соглашения и Политику конфиденциальности, которая описывает обработку данных** для продолжения установки.
6. Нажмите на кнопку **Далее**.

Откроется окно **Выборочная установка**.

7. По умолчанию в список устанавливаемых объектов включены все компоненты Kaspersky Embedded Systems Security 2.1, за исключением компонента Управление сетевым экраном.

Компонент Поддержка SNMP-протокола Kaspersky Embedded Systems Security 2.1 отображается в списке устанавливаемых компонентов только в случае, если на компьютере установлена Служба SNMP Microsoft Windows.

Выберите компоненты, которые вы хотите установить. Чтобы отменить все изменения в окне **Выборочная установка**, нажмите на кнопку **Сбросить**. Затем, нажмите на кнопку **Далее**.

8. В открывшемся окне **Выбор папки назначения** выполните следующие действия:

- Если требуется, укажите папку, в которой будут сохранены файлы Kaspersky Embedded Systems Security 2.1.
- Если требуется, просмотрите информацию о доступном пространстве на локальных жестких дисках по кнопке **Обзор**.

Нажмите на кнопку **Далее**.

9. 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**.

10. В окне **Импорт параметров из конфигурационного файла** выберите конфигурационный файл, если требуется.

11. 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 2.1 для активации программы.
- Если вы хотите активировать программу позже, нажмите на кнопку **Далее**.
- Если вы предварительно сохранили файл ключа в папке \product комплекта поставки, имя этого файла отобразится в поле **Ключ**.
- Если вы хотите добавить ключ с помощью файла ключа, который хранится в другой папке, укажите файл ключа.

Вы не можете активировать программу с помощью кода активации из мастера установки. Если вы хотите активировать программу с помощью кода активации, вы сможете добавить код активации после установки программы.

После добавления файла ключа в окне отобразится информация о лицензии. Kaspersky Embedded Systems Security 2.1 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 2.1.

14. По завершении установки откроется окно **Установка завершена**.

15. Установите флажок **Прочитать Release Notes**, чтобы просмотреть информацию о выпуске после завершения работы мастера установки.

16. Нажмите на кнопку **ОК**.

Окно мастера установки программы будет закрыто. По завершении установки Kaspersky Embedded Systems Security 2.1 будет готов к работе, если вы добавили ключ для активации программы..

# Установка Консоли Kaspersky Embedded Systems Security 2.1

Следуя инструкциям мастера установки, задайте параметры установки Консоли Kaspersky Embedded Systems Security 2.1. Вы можете прервать установку на любом шаге мастера. Для этого в окне мастера нажмите на кнопку **Отмена**.

► *Чтобы установить Консоль Kaspersky Embedded Systems Security 2.1, выполните следующие действия:*

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

2. Запустите на компьютере файл программы-приветствия setup.exe.

Откроется окно программы-приветствия.

3. Нажмите на ссылку **Установить Консоль Kaspersky Embedded Systems Security 2.1**.

Откроется окно приветствия мастера установки.

4. Нажмите на кнопку **Далее**.

Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.

5. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности.

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

7. Нажмите на кнопку **Далее**.

8. В окне **Выборочная установка** выберите компоненты из списка.

По умолчанию все компоненты набора "Средства администрирования" включены в список устанавливаемых. Выберите компоненты, которые вы хотите установить. Нажмите на кнопку **Далее**.

9. В открывшемся окне **Выбор папки назначения** выполните следующие действия:



Если требуется, укажите другую папку, в которой будут сохранены устанавливаемые файлы. Нажмите на кнопку **Далее**.

10. В открывшемся окне **Дополнительные параметры установки** выполните следующие действия:

Если вы планируете с помощью Консоли Kaspersky Embedded Systems Security 2.1 управлять Kaspersky Embedded Systems Security 2.1, установленным на удаленном компьютере, установите флажок **Разрешить удаленный доступ**. Нажмите на кнопку **Далее**.

11. В открывшемся окне **Готовность к установке** нажмите на кнопку **Установить**. Мастер приступит к установке выбранных компонентов.

12. По окончании установки откроется окно **Установка завершена**. Установите флажок **Прочитать Release Notes**, чтобы просмотреть информацию о выпуске после завершения работы мастера установки.

13. Нажмите на кнопку **ОК**.

Окно мастера установки будет закрыто. Консоль Kaspersky Embedded Systems Security 2.1 будет установлена на защищаемый компьютер.

Если вы установили набор "Средства администрирования" не на защищаемом компьютере, а на другом компьютере сети, выполните дополнительную настройку (см. раздел "Дополнительная настройка после установки Консоли Kaspersky Embedded Systems Security 2.1 на другом компьютере" на стр. [65](#)).

## Дополнительная настройка после установки Консоли Kaspersky Embedded Systems Security 2.1 на другом компьютере

Если вы установили Консоль Kaspersky Embedded Systems Security 2.1 не на защищаемом компьютере, а на другом компьютере сети, выполните описанные ниже действия для того, чтобы пользователи могли удаленно управлять Kaspersky Embedded Systems Security 2.1:

- На защищаемом компьютере добавьте пользователей Kaspersky Embedded Systems Security 2.1 в группу ESS Administrators.

- Разрешите сетевые соединения для службы Kaspersky Security Management Service (kavfsgt.exe), если на защищаемом компьютере используется брандмауэр Windows или сторонний сетевой экран.
- Если при установке Консоли Kaspersky Embedded Systems Security 2.1 на компьютере под управлением Microsoft Windows вы не установили флажок **Разрешить сетевые соединения для Консоли Kaspersky Embedded Systems Security 2.1**, разрешите сетевые соединения для Консоли Kaspersky Embedded Systems Security 2.1 вручную через брандмауэр на этом компьютере.

## В этом разделе

О правах доступа к службе Kaspersky Security Management Service.....	<a href="#">66</a>
Разрешение сетевых соединений для Консоли Kaspersky Embedded Systems Security 2.1.....	<a href="#">67</a>
Разрешение сетевых соединений для службы Kaspersky Security Management Service.....	<a href="#">70</a>

## О правах доступа к службе Kaspersky Security Management Service

Вы можете просмотреть список служб Kaspersky Embedded Systems Security 2.1 (см. раздел "Изменения в системе после установки Kaspersky Embedded Systems Security 2.1" на стр. [39](#)).

При установке Kaspersky Embedded Systems Security 2.1 обязательно регистрирует службу управления программой Kaspersky Security Management Service (KAVFSGT). Чтобы управлять программой через Консоль Kaspersky Embedded Systems Security 2.1, установленную на другом компьютере, требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Embedded Systems Security 2.1, имела полный доступ к службе Kaspersky Security Management Service на защищаемом компьютере.

По умолчанию доступ к управлению службой Kaspersky Security Management Service имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере, и пользователи группы ESS Administrators, созданной на защищаемом компьютере при установке Kaspersky Embedded Systems Security 2.1.

Вы можете управлять службой Kaspersky Security Management Service только через оснастку **Службы** Microsoft Windows.

Вы не можете разрешать или запрещать пользователям доступ к Kaspersky Security Management Service, настраивая параметры Kaspersky Embedded Systems Security 2.1.

Вы можете соединиться с Kaspersky Embedded Systems Security 2.1 под локальной учетной записью, если на защищаемом компьютере зарегистрирована учетная запись с таким же именем и с таким же паролем.

## Разрешение сетевых соединений для Консоли Kaspersky Embedded Systems Security 2.1

Названия параметров могут отличаться в разных операционных системах Windows.

Консоль Kaspersky Embedded Systems Security 2.1 на удаленном компьютере использует протокол DCOM, чтобы получать информацию о событиях Kaspersky Embedded Systems Security 2.1, например, проверенных объектах или завершении задач, от службы управления Kaspersky Embedded Systems Security 2.1 на защищаемом компьютере. Вам нужно разрешить сетевые соединения в брандмауэре Windows для Консоли Kaspersky Embedded Systems Security 2.1, чтобы устанавливать соединения между Консолью программы и службой управления Kaspersky Embedded Systems Security 2.1.

Выполните следующие действия:

- убедитесь, что разрешен анонимный удаленный доступ к программам COM (но не удаленный запуск и активация программ COM);

- в брандмауэре Windows откройте порт TCP 135 и разрешите сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Embedded Systems Security 2.1 kavfsrcl.exe.

Через порт TCP 135 клиентский компьютер, на котором установлена Консоль Kaspersky Embedded Systems Security 2.1, обменивается информацией с защищаемым компьютером.

Если Консоль Kaspersky Embedded Systems Security 2.1 открыта во время настройки параметров соединения между защищаемым компьютером и компьютером, на котором установлена Консоль Kaspersky Embedded Systems Security 2.1, вам нужно закрыть Консоль программы, дождаться завершения процесса удаленного управления Kaspersky Embedded Systems Security 2.1 kavfsrcl.exe и снова запустить Консоль. Новые параметры соединения будут применены.

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

1. На компьютере, на котором установлена Консоль Kaspersky Embedded Systems Security 2.1, откройте консоль Службы компонентов.
2. Выберите **Пуск** → **Выполнить**.
3. Введите команду `dcomcnfg`.
4. Нажмите на кнопку **ОК**.
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 **ОК**.

- Чтобы открыть в брандмауэре Windows TCP-порт 135 и разрешить сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Embedded Systems Security 2.1, выполните следующие действия:

1. На удаленном компьютере закройте Консоль Kaspersky Embedded Systems Security 2.1.

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 (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 2.1, в поле **Номер порта** укажите номер порта: 135.
  - d. Выберите протокол **TCP**.
  - e. Нажмите на кнопку **ОК**.
  - f. На закладке **Исключения** нажмите на кнопку **Добавить программу**.
- В Microsoft Windows 7 и выше:
  - a. Выберите **Пуск → Панель управления → Брандмауэр Windows** в окне **Брандмауэр Windows** выберите пункт **Разрешить запуск программы или компонента через брандмауэр Windows**.
  - b. В окне **Разрешить связь программ через брандмауэр Windows** нажмите на кнопку **Разрешить другую программу**.

3. В окне **Добавление программы** укажите файл kavfsrpn.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке Консоли Kaspersky Embedded Systems Security 2.1.
4. Нажмите на кнопку **ОК**.
5. Нажмите на кнопку **ОК** в окне **Брандмауэр Windows (Параметры брандмауэра Windows)**.

## Разрешение сетевых соединений для службы Kaspersky Security Management Service

Названия параметров могут отличаться в разных операционных системах Windows.

Чтобы установить соединение между Консолью Kaspersky Embedded Systems Security 2.1 и службой Kaspersky Security Management Service, вам нужно разрешить сетевые соединения для службы через брандмауэр на защищаемом компьютере.

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

1. На защищаемом компьютере под управлением Windows выберите **Пуск → Панель управления → Безопасность → Брандмауэр Windows**.
2. В окне **Параметры брандмауэра Windows** выберите команду **Изменить параметры**.
3. На закладке **Исключения** в списке предустановленных исключений установите флажки **COM + Сетевой доступ**, **Windows Management Instrumentation (WMI)** и **Remote Administration**.
4. Нажмите на кнопку **Добавить программу**.
5. В диалоговом окне **Добавление программы** укажите файл kavfsgr.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке Kaspersky Embedded Systems Security 2.1.
6. Нажмите на кнопку **ОК**.

7. Нажмите на кнопку **ОК** в диалоговом окне **Параметры брандмауэра Windows**.

Сетевые соединения для службы Kaspersky Security Management Service будут разрешены.

## Действия после установки Kaspersky Embedded Systems Security 2.1

Kaspersky Embedded Systems Security 2.1 запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Embedded Systems Security 2.1 был выбран пункт **Включить постоянную защиту после установки программы** (настройка по умолчанию), Kaspersky Embedded Systems Security 2.1 проверяет объекты файловой системы компьютера при доступе к ним. Каждую пятницу в 20:00 Kaspersky Embedded Systems Security 2.1 выполняет задачу Проверка важных областей.

После установки Kaspersky Embedded Systems Security 2.1 рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз Kaspersky Embedded Systems Security 2.1. После установки Kaspersky Embedded Systems Security 2.1 проверяет объекты с использованием баз, которые входили в состав программы при поставке.

Рекомендуется сразу же обновить базы Kaspersky Embedded Systems Security 2.1, 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 2.1 на защищаемом компьютере не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.
- Настроить уведомления администратора о событиях Kaspersky Embedded Systems Security 2.1.

## В этом разделе

Настройка и запуск задачи обновления баз Kaspersky Embedded Systems Security 2.1.....	<a href="#">72</a>
Проверка важных областей .....	<a href="#">74</a>

## Настройка и запуск задачи обновления баз Kaspersky Embedded Systems Security 2.1

Чтобы обновить базы программы после установки, выполните следующие действия:

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

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

1. Запустите Консоль Kaspersky Embedded Systems Security 2.1 одним из следующих способов:
  - Откройте Консоль Kaspersky Embedded Systems Security 2.1 на защищаемом компьютере. Для этого выберите **Пуск → Программы → Kaspersky Embedded Systems Security 2.1 → Средства администрирования → Консоль Kaspersky Embedded Systems Security 2.1**.
  - Если вы запустили Консоль Kaspersky Embedded Systems Security 2.1 не на защищаемом компьютере, подключитесь к защищаемому компьютеру:
    - а. Откройте контекстное меню узла **Kaspersky Embedded Systems Security 2.1** в дереве Консоли.
    - б. Выберите пункт **Подключиться к другому компьютеру**.
    - с. В диалоговом 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 управления Kaspersky Security Management Service (см. раздел "О правах доступа к службе Kaspersky Security Management Service" на стр. [66](#)), укажите учетную запись, которая обладает этими правами.

Откроется окно Консоли Kaspersky Embedded Systems Security 2.1.

2. В дереве Консоли Kaspersky Embedded Systems Security 2.1 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 2.1 будет использовать для доступа к прокси-серверу учетную запись, указанную в параметрах задачи (по умолчанию задача выполняется 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 2.1 будет использовать для доступа к прокси-серверу учетную запись, указанную вами. Введите имя и пароль пользователя или выберите пользователя в списке.

- **Использовать имя и пароль пользователя**, чтобы выбрать обычную проверку подлинности (Basic authentication). 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 Kaspersky Embedded Systems Security 2.1 разверните узел **Обновление**.
2. В контекстном меню вложенного узла **Обновление баз программы** выберите пункт **Запустить**.

Задача Обновление баз программы будет запущена.

После того как задача успешно завершится, вы сможете посмотреть дату выпуска последних установленных обновлений баз в панели результатов узла **Kaspersky Embedded Systems Security 2.1**.

## Проверка важных областей

После того как вы обновили базы Kaspersky Embedded Systems Security 2.1, 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 Kaspersky Embedded Systems Security 2.1 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 2.1

Вы можете добавлять или удалять компоненты Kaspersky Embedded Systems Security 2.1. 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 Service не требуется.

Если доступ к управлению программой защищен паролем, Kaspersky Embedded Systems Security 2.1 запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов на дополнительном шаге Мастера.

► Чтобы изменить состав компонентов Kaspersky Embedded Systems Security 2.1, выполните следующие действия:

1. На защищаемом компьютере с установленным Kaspersky Embedded Systems Security 2.1 запустите файл программы-приветствия setup.exe.
2. В открывшемся окне в блоке **Установка** перейдите по ссылке **Установить Kaspersky Embedded Systems Security 2.1**.

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

3. Выберите пункт **Изменение состава компонентов программы**. Нажмите на кнопку **Далее**.

Откроется окно **Выборочная установка**.

4. В окне **Выборочная установка** в списке компонентов, доступных для использования, выберите компоненты, которые вы хотите добавить в Kaspersky Embedded Systems Security 2.1 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**.

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

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

Состав компонентов Kaspersky Embedded Systems Security 2.1 будет изменен в соответствии с заданными параметрами.

Если в работе Kaspersky Embedded Systems Security 2.1 возникли проблемы (Kaspersky Embedded Systems Security 2.1 завершается аварийно; задачи завершаются аварийно или не запускаются), вы можете попробовать восстановить Kaspersky Embedded Systems Security 2.1. Вы можете выполнить восстановление, сохранив текущие значения параметров Kaspersky Embedded Systems Security 2.1 или выбрать режим, при котором все параметры Kaspersky Embedded Systems Security 2.1 примут значения по умолчанию.

► *Чтобы восстановить Kaspersky Embedded Systems Security 2.1 после аварийного завершения работы программы или задач, выполните следующие действия:*

1. На защищаемом компьютере с установленным Kaspersky Embedded Systems Security 2.1 запустите файл программы-приветствия setup.exe.

2. В открывшемся окне в блоке **Установка** перейдите по ссылке **Установить Kaspersky Embedded Systems Security 2.1**.

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

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

Откроется окно **Восстановление установленных компонентов**.

4. В окне **Восстановление установленных компонентов** установите флажок **Восстановить рекомендуемые параметры работы программы**, если хотите сбросить настроенные параметры программы и восстановить Kaspersky Embedded Systems Security 2.1 с предустановленными параметрами по умолчанию. Нажмите на кнопку **Установить**.

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

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

Kaspersky Embedded Systems Security 2.1 будет восстановлен в соответствии с заданными параметрами.

## Удаление с помощью мастера установки

Этот раздел содержит инструкции для удаления Kaspersky Embedded Systems Security 2.1 и Консоли Kaspersky Embedded Systems Security 2.1 с защищаемого компьютера с помощью мастера установки.

### В этом разделе

Удаление Kaspersky Embedded Systems Security 2.1 .....	<a href="#">78</a>
Удаление Консоли Kaspersky Embedded Systems Security 2.1 .....	<a href="#">79</a>

# Удаление Kaspersky Embedded Systems Security 2.1

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Kaspersky Embedded Systems Security 2.1 с защищаемого компьютера с помощью мастера установки / удаления.

После удаления Kaspersky Embedded Systems Security 2.1 с защищаемого компьютера 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 пользователя (User Account Control), или доступ к управлению программой защищен паролем.

Если доступ к управлению программой защищен паролем, Kaspersky Embedded Systems Security 2.1 запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов на дополнительном шаге Мастера.

► *Чтобы удалить Kaspersky Embedded Systems Security 2.1, выполните следующие действия:*

1. В меню **Пуск** выберите пункт **Все программы** → **Kaspersky Embedded Systems Security 2.1** → **Изменение или удаление**.

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

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 карантин**, чтобы Kaspersky Embedded Systems Security 2.1 экспортировал объекты, помещенные на карантин. По умолчанию флажок снят.
- b. Установите флажок **Экспортировать объекты резервного хранилища**, чтобы Kaspersky Embedded Systems Security 2.1 экспортировал 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\2.1\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**.

Kaspersky Embedded Systems Security 2.1 будет удален с защищаемого компьютера.

## Удаление Консоли Kaspersky Embedded Systems Security 2.1

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Консоль Kaspersky Embedded Systems Security 2.1 с компьютера с помощью мастера установки / удаления.

После удаления Консоли Kaspersky Embedded Systems Security 2.1 перезагрузка компьютера не требуется.

► *Чтобы удалить Консоль Kaspersky Embedded Systems Security 2.1, выполните следующие действия:*

- 1. В меню **Пуск** выберите пункт **Все программы** → **Kaspersky Embedded Systems Security 2.1** → **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 2.1 из командной строки, примеры команд для установки и удаления Kaspersky Embedded Systems Security 2.1 из командной строки, примеры команд для добавления и удаления компонентов Kaspersky Embedded Systems Security 2.1 из командной строки.

## В этом разделе

Об установке и удалении Kaspersky Embedded Systems Security 2.1 из командной строки.....	<a href="#">81</a>
Примеры команд для установки Kaspersky Embedded Systems Security 2.1 .....	<a href="#">82</a>
Действия после установки Kaspersky Embedded Systems Security 2.1.....	<a href="#">84</a>
Добавление и удаление компонентов. Примеры команд.....	<a href="#">85</a>
Удаление Kaspersky Embedded Systems Security 2.1. Примеры команд.....	<a href="#">86</a>
Коды возврата .....	<a href="#">87</a>

## Об установке и удалении Kaspersky Embedded Systems Security 2.1 из командной строки

Вы можете устанавливать и удалять Kaspersky Embedded Systems Security 2.1, добавлять или удалять его компоненты, запустив из командной строки файлы инсталляционного пакета \product\less\_x86(x64).msi, указав параметры установки с помощью ключей.

Вы можете установить набор "Средства администрирования" на защищаемом компьютере или другом компьютере в сети, чтобы работать с Консолью Kaspersky Embedded Systems

Security 2.1 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, Kaspersky Embedded Systems Security 2.1 будет установлен с параметрами установки по умолчанию (см. стр. [46](#)).

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

## Примеры команд для установки Kaspersky Embedded Systems Security 2.1

В этом разделе приводятся примеры команд для установки Kaspersky Embedded Systems Security 2.1.

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

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

### Примеры команд установки Kaspersky Embedded Systems Security 2.1: запуск файла setup.exe

- Чтобы установить Kaspersky Embedded Systems Security 2.1 с параметрами установки по умолчанию в режиме без взаимодействия с пользователем, выполните следующую команду:

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

► *Чтобы установить Kaspersky Embedded Systems Security 2.1 со следующими параметрами:*

- установить только компоненты Постоянная защита файлов и Проверка по требованию;
- не запускать постоянную защиту при запуске Kaspersky Embedded Systems Security 2.1;
- 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 2.1 с параметрами установки по умолчанию, в режиме без взаимодействия с пользователем, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Embedded Systems Security 2.1 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 2.1 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 2.1 с предварительной проверкой активных процессов и загрузочных секторов локальных дисков компьютера, выполните следующую команду:*

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

► *Чтобы установить Kaspersky Embedded Systems Security 2.1, сохранив его 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 2.1; сохранить файл журнала установки с именем ess.log в папке, в которой хранится msi-файл*

инсталляционного пакета *Kaspersky Embedded Systems Security 2.1*, выполните следующую команду:

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

- Чтобы установить Консоль *Kaspersky Embedded Systems Security 2.1*, выполните следующую команду:

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

- Чтобы установить *Kaspersky Embedded Systems Security 2.1* с активацией с помощью файла ключа *C:\0000000A.key*; настроить *Kaspersky Embedded Systems Security 2.1* 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
```

## См. также

Действия после установки *Kaspersky Embedded Systems Security 2.1* ..... [84](#)

Параметры установки и удаления и их ключи для службы Windows Installer ..... [46](#)

# Действия после установки *Kaspersky Embedded Systems Security 2.1*

*Kaspersky Embedded Systems Security 2.1* запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки *Kaspersky Embedded Systems Security 2.1* вы выбрали пункт **Включить постоянную защиту после установки программы**, *Kaspersky Embedded Systems Security 2.1* проверяет объекты файловой системы компьютера при доступе к ним. Каждую пятницу в 20:00 *Kaspersky Embedded Systems Security 2.1* выполняет задачу Проверка важных областей.

После установки *Kaspersky Embedded Systems Security 2.1* рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз *Kaspersky Embedded Systems Security 2.1*. После установки *Kaspersky Embedded Systems Security 2.1* проверяет объекты с

использованием баз, которые входили в его состав при поставке. Рекомендуется сразу же обновить базы Kaspersky Embedded Systems Security 2.1. 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 2.1 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) под учетной записью (имя пользователя: inetuser; пароль: 123456).

- Выполнить проверку важных областей компьютера, если перед установкой Kaspersky Embedded Systems Security 2.1 на защищаемом компьютере не было установлено антивирусной программы 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 2.1.

## Добавление и удаление компонентов. Примеры команд

Компонент Проверка по требованию устанавливается автоматически. Вам не нужно указывать его в списке значений ключа ADDLOCAL, добавляя или удаляя компоненты Kaspersky Embedded Systems Security 2.1.

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

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

или

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

Если вы укажете не только компоненты, которые хотите установить, но и уже установленные компоненты, Kaspersky Embedded Systems Security 2.1 переустановит указанные установленные компоненты.

- Чтобы удалить установленные компоненты, выполните следующую команду:

```
msiexec /i ess.msi REMOVE=AppCtrl,WiFiControl /qn EULA=1  
PRIVACYPOLICY=1
```

## Удаление Kaspersky Embedded Systems Security 2.1. Примеры команд

- Чтобы удалить Kaspersky Embedded Systems Security 2.1 с защищаемого компьютера, выполните следующую команду:

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

- Чтобы удалить Консоль Kaspersky Embedded Systems Security 2.1, выполните следующую команду:

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

- Чтобы удалить Kaspersky Embedded Systems Security 2.1 и Консоль Kaspersky Embedded Systems Security 2.1 с защищаемого компьютера, на котором установлен пароль, выполните следующую команду:

- Для x86-разрядной операционной системы:

```
msiexec.exe /x {36661EA4-38DA-48C1-B12F-B161554D634E}  
UNLOCK_PASSWORD=*** /qn
```

- Для x64-разрядной операционной системы:

```
msiexec.exe /x {033D9279-093E-4A17-A00A-7E6A012692CE}
```

```
UNLOCK_PASSWORD=*** /qn
```

- Чтобы удалить Консоль Kaspersky Embedded Systems Security 2.1 с защищаемого компьютера, на котором установлен пароль, выполните следующую команду:

- Для x86-разрядной операционной системы:

```
msiexec.exe /x {2B789CD8-3381-4D62-BD4D-A9066C8136E6}  
UNLOCK_PASSWORD=*** /qn
```

- Для x64-разрядной операционной системы:

```
msiexec.exe /x {40AD72B7-0B70-496F-9012-8FE81DB0F448}  
UNLOCK_PASSWORD=*** /qn
```

- Чтобы удалить плагин Kaspersky Embedded Systems Security 2.1 с защищаемого компьютера, на котором установлен пароль, выполните следующую команду:

```
msiexec.exe /x {DA15CF4A-75FF-4C92-AFC2-0A16DC645D2E}  
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 программы Kaspersky Embedded Systems Security 2.1. Чтобы установить программу, запустите мастер установки с правами локального администратора.
25003	Kaspersky Embedded Systems Security 2.1 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 следующие программы с защищаемого компьютера: <список несовместимого ПО>.
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 общие сведения об установке Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center, описание процедуры установки и удаления Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center, а также описание действий после установки Kaspersky Embedded Systems Security 2.1.

## В этом разделе

Общие сведения об установке через Kaspersky Security Center .....	<a href="#">89</a>
Права для установки или удаления Kaspersky Embedded Systems Security 2.1 .....	<a href="#">90</a>
Процедура установки Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center .....	<a href="#">91</a>
Действия после установки Kaspersky Embedded Systems Security 2.1 .....	<a href="#">93</a>
Установка Консоли Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center .....	<a href="#">94</a>
Удаление Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center .....	<a href="#">96</a>

## Общие сведения об установке через Kaspersky Security Center

Вы можете установить Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center с помощью задачи удаленной установки.

После выполнения задачи удаленной установки Kaspersky Embedded Systems Security 2.1 будет установлен с одинаковыми параметрами на нескольких компьютерах.

Вы можете объединить компьютеры в одну группу администрирования и создать групповую задачу для установки Kaspersky Embedded Systems Security 2.1 на компьютерах этой группы.

Вы можете создать задачу удаленной установки Kaspersky Embedded Systems Security 2.1 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 2.1.

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

## Права для установки или удаления Kaspersky Embedded Systems Security 2.1

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 2.1, 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 2.1 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 2.1, 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**.

## Процедура установки Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center

Подробная информация о формировании инсталляционного пакета и создании задачи удаленной установки содержится в *Справочной системе Kaspersky Security Center*.

Если вы планируете в дальнейшем управлять Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center, убедитесь, что выполняются следующие условия:

- На компьютере с установленным Сервером администрирования Kaspersky Security Center установлен плагин управления Kaspersky Embedded Systems Security 2.1 (файл \product\klcfginst.exe комплекта поставки Kaspersky Embedded Systems Security 2.1).
- На защищаемых компьютерах установлен Агент администрирования Kaspersky Security Center. Если на защищаемых компьютерах не установлен Агент администрирования Kaspersky Security Center, вы можете установить его вместе с Kaspersky Embedded Systems Security 2.1 в задаче 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 2.1 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** создайте новый инсталляционный пакет.
3. Введите имя инсталляционного пакета.
4. Выберите файл ess.kud из комплекта поставки Kaspersky Embedded Systems Security 2.1 в качестве файла инсталляционного пакета.

Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.

5. Если вы прочли Лицензионное соглашение и Политику конфиденциальности, установите флажки, свидетельствующие, что вы принимаете **положения и условия настоящего Лицензионного соглашения и Политику конфиденциальности, которая описывает обработку данных** для продолжения установки.

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

6. Если требуется, в свойствах созданного инсталляционного пакета измените набор устанавливаемых компонентов Kaspersky Embedded Systems Security 2.1 (см. раздел "Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security 2.1" на стр. [75](#)), Если требуется, измените параметры установки по умолчанию (см. раздел "Параметры установки и удаления и их ключи для службы Windows Installer" на стр. [46](#)).

В Kaspersky Security Center разверните узел **Удаленная установка** и во вложенном узле **Инсталляционные пакеты** в рабочей области откройте контекстное меню созданного инсталляционного пакета Kaspersky Embedded Systems Security 2.1 и выберите команду **Свойства**. В окне **Свойства: <название инсталляционного пакета>** в разделе **Настройка** выполните следующие действия:

- а. В группе параметров **Устанавливаемые компоненты** установите флажки рядом с названиями компонентов Kaspersky Embedded Systems Security 2.1, 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 сервере, 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".

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

7. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Kaspersky Embedded Systems Security 2.1 на выбранные компьютеры (группу администрирования). Настройте параметры задачи.

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

8. Запустите созданную задачу удаленной установки Kaspersky Embedded Systems Security 2.1.

Kaspersky Embedded Systems Security 2.1 будет установлен на указанные в задаче компьютеры.

## Действия после установки Kaspersky Embedded Systems Security 2.1

После установки Kaspersky Embedded Systems Security 2.1 рекомендуется обновить базы Kaspersky Embedded Systems Security 2.1 на компьютерах, а также выполнить проверку важных областей компьютеров, если до установки Kaspersky Embedded Systems Security 2.1

на компьютерах не были установлены антивирусные программы с включенной функцией постоянной защиты.

Если компьютеры, на которых вы установили Kaspersky Embedded Systems Security 2.1, объединены в одной группе администрирования Kaspersky Security Center, вы можете выполнить эти задачи следующими способами:

1. Создать задачу обновления баз программы для группы компьютеров, на которых вы установили Kaspersky Embedded Systems Security 2.1. 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** отключить 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 2.1.

## Установка Консоли Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center

Подробная информация о создании инсталляционного пакета и задачи удаленной установки содержится в *Справочной системе Kaspersky Security Center*.

- Чтобы установить Консоль Kaspersky Embedded Systems Security 2.1 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 2.1 и установите флажок **Копировать всю папку 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 Kaspersky Embedded Systems Security 2.1, не устанавливая файла справки и документации, выполните следующую команду:

```
/s /p EULA=1 "ADDLOCAL=MmcSnapin INSTALLDIR=c:\KasperskyC  
onsole EULA=1 PRIVACYPOLICY=1 "
```

2. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Консоли Kaspersky Embedded Systems Security 2.1 на выбранные компьютеры (группу администрирования). Настройте параметры задачи.

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

3. Запустите созданную задачу удаленной установки.

Консоль Kaspersky Embedded Systems Security 2.1 будет установлена на указанных в задаче компьютерах.

# Удаление Kaspersky Embedded Systems Security 2.1 через Kaspersky Security Center

Если доступ к управлению Kaspersky Embedded Systems Security 2.1 на компьютерах сети защищен паролем, введите пароль при создании задачи группового удаления программ. Если защита паролем не управляется политикой Kaspersky Security Center централизованно, Kaspersky Embedded Systems Security 2.1 будет успешно удален на компьютерах, где доступ к управлению программой защищен паролем, совпавшим с введенным значением. Kaspersky Embedded Systems Security 2.1 на других компьютерах удален не будет.

► *Чтобы удалить Kaspersky Embedded Systems Security 2.1 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 2.1 только с параметрами удаления по умолчанию (см. раздел "Параметры установки и удаления и их ключи для службы Windows Installer" на стр. [46](#)).



# Установка и удаление программы через групповые политики Active Directory

Этот раздел содержит описание установки и удаления Kaspersky Embedded Systems Security 2.1 через групповые политики Active Directory, а также информацию о действиях после установки Kaspersky Embedded Systems Security 2.1 через групповые политики Active Directory.

## В этом разделе

Установка Kaspersky Embedded Systems Security 2.1 через групповые политики Active Directory .....	<a href="#">97</a>
Действия после установки Kaspersky Embedded Systems Security 2.1 .....	<a href="#">99</a>
Удаление Kaspersky Embedded Systems Security 2.1 через групповые политики Active Directory .....	<a href="#">99</a>

## Установка Kaspersky Embedded Systems Security 2.1 через групповые политики Active Directory

Вы можете установить Kaspersky Embedded Systems Security 2.1 на нескольких компьютерах через групповую политику Active Directory. Таким же образом вы можете установить Консоль Kaspersky Embedded Systems Security 2.1.

Компьютеры, на которых вы хотите установить Kaspersky Embedded Systems Security 2.1 или Консоль Kaspersky Embedded Systems Security 2.1 должны быть в одном домене и в одной организационной единице.

Операционные системы на компьютерах, на которых вы хотите установить Kaspersky Embedded Systems Security 2.1 с помощью политики, должны быть одной разрядности (32-разрядные или 64-разрядные).

Вы должны обладать правами администратора домена.

Чтобы установить Kaspersky Embedded Systems Security 2.1, используйте инсталляционные пакеты ess\_x86(x64).msi. Чтобы установить Консоль Kaspersky Embedded Systems Security 2.1, используйте инсталляционный пакет esstools.msi.

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

► *Чтобы установить Kaspersky Embedded Systems Security 2.1 (Консоль Kaspersky Embedded Systems Security 2.1), 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, в которую объединены компьютеры.
3. С помощью **Group Policy Object Editor** создайте новый инсталляционный пакет в узле **Конфигурация компьютеров**. Укажите путь к msi-файлу инсталляционного пакета Kaspersky Embedded Systems Security 2.1 (Консоли Kaspersky Embedded Systems Security 2.1) в формате UNC (Universal Naming Convention).
4. Установите флажок **Always install with elevated privileges** службы Windows Installer, 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 2.1 будет установлен на компьютерах группы после их перезагрузки, перед входом в Microsoft Windows.

# Действия после установки Kaspersky Embedded Systems Security 2.1

После установки Kaspersky Embedded Systems Security 2.1 на защищаемых компьютерах рекомендуется сразу обновить базы программы и выполнить проверку важных областей компьютера. Вы можете выполнить эти действия из Консоли Kaspersky Embedded Systems Security 2.1 (см. раздел "Действия после установки Kaspersky Embedded Systems Security 2.1" на стр. [71](#)).

Вы можете также настроить уведомления администратора о событиях Kaspersky Embedded Systems Security 2.1.

## Удаление Kaspersky Embedded Systems Security 2.1 через групповые политики Active Directory

Если вы устанавливали Kaspersky Embedded Systems Security 2.1 или Консоль программы на компьютерах группы, используя групповую политику Active Directory, вы можете использовать эту политику, чтобы удалить Kaspersky Embedded Systems Security 2.1 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 2.1 через групповые политики Active Directory невозможно.

► *Чтобы удалить Kaspersky Embedded Systems Security 2.1 (Консоль Kaspersky Embedded Systems Security 2.1), выполните следующие действия:*

1. На контроллере домена выберите организационную единицу, с компьютеров которой вы хотите удалить Kaspersky Embedded Systems Security 2.1 или Консоль Kaspersky Embedded Systems Security 2.1.

2. Выберите политику, созданную для установки Kaspersky Embedded Systems Security 2.1, и в **Редакторе групповых политик**, в узле **Software Installation** (**Конфигурация компьютеров** → **Конфигурация программ** → **Software Installation**) откройте контекстное меню инсталляционного пакета Kaspersky Embedded Systems Security 2.1 (Консоли Kaspersky Embedded Systems Security 2.1) и выберите команду **Все задачи** → **Удалить**.
3. Выберите метод удаления **Немедленно удалить программу со всех компьютеров**.
4. Примените изменения с помощью команды `gpupdate / force`.

Kaspersky Embedded Systems Security 2.1 будет удален с компьютеров после их перезагрузки, перед входом в Microsoft Windows.

## Проверка функций Kaspersky Embedded Systems Security 2.1. Использование тестового вируса EICAR

Этот раздел содержит описание тестового вируса EICAR и процедуру проверки функций Kaspersky Embedded Systems Security 2.1 Постоянная защита и Проверка по требованию с помощью тестового вируса EICAR.

### В этом разделе

О тестовом вирусе EICAR.....	<a href="#">100</a>
Проверка функций Kaspersky Embedded Systems Security 2.1 Постоянная защита и Проверка по требованию .....	<a href="#">102</a>

## 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. Вы можете загрузить его со страницы сайта **EICAR** [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](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 2.1 обнаруживает в этой текстовой строке тестовую угрозу, присваивает файлу статус **Зараженный** и удаляет его. Информация об обнаруженной в файле угрозе появляется в Консоли Kaspersky Embedded Systems Security 2.1, в журнале выполнении задачи.

Вы также можете использовать файл eicar.com, чтобы проверить, как Kaspersky Embedded Systems Security 2.1 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 2.1 обработал файл eicar.com с префиксом, в блоке параметров безопасности **Защита объектов** установите значение **Все объекты** для задач Kaspersky Embedded Systems Security 2.1 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 2.1
Без префикса	Kaspersky Embedded Systems Security 2.1 присваивает объекту статус <b>Зараженный</b> и удаляет его.
SUSP–	Kaspersky Embedded Systems Security 2.1 присваивает объекту статус <b>Возможно зараженный</b> (обнаружен с помощью эвристического анализатора) и удаляет его (возможно зараженные объекты не подвергаются лечению).
WARN–	Kaspersky Embedded Systems Security 2.1 присваивает объекту статус <b>Возможно зараженный</b> (код объекта частично совпадает с известным вредоносным кодом) и удаляет его (возможно зараженные объекты не подвергаются лечению).
CURE–	Kaspersky Embedded Systems Security 2.1 присваивает объекту статус <b>Зараженный</b> и лечит его. Если лечение успешно, весь текст в файле заменяется словом "CURE".

## Проверка функций Kaspersky Embedded Systems Security 2.1 Постоянная защита и Проверка по требованию

После установки Kaspersky Embedded Systems Security 2.1 вы можете убедиться, что Kaspersky Embedded Systems Security 2.1 обнаруживает объекты, содержащие вредоносный код. Для проверки вы можете использовать тестовый вирус **EICAR** (см. раздел "**О тестовом вирусе EICAR**" на стр. [100](#)).

► Чтобы проверить функцию Постоянная защита, выполните следующие действия:

1. Загрузите файл eicar.com со страницы сайта **EICAR** [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](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 также проверить работу уведомлений пользователей сети, убедитесь в том, что и на защищаемом компьютере, и на компьютере, на котором вы сохранили файл eicar.com, включена Служба сообщений Microsoft Windows.
3. Откройте Консоль Kaspersky Embedded Systems Security 2.1.
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 программы "Подключение к удаленному рабочему столу" (Remote Desktop Connection).
  - 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 диска защищаемого компьютера.
- В Консоли Kaspersky Embedded Systems Security 2.1 журнал выполнения задачи получил статус **Критический**. В журнале появилась строка с информацией об угрозе в файле eicar.com. (Чтобы просмотреть журнал выполнения задачи, в дереве Консоли Kaspersky Embedded Systems Security 2.1 разверните узел **Постоянная защита**, выберите задачу Постоянная защита файлов и в панели результатов узла перейдите по ссылке **Открыть журнал выполнения**).

- Появилось сообщение Службы сообщений Microsoft Windows на компьютере, с которого вы скопировали файл следующего содержания: "Kaspersky Embedded Systems Security 2.1 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 объекта: <имя пользователя>. Имя компьютера пользователя объекта: <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 Проверка по требованию, выполните следующие действия:*

1. Загрузите файл eicar.com со страницы сайта **EICAR** [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](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 Kaspersky Embedded Systems Security 2.1.
3. Выполните следующие действия:
  - a. В дереве Консоли Kaspersky Embedded Systems Security 2.1 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).



е. Установите флажок, чтобы включить добавленный сетевой путь в область проверки.

ф. Запустите задачу Проверка важных областей.

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

- Файл eicar.com удален с диска компьютера.
- В Консоли Kaspersky Embedded Systems Security 2.1 журнал выполнения задачи получил 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 Kaspersky Embedded Systems Security 2.1 разверните узел **Проверка по требованию**, выберите вложенный узел **Проверка важных областей** и в панели результатов узла перейдите по ссылке **Открыть журнал выполнения**.

## Миграция параметров из Kaspersky Embedded Systems Security 1.1

Вы можете установить Kaspersky Embedded Systems Security 2.1 без удаления предыдущей версии программы, если на вашем компьютере установлена версия программы Kaspersky Embedded Systems Security 1.1.

При переходе с Kaspersky Embedded Systems Security 1.1 на Kaspersky Embedded Systems Security 2.1 все локальные параметры программы сохраняются без изменения.

При обновлении программы до Kaspersky Embedded Systems Security 2.1 может потребоваться перезагрузка компьютера.

Подробная информация о миграции параметров содержится в текстовом документе migration.txt, который входит в комплект поставки *Kaspersky Embedded Systems Security 2.1*.

---

# Интерфейс программы

Вы можете управлять Kaspersky Embedded Systems Security 2.1 через локальную Консоль и плагин управления Kaspersky Security Center. Действия с локальной Консолью описаны в *Руководстве пользователя Kaspersky Embedded Systems Security 2.1*. Действия с плагином управления осуществляются в интерфейсе Консоли администрирования Kaspersky Security Center. Подробная информация об интерфейсе Kaspersky Security Center содержится в документации для Kaspersky Security Center.

---

# Лицензирование программы

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

## В этом разделе

О Лицензионном соглашении .....	<a href="#">107</a>
О лицензии .....	<a href="#">108</a>
О лицензионном сертификате .....	<a href="#">109</a>
О ключе .....	<a href="#">110</a>
О коде активации .....	<a href="#">110</a>
О файле ключа .....	<a href="#">111</a>
О предоставлении данных .....	<a href="#">111</a>
Активация программы с помощью ключа .....	<a href="#">113</a>
Просмотр информации о действующей лицензии .....	<a href="#">114</a>
Продление срока действия лицензии .....	<a href="#">118</a>
Удаление ключа .....	<a href="#">119</a>

## 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 2.1.
- 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 предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Программа активируется с помощью файла ключа приобретаемой *коммерческой лицензии*.

Коммерческая – платная лицензия, предоставляемая при приобретении программы.

Kaspersky Embedded Systems Security 2.1 предусматривает два типа коммерческих лицензий:

- Стандартная лицензия **Kaspersky Embedded Systems Security 2.1**.
- Расширенная лицензия **Kaspersky Embedded Systems Security 2.1 Compliance Edition**, которая включает в себя два дополнительных компонента для диагностики 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 2.1). Чтобы продолжить использование Kaspersky Embedded Systems Security 2.1 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

## О лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

## 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 пробной или 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.

Ключ для пробной лицензии может быть добавлен только в качестве активного ключа. Ключ для пробной лицензии не может быть добавлен в качестве дополнительного ключа.

## О коде активации

*Код активации* – это код, который вы получаете, приобретая коммерческую лицензию Kaspersky Embedded Systems Security 2.1. Этот код требуется для получения файла ключа и активации программы установкой файла ключа.

Код активации представляет собой последовательность из двадцати цифр и латинских букв в формате xxxxx-xxxxx-xxxxx-xxxxx.

Отсчет срока действия лицензии начинается с момента активации программы. Если вы приобрели лицензию, предназначенную для использования Kaspersky Embedded Systems Security 2.1 на нескольких компьютерах, то отсчет срока действия лицензии начинается с момента активации программы на первом из компьютеров.

Если код активации был потерян или случайно удален после активации, то для его восстановления требуется отправить запрос в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на стр. [405](#)).

## 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 2.1 или после заказа пробной версии Kaspersky Embedded Systems Security 2.1.

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:

- Обратиться в Службу технической поддержки (<http://support.kaspersky.ru>).
- Получить файл ключа на веб-сайте "Лаборатории Касперского" (<https://activation.kaspersky.com/ru/>) на основе имеющегося кода активации.

## О предоставлении данных

Лицензионное соглашение для Kaspersky Embedded System Security 2.1, 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](http://www.kaspersky.ru/Products-and-Services-Privacy-Policy).

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

- Для обеспечения механизма получения обновлений - информацию об установленной программе и активации программы: идентификатор устанавливаемой программы и ее полную версию, включая номер сборки, тип и идентификатор лицензии, идентификатор установки, 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.

## Локальная обработка данных

В процессе выполнения основных функций программы, описанных в настоящем Руководстве, Kaspersky Embedded System Security 2.1 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;
- информация о сетевой активности, в том числе IP-адреса заблокированных клиентских компьютеров.

Kaspersky Embedded System Security 2.1 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 System Security 2.1 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, содержится в соответствующих разделах настоящего Руководства.

## Активация программы с помощью ключа

Вы можете активировать Kaspersky Embedded Systems Security 2.1, применив ключ.

Если в Kaspersky Embedded Systems Security 2.1 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 2.1 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 2.1 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 2.1 с помощью ключа, выполните следующие действия:

1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 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 статуса лицензии

Информация о статусе действующей лицензии отображается в панели результатов узла **Kaspersky Embedded Systems Security 2.1** Консоли Kaspersky Embedded Systems Security 2.1. Статус лицензии может принимать следующие значения:

- **Выполняется проверка статуса лицензии** – Kaspersky Embedded Systems Security 2.1 проверяет добавленный файл ключа или код активации и ожидает ответа о текущем статусе лицензии.
- **Действующая лицензия: до <дата окончания действия лицензии>** – Kaspersky Embedded Systems Security 2.1 активирован до указанной даты. Статус лицензии 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** – Kaspersky Embedded Systems Security 2.1 не активирован, так как не добавлен ключ или код активации. Статус выделен красным цветом.
- **Срок действия лицензии истек** – Kaspersky Embedded Systems Security 2.1 не активирован, так как истек период действия лицензии. Статус выделен красным цветом.
- **Нарушено Лицензионное соглашение** – Kaspersky Embedded Systems Security 2.1 не активирован, так как нарушены условия Лицензионного соглашения (см. раздел "О Лицензионном соглашении" на стр. [107](#)). Статус выделен красным цветом.
- **Ключ помещен в черный список** – добавленный ключ заблокирован и помещен в черный список специалистами "Лаборатории Касперского", например, если ключ был использован сторонними лицами для незаконной активации программы. Статус выделен красным цветом.

## Просмотр информации о действующей лицензии

► *Чтобы просмотреть информацию о действующей лицензии,*

в дереве Консоли Kaspersky Embedded Systems Security 2.1 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
<b>Код активации</b>	Номер кода активации. Поле заполняется, если вы активируете программу с помощью кода активации.
<b>Статус активации</b>	<p>Информация о статусе активации программы. Информация в графе <b>Статус активации</b> в панели управления узла <b>Лицензирование</b> может принимать следующие значения:</p> <ul style="list-style-type: none"> <li>• <b>Применено</b> – если вы активировали программу с помощью кода активации или ключа.</li> <li>• <b>Активация</b> – если вы применили код активации для активации программы и процесс активации еще не закончен. Статус принимает значение <b>Применено</b> по завершении активации программы и после обновления содержимого панели результатов узла.</li> <li>• <b>Ошибка активации</b> – если не удалось активировать программу. Вы можете посмотреть причину неудачного завершения активации в журнале выполнения задач.</li> </ul>
<b>Ключ</b>	Номер ключа, с помощью которого вы активировали программу.
<b>Тип лицензии</b>	Тип лицензии: коммерческая.
<b>Дата окончания срока действия</b>	Дата окончания срока действия лицензии по активному ключу.
<b>Статус кода активации или ключа</b>	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 2.1 (см. таблицу ниже).

Таблица 16. Подробная информация о лицензии в окне **Свойства <Номер ключа>**

Поле	Описание
<b>Закладка Общие</b>	
<b>Ключ</b>	Номер ключа, с помощью которого вы активировали программу.
<b>Дата добавления ключа</b>	Дата добавления ключа в программу.
<b>Тип лицензии</b>	Тип лицензии: коммерческая.
<b>Истекает через (сут)</b>	Число суток, оставшихся до даты окончания срока действия лицензии по активному ключу.
<b>Дата окончания срока действия</b>	Дата окончания срока действия лицензии по активному ключу. Если вы активируете программу по неограниченной подписке, в поле указывается значение <i>Не ограничена</i> . Если Kaspersky Embedded Systems Security 2.1 не удастся определить дату окончания действия лицензии, указывается значение <i>Неизвестна</i> .
<b>Программа</b>	Название программы, для которой добавлен ключ или код активации.
<b>Ограничение на использование ключа</b>	Предусмотренное ограничение на использование ключа (если имеется).
<b>Осуществление технической поддержки</b>	Информация о том, оказывает ли "Лаборатория Касперского" или ее партнер техническую поддержку заказчику по условиям предоставления лицензии.
<b>Закладка Дополнительно</b>	
<b>Информация о лицензии</b>	Номер и тип действующей лицензии.

<b>Информация о поддержке</b>	Контактная информация "Лаборатории Касперского" или партнера, который осуществляет техническую поддержку. Поле может быть пустым, если техническая поддержка не осуществляется.
<b>Информация о владельце</b>	Информация о заказчике лицензии: имя заказчика и название организации, для которой приобретена лицензия.

## 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 статус **Действующая лицензия: до <дата окончания действия лицензии>** в панели результатов узла **Kaspersky Embedded Systems Security 2.1** выделяется желтым цветом.

Вы можете продлить срок действия лицензии, не дожидаясь его окончания, с помощью добавления дополнительного кода активации или ключа. Это позволяет не прерывать защиту компьютера 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 Kaspersky Embedded Systems Security 2.1 откройте узел **Лицензирование**.
3. В панели результатов узла **Лицензирование** выполните одно из следующих действий:
  - Если вы хотите продлить срок действия лицензии с помощью дополнительного ключа:
    - а. Перейдите по ссылке **Добавить ключ**.
    - б. В открывшемся окне нажмите на кнопку **Обзор** и выберите новый файл ключа с расширением key.
    - с. 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 **ОК**.

Дополнительный ключ или код активации будет добавлен и автоматически станет активным по истечении срока действия используемого ключа или кода активации Kaspersky Embedded Systems Security 2.1.

## Удаление ключа

Вы можете удалить добавленный ключ из программы.

Если в Kaspersky Embedded Systems Security 2.1 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 Kaspersky Embedded Systems Security 2.1 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 Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о запуске плагина управления Kaspersky Embedded Systems Security 2.1, а также запуске и остановке службы Kaspersky Security Service.

## В этом разделе

Запуск плагина управления Kaspersky Security Center .....	<a href="#">120</a>
Запуск и остановка службы Kaspersky Security Service.....	<a href="#">120</a>

## Запуск плагина управления Kaspersky Security Center

Запуск плагина управления Kaspersky Security Center, в котором осуществляется работа с Kaspersky Embedded Systems Security 2.1, не требует дополнительных действий. После установки плагина на компьютер администратора, запуск происходит одновременно с Kaspersky Security Center. Подробная информация о запуске Kaspersky Security Center содержится в *Справочной системе Kaspersky Security Center*.

## Запуск и остановка службы Kaspersky Security Service

По умолчанию служба Kaspersky Security Service запускается автоматически при старте операционной системы. Служба Kaspersky Security Service управляет рабочими процессами, в которых выполняются задачи постоянной защиты, контроля компьютера, проверки по требованию и обновления.



По умолчанию при запуске службы Kaspersky Security Service запускаются задачи Постоянная защита файлов, Проверка при старте операционной системы, Проверка целостности программы, а также другие задачи, в расписании которых указана частота запуска **При запуске программы**.

Если вы остановите службу Kaspersky Security Service, все выполняющиеся задачи будут остановлены. После того как вы снова запустите службу Kaspersky Security Service, 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 Service с помощью контекстного меню узла **Kaspersky Embedded Systems Security 2.1** или с помощью оснастки **Службы** Microsoft Windows.

Вы можете запускать и останавливать Kaspersky Embedded Systems Security 2.1, если вы входите в группу "Администраторы" на защищаемом сервере.

- *Чтобы остановить или запустить программу с помощью Консоли управления, выполните следующие действия:*
1. В дереве Консоли Kaspersky Embedded Systems Security 2.1 откройте контекстное меню узла **Kaspersky Embedded Systems Security 2.1**.
  2. Выберите одну из следующих команд:
    - **Остановить Kaspersky Embedded Systems Security 2.1**, чтобы остановить службу Kaspersky Security Service;
    - **Запустить Kaspersky Embedded Systems Security 2.1**, чтобы запустить службу Kaspersky Security Service.

Служба Kaspersky Security Service будет запущена или остановлена.

---

# Права доступа к функциям Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о правах на управление Kaspersky Embedded Systems Security 2.1 и службами Windows, которые регистрирует программа, а также инструкции по настройке этих прав.

## В этом разделе

О правах на управление Kaspersky Embedded Systems Security 2.1.....	<a href="#">122</a>
О правах на управление службой Kaspersky Security Service .....	<a href="#">125</a>
О правах доступа к службе Kaspersky Security Management .....	<a href="#">128</a>
Настройка прав доступа на управление Kaspersky Embedded Systems Security 2.1 и службой Kaspersky Security Service .....	<a href="#">129</a>
Защита доступа к функциям Kaspersky Embedded Systems Security 2.1 с помощью пароля.....	<a href="#">132</a>
Разрешение сетевых соединений для службы Kaspersky Security Management Service .....	<a href="#">135</a>

## О правах на управление Kaspersky Embedded Systems Security 2.1

По умолчанию доступ ко всем функциям Kaspersky Embedded Systems Security 2.1 имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере, пользователи группы ESS Administrators, созданной на защищаемом компьютере при установке Kaspersky Embedded Systems Security 2.1, а также системная группа SYSTEM.

Вы не можете удалять учетную запись пользователя SYSTEM, а также редактировать права данной учетной записи. Если в учетную запись SYSTEM были внесены изменения, при сохранении настроек будут восстановлены максимальные права данной учетной записи.

Пользователи, которые имеют доступ к функции **Изменение прав** Kaspersky Embedded Systems Security 2.1, могут предоставлять доступ к функциям Kaspersky Embedded Systems Security 2.1 другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Если пользователь не зарегистрирован в списке пользователей Kaspersky Embedded Systems Security 2.1, он не может открыть Консоль Kaspersky Embedded Systems Security 2.1.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Embedded Systems Security 2.1 один из следующих предустановленных уровней доступа к функциям Kaspersky Embedded Systems Security 2.1:

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры работы Kaspersky Embedded Systems Security 2.1, параметры работы компонентов Kaspersky Embedded Systems Security 2.1, права пользователей Kaspersky Embedded Systems Security 2.1, а также просматривать статистику работы Kaspersky Embedded Systems Security 2.1.
- **Изменение** – доступ ко всем функциям программы, кроме изменения прав пользователей: возможность просматривать и изменять общие параметры работы Kaspersky Embedded Systems Security 2.1, параметры работы компонентов Kaspersky Embedded Systems Security 2.1.
- **Чтение** – возможность просматривать общие параметры работы Kaspersky Embedded Systems Security 2.1, параметры работы компонентов Kaspersky Embedded Systems Security 2.1, статистику работы Kaspersky Embedded Systems Security 2.1 и права пользователей Kaspersky Embedded Systems Security 2.1.

Также вы можете выполнять расширенную настройку прав доступа: разрешать или запрещать доступ к отдельным функциям Kaspersky Embedded Systems Security 2.1.

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 2.1

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Embedded Systems Security 2.1.
Создание и удаление задач	Возможность создавать и удалять задачи проверки по требованию.
Изменение параметров	Возможность импортировать из конфигурационного файла параметры работы Kaspersky Embedded Systems Security 2.1.
Чтение параметров	Возможности: <ul style="list-style-type: none"> <li>• просматривать общие параметры работы Kaspersky Embedded Systems Security 2.1 и параметры задач;</li> <li>• экспортировать в конфигурационный файл параметры работы Kaspersky Embedded Systems Security 2.1;</li> <li>• просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.</li> </ul>
Управление хранилищами	Возможности: <ul style="list-style-type: none"> <li>• помещать объекты на карантин;</li> <li>• удалять объекты из карантина и резервного хранилища;</li> <li>• восстанавливать объекты из карантина и резервного хранилища.</li> </ul>
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 2.1.

Лицензирование программы	Возможность активировать и деактивировать Kaspersky Embedded Systems Security 2.1.
Удаление программы	Возможность удалять Kaspersky Embedded Systems Security 2.1.
Чтение прав	Возможность просматривать список пользователей Kaspersky Embedded Systems Security 2.1 и права доступа каждого пользователя.
Изменение прав	<p>Возможности:</p> <ul style="list-style-type: none"> <li>• изменять список пользователей, имеющих доступ к управлению программой;</li> <li>• изменять права доступа пользователей к функциям Kaspersky Embedded Systems Security 2.1.</li> </ul>

## О правах на управление службой Kaspersky Security Service

При установке Kaspersky Embedded Systems Security 2.1 регистрирует в Windows службу Kaspersky Security Service (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 через управление Kaspersky Security Service, вы можете ограничивать права на управление службой Kaspersky Security Service с помощью локальной Консоли Kaspersky Embedded Systems Security 2.1 или плагина управления Kaspersky Security Center.

По умолчанию доступ к управлению Kaspersky Security Service 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 удалять учетную запись пользователя SYSTEM, а также редактировать права данной учетной записи. Если в учетную запись SYSTEM были внесены изменения, при сохранении настроек будут восстановлены максимальные права данной учетной записи.

Пользователи, которые имеют доступ к функции уровня **Изменение прав** (см. раздел "**О правах на управление Kaspersky Embedded Systems Security 2.1**" на стр. [122](#)), могут предоставлять доступ к управлению Kaspersky Security Service другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Embedded Systems Security 2.1 один из следующих предустановленных уровней доступа на управление Kaspersky Security Service:

- **Полный контроль** – возможность просматривать и изменять общие параметры работы и права пользователей Kaspersky Security Service, а также запускать и останавливать работу Kaspersky Security Service.
- **Чтение** – возможность просматривать общие параметры работы и права пользователей Kaspersky Security Service.
- **Изменение** – возможность просматривать и изменять общие параметры работы и права пользователей Kaspersky Security Service.
- **Исполнение** – возможность запускать и останавливать работу Kaspersky Security Service.

Также вы можете выполнять расширенную настройку прав доступа: давать или ограничивать права на управление Kaspersky Security Service (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 2.1

Функция	Описание
Чтение настроек службы	Возможность просматривать общие параметры работы и права пользователей Kaspersky Security Service.
Запрос статуса службы у Диспетчера управления службами	Возможность запрашивать статус выполнения Kaspersky Security Service у Диспетчера управления службами Microsoft Windows.
Запрос статуса у службы	Возможность запрашивать статус выполнения службы у Kaspersky Security Service.
Перечисление зависимых служб	Возможность просматривать список служб, от которых зависит Kaspersky Security Service, а также служб, зависимых от Kaspersky Security Service.
Изменение параметров службы	Возможность просматривать и изменять общие параметры работы и права пользователей Kaspersky Security Service.
Запуск службы	Возможность запускать выполнение Kaspersky Security Service.
Остановка службы	Возможность останавливать выполнение Kaspersky Security Service.
Приостановка / Возобновление службы	Возможность приостанавливать и возобновлять выполнение Kaspersky Security Service.
Чтение прав	Возможность просматривать список пользователей Kaspersky Security Service и права доступа каждого пользователя.
Изменение прав	Возможности: <ul style="list-style-type: none"> <li>• добавлять и удалять пользователей Kaspersky Security Service;</li> <li>• изменять права доступа пользователей к Kaspersky Security Service.</li> </ul>

Функция	Описание
Удаление службы	Возможность разрегистрации Kaspersky Security Service в Диспетчере управления службами Microsoft Windows.
Пользовательские запросы к службе	Возможность создавать и отправлять пользовательские запросы к Kaspersky Security Service.

## О правах доступа к службе Kaspersky Security Management

При установке Kaspersky Embedded Systems Security 2.1 регистрирует службу управления программой Kaspersky Security Management Service (KAVFSGT). Для управления программой через Консоль Kaspersky Embedded Systems Security 2.1, установленную на другом компьютере, требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Embedded Systems Security 2.1, имела полный доступ к Kaspersky Security Management Service на защищаемом компьютере.

По умолчанию доступ к управлению Kaspersky Security Management Service имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере, и пользователи группы ESS Administrators, созданной на защищаемом компьютере при установке Kaspersky Embedded Systems Security 2.1.

Вы можете управлять Kaspersky Security Management Service только через оснастку **Службы** Microsoft Windows.

Вы не можете разрешать или запрещать пользователям доступ к Kaspersky Security Management Service, настраивая параметры Kaspersky Embedded Systems Security 2.1.

Вы можете соединиться с Kaspersky Embedded Systems Security 2.1 под локальной учетной записью, если на защищаемом компьютере зарегистрирована учетная запись с таким же именем и с таким же паролем.



# Настройка прав доступа на управление Kaspersky Embedded Systems Security 2.1 и службой Kaspersky Security Service

Вы можете изменить список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Embedded Systems Security 2.1 и управлению службой Kaspersky Security Service, 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**. 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, в Консоли администрирования Kaspersky Security Center в группе компьютеров выберите закладку **Политики** и откройте свойства **<Имя политики>** → **Дополнительные возможности**.
  - Если вы хотите настроить параметры программы для одного компьютера, перейдите к параметрам, которые требуется настроить, в окне **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [159](#)) в Kaspersky Security Center.
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 2.1.
  - Выберите пункт **Изменить права пользователей на управление Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью Kaspersky Security Service.

Откроется окно **Разрешения для группы "Kaspersky Embedded Systems Security 2.1"**.

4. В открывшемся окне выполните следующие действия:

- Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу, которым вы хотите предоставить права.
- Чтобы удалить пользователя или группу из списка, выберите пользователя или группу, доступ для которых вы хотите ограничить, и нажмите на кнопку **Удалить**.

5. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права пользователя или группы на управление Kaspersky Embedded Systems Security 2.1 или службой Kaspersky Security Service, 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, в Консоли администрирования Kaspersky Security Center в группе компьютеров выберите закладку **Политики** и откройте свойства **<Имя политики>** → **Дополнительные возможности**.
- Если вы хотите настроить параметры программы для одного компьютера, перейдите к параметрам, которые требуется настроить, в окне **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [159](#)) в Kaspersky Security Center.

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 2.1.
- Выберите пункт **Изменить права пользователей на управление Kaspersky Security Service**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью Kaspersky Security Service.

Откроется окно **Разрешения для группы "Kaspersky Embedded Systems Security 2.1"**.

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 2.1 или службой Kaspersky Security Service.
  - **Чтение:**
    - следующие права на управление Kaspersky Embedded Systems Security 2.1: **Чтение статистики, Чтение параметров, Чтение журналов и Чтение прав;**
    - следующие права на управление службой Kaspersky Security Service: **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 2.1, кроме **Изменение прав;**
    - следующие права на управление службой Kaspersky Security Service: **Изменение параметров службы, Чтение прав.**
  - **Исполнение:** следующие права на управление службой Kaspersky Security Service: **Запуск службы, Остановка службы, Приостановка / Возобновление службы, Чтение прав, Пользовательские запросы к службе.**
6. Если вы хотите 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 2.1** выберите нужного пользователя или группу.
  - b. Нажмите на кнопку **Изменить**.
  - c. В открывшемся окне перейдите по ссылке **Показать особые разрешения**.

- d. В раскрывающемся списке в верхней части окна выберите тип контроля доступа (**Разрешить** или **Запретить**).
- e. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или группе.
- f. Нажмите на кнопку **ОК**.
- g. В окне **Дополнительные параметры безопасности для Kaspersky Embedded Systems Security 2.1** нажмите на кнопку **ОК**.

7. В окне **Разрешения для группы "Kaspersky Embedded Systems Security 2.1"** нажмите на кнопку **Применить**.

Настроенные права на управление Kaspersky Embedded Systems Security 2.1 или службой Kaspersky Security Service будут сохранены.

## Защита доступа к функциям Kaspersky Embedded Systems Security 2.1 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 2.1" на стр. [122](#)). Вы также можете дополнительно защитить доступ к выполнению критичных операций, установив защиту паролем в параметрах Kaspersky Embedded Systems Security 2.1.

Kaspersky Embedded Systems Security 2.1 запрашивает пароль при попытке доступа к следующим функциям программы:

- подключение к локальной Консоли Kaspersky Embedded Systems Security 2.1;
- удаление Kaspersky Embedded Systems Security 2.1;
- изменение компонентного состава Kaspersky Embedded Systems Security 2.1.

Kaspersky Embedded Systems Security 2.1 не отображает заданный пароль в читаемом виде в интерфейсе программы. Kaspersky Embedded Systems Security 2.1 хранит заданный пароль в виде контрольной суммы, рассчитанной при задании пароля.

Вы можете экспортировать и импортировать параметры программы, защищенной паролем. Конфигурационный файл, созданный по результатам экспорта параметров защищенной программы, содержит значение контрольной суммы пароля и значение модификатора, используемого для удлинения строки пароля.

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

► *Чтобы защитить доступ к функциям Kaspersky Embedded Systems Security 2.1, 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, в Консоли администрирования Kaspersky Security Center в группе компьютеров выберите закладку **Политики** и откройте свойства **<Имя политики> → Свойства программы**.
  - Если вы хотите настроить параметры программы для одного компьютера, перейдите к параметрам, которые требуется настроить, в окне **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)) в Kaspersky Security Center.
3. В блоке **Безопасность и надежность** 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 2.1.

6. В поле **Подтверждение пароля** введите пароль повторно.

7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены; Kaspersky Embedded Systems Security 2.1 будет запрашивать пароль при доступе к защищаемым операциям.

Установленный пароль невозможно восстановить. Утеря пароля ведет к полному блокированию доступа к управлению программой, а также делает невозможным удаление программы с защищаемого компьютера.

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

► *Чтобы сбросить заданный пароль, 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, в Консоли администрирования Kaspersky Security Center в группе компьютеров выберите закладку **Политики** и откройте свойства **<Имя политики> → Свойства программы**.
  - Если вы хотите настроить параметры программы для одного компьютера, перейдите к параметрам, которые требуется настроить, в окне **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [159](#)) в Kaspersky Security Center.
3. В блоке **Безопасность и надежность** нажмите на кнопку **Настройка**.  
  
Откроется окно **Параметры безопасности**.
4. В блоке **Параметры применения пароля** снимите флажок **Использовать защиту паролем**.

Поля **Пароль** и **Подтверждение пароля** будут очищены и станут неактивными.

5. Нажмите на кнопку **ОК**.

Защита паролем будет отключена; Kaspersky Embedded Systems Security 2.1 удалит контрольную сумму старого пароля из параметров программы.

## Разрешение сетевых соединений для службы Kaspersky Security Management Service

Названия параметров могут отличаться в разных операционных системах Windows.

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

1. На защищаемом компьютере под управлением Microsoft Windows выберите пункт **Пуск → Панель управления → Безопасность → Брандмауэр Windows**.
2. В окне **Параметры брандмауэра Windows** выберите пункт **Изменить параметры**.
3. На закладке **Исключения** в списке предустановленных исключений установите флажки **COM + Сетевой доступ**, **Windows Management Instrumentation (WMI)** и **Remote Administration**.
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 Kaspersky Embedded Systems Security 2.1.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК** в окне **Параметры брандмауэра Windows**.

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

---

## Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления задачами Kaspersky Embedded Systems Security 2.1 на нескольких компьютерах.

### В этом разделе

О политиках .....	<a href="#">136</a>
Настройка запуска по расписанию локальных системных задач .....	<a href="#">148</a>

## О политиках

Вы можете создавать единые политики Kaspersky Security Center для управления защитой нескольких компьютеров, на которых установлен Kaspersky Embedded Systems Security 2.1.



Политика применяет указанные в ней значения параметров Kaspersky Embedded Systems Security 2.1, его функций и задач 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 2.1. Вы можете просмотреть ее в Консоли Kaspersky Embedded Systems Security 2.1, 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 2.1 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 2.1 не применяет значения параметров активной политики, рядом с которыми в свойствах политики установлен значок .

Если политика активна, то в Консоли Kaspersky Embedded Systems Security 2.1 значения параметров, помеченные в политике значком , отображаются, но недоступны для редактирования. Значения остальных параметров (которые в политике помечены значком ) доступны для редактирования в Консоли Kaspersky Embedded Systems Security 2.1.

Параметры, настроенные в активной политике и помеченные значком , также блокируют редактирование параметров в Kaspersky Security Center для одного компьютера из окна **Свойства: <Имя 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 какой-либо из задач постоянной защиты и эта задача выполняется, параметры, определенные политикой, изменяются 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 вы можете установить параметры постоянной защиты.
2. Настройка параметров политики. В окне **Свойства: <Имя политики>** созданной политики вы можете настроить параметры постоянной защиты, общие параметры Kaspersky Embedded Systems Security 2.1, параметры карантина и резервного хранилища, уровень детализации в журналах выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Embedded Systems Security 2.1.

► *Чтобы создать политику для группы компьютеров, на которых установлен Kaspersky Embedded Systems Security 2.1, выполните следующие действия:*

1. В дереве Консоли администрирования разверните узел **Управляемые устройства**, а затем 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**.
3. В окне **Определение названия групповой политики для программы** в поле ввода **Имя** введите имя создаваемой политики. Имя политики не может содержать символы " \* < : > ? \ / | ).
4. В окне **Выбор программы для создания групповой политики** в списке **Название программы** выберите пункт **Kaspersky Embedded Systems Security 2.1**.
5. В окне **Выбор типа операции** выберите один из следующих вариантов:
  - **Создать**, чтобы создать новую политику с параметрами, установленными для вновь созданных политик по умолчанию;
  - **Импортировать политику, созданную с помощью предыдущей версии Kaspersky Embedded Systems Security 2.1**, чтобы использовать в качестве шаблона политику Kaspersky Embedded Systems Security 1.1.

Нажмите на кнопку **Обзор** и выберите конфигурационный файл, в котором вы сохранили существующую политику.
6. В окне **Постоянная защита**, если требуется, настройте параметры задач Постоянная защита файлов и Использование KSN согласно вашим требованиям. Разрешите или запретите применение настроенных задач политики на локальных компьютерах сети:
  - Нажмите на кнопку , чтобы разблокировать настройку параметров задачи на компьютерах сети и запретить применение настроенных в политике параметров задачи.
  - Нажмите на кнопку , чтобы заблокировать настройку параметров задачи на компьютерах сети и разрешить применение настроенных в политике параметров задачи.

Во вновь созданной политике параметры задач постоянной защиты установлены по умолчанию.

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

Задача Использование KSN доступна для использования, если принято Положение о KSN.

7. В окне **Создание групповой политики для программ** выберите одно из следующих состояний политики:

- **Активная политика**, если вы хотите, чтобы политика вступила в действие сразу после ее создания. Если в группе уже существует активная политика, эта существующая политика станет неактивной, а создаваемая вами политика будет активирована.
- **Неактивная политика**, если вы не хотите сразу применять создаваемую политику. Вы сможете активировать эту политику позже.
- **Политика для автономных пользователей**, если вы хотите создать политику для управляемого компьютера, расположенного вне сети организации. Политика для автономных пользователей доступна только для Kaspersky Embedded Systems Security 2.1 для рабочих станций (на платформе Microsoft Windows).

8. 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, и задачи и функции Kaspersky Embedded Systems Security 2.1.

# Настройка политики

В окне **Свойства:<Имя политики>** существующей политики вы можете настроить общие параметры Kaspersky Embedded Systems Security 2.1, параметры карантина и резервного хранилища, параметры доверенной зоны, параметры постоянной защиты, параметры контроля компьютера, уровень детализации в журналах выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Embedded Systems Security 2.1, права доступа к управлению программой и службой Kaspersky Security Service, параметры применения профилей политики.

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

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**, разверните группу администрирования, параметры политики которой вы хотите настроить, затем выберите в панели результатов закладку **Политики**.
2. В контекстном меню политики, параметры которой вы хотите настроить, выберите пункт **Свойства**.
3. В окне **Свойства:<Имя политики>** настройте нужные параметры политики.
4. В разделе **Общие** в блоке **Состояние политики** включите или выключите применение политики. Для этого выберите один из следующих вариантов:
  - **Активная политика**, если хотите, чтобы политика применялась на всех компьютерах, входящих в выбранную группу администрирования.
  - **Неактивная политика**, если не хотите, чтобы политика применялась на всех компьютерах, входящих в выбранную группу.

Вариант **Политика для автономных пользователей** недоступен при работе с Kaspersky Embedded Systems Security 2.1.

5. В разделах **Оповещение о событиях**, **Параметры программы**, **Журналы и уведомления**, **Дополнительные возможности**, **История ревизий** настройте общие параметры работы программы (см. таблицу ниже).

6. В разделах **Постоянная защита**, **Контроль активности на компьютерах**, **Контроль активности в сети**, **Диагностика системы**, настройте параметры выполнения задач программы, а также параметры их запуска (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 **ОК**.

Настроенные параметры будут применены в политике.

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

## Разделы свойств политики Kaspersky Embedded Systems Security 2.1

### Общие

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

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

### Оповещение о событиях

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

- *Критические события*;
- *Отказ функционирования*;

- *Предупреждение;*
- *Информационное сообщение.*

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

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

## Параметры программы

Таблица 19. Настройки раздела Параметры программы

Блок	Параметры
<b>Масштабируемость и интерфейс</b>	<p>В блоке <b>Масштабируемость и интерфейс</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры:</p> <ul style="list-style-type: none"> <li>• выбрать автоматическую или ручную настройку параметров масштабирования;</li> <li>• настроить параметры отображения значка программы.</li> </ul>
<b>Безопасность</b>	<p>В блоке <b>Безопасность</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры:</p> <ul style="list-style-type: none"> <li>• настроить параметры восстановления задач;</li> <li>• указать действия программы при переходе на источник бесперебойного питания;</li> <li>• выключить или включить защиту функций программы паролем.</li> </ul>

Блок	Параметры
<b>Параметры соединения</b>	<p>В блоке <b>Параметры соединения</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры прокси-сервера для соединения с серверами обновлений, серверами активации и KSN:</p> <ul style="list-style-type: none"> <li>указать параметры использования прокси-сервера;</li> <li>указать параметры аутентификации на прокси-сервере.</li> </ul>
<b>Запуск системных задач</b>	<p>В блоке <b>Запуск системных задач</b> по кнопке <b>Настройка</b> вы можете разрешить или запретить запуск следующих системных задач по расписанию, настроенному на локальных компьютерах:</p> <ul style="list-style-type: none"> <li>задачи проверки по требованию;</li> <li>задачи обновления и копирования обновлений.</li> </ul>

## Дополнительные возможности

Таблица 20. Настройки раздела *Дополнительные возможности*

Блок	Параметры
<b>Доверенная зона</b>	<p>В блоке <b>Доверенная зона</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры применения доверенной зоны:</p> <ul style="list-style-type: none"> <li>сформировать список исключений доверенной зоны;</li> <li>включить или выключить проверку операций резервного копирования файлов;</li> <li>сформировать список доверенных процессов.</li> </ul>
<b>Проверка съемных дисков</b>	<p>В блоке <b>Менеджер устройств</b> по кнопке <b>Настройка</b> вы можете настроить параметры проверки съемных дисков, подключаемых по USB.</p>

Блок	Параметры
<b>Права пользователей на управление программой</b>	В блоке <b>Права пользователей на управление программой</b> вы можете настроить параметры доступа пользователей и групп пользователей к управлению Kaspersky Embedded Systems Security 2.1.
<b>Права пользователей на управление службой</b>	В блоке <b>Права пользователей на управление службой</b> вы можете настроить параметры доступа пользователей и групп пользователей к управлению Kaspersky Security Service.
<b>Хранилища</b>	<p>В блоке <b>Хранилища</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры карантина и резервного хранилища:</p> <ul style="list-style-type: none"> <li>• указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище;</li> <li>• настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства;</li> <li>• указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина;</li> <li>• настроить передачу на Сервер администрирования информации об объектах резервного хранилища и карантина.</li> </ul>



## Постоянная защита

Таблица 21. Настройки раздела Постоянная защита

Блок	Параметры
<b>Постоянная защита файлов</b>	<p>В блоке <b>Постоянная защита файлов</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры выполнения задачи:</p> <ul style="list-style-type: none"><li>• указать режим защиты объектов;</li><li>• настроить применение эвристического анализатора;</li><li>• настроить применение доверенной зоны;</li><li>• указать область защиты;</li><li>• задать уровень безопасности для выбранной области защиты: вы можете выбрать предустановленный уровень безопасности или настроить параметры безопасности вручную;</li><li>• настроить параметры запуска задачи.</li></ul>
<b>Использование KSN</b>	<p>В блоке <b>Использование KSN</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры выполнения задачи:</p> <ul style="list-style-type: none"><li>• указать действия над объектами, недоверенными в KSN;</li><li>• настроить производительность задачи;</li><li>• настроить параметры использования Kaspersky Security Center в качестве прокси-сервера KSN;</li><li>• принять Положение и KSN;</li><li>• настроить параметры запуска задачи.</li></ul>
<b>Защита от эксплойтов</b>	<p>В блоке <b>Защита от эксплойтов</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры выполнения задачи:</p> <ul style="list-style-type: none"><li>• выбрать режим защиты памяти процессов;</li><li>• указать действия для снижения рисков эксплуатации уязвимостей;</li><li>• дополнить и отредактировать список защищаемых процессов.</li></ul>

## Контроль активности на компьютерах

Таблица 22. Настройки раздела Контроль активности на компьютерах

Блок	Параметры
Контроль запуска программ	<p>В блоке <b>Контроль запуска программ</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры выполнения задачи:</p> <ul style="list-style-type: none"><li>• выбрать режим работы задачи;</li><li>• настроить параметры контроля повторных запусков программ;</li><li>• указать область применения правил контроля запуска программ;</li><li>• настроить использование KSN;</li><li>• настроить параметры запуска задачи.</li></ul>
Контроль устройств	<p>В блоке <b>Контроль устройств</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры выполнения задачи:</p> <ul style="list-style-type: none"><li>• выбрать режим работы задачи;</li><li>• настроить параметры запуска задачи.</li></ul>

## Контроль активности в сети

В блоке **Управление сетевым экраном** по кнопке **Настройка** вы можете настроить следующие параметры выполнения задачи:

- настроить правила сетевого экрана;
- настроить параметры запуска задачи.

## Диагностика системы

Таблица 23. Настройки раздела Диагностика системы

Блок	Параметры
Мониторинг файловых операций	В блоке <b>Мониторинг файловых операций</b> можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом компьютере.
Анализ журналов	В блоке <b>Анализ журналов</b> можно настроить контроль целостности защищаемого сервера на основе результатов анализа журналов событий Windows.

## Журналы и уведомления

Таблица 24. Настройки раздела Журналы и уведомления

Блок	Параметры
Журналы выполнения задач	<p>В блоке <b>Журналы выполнения задач</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры:</p> <ul style="list-style-type: none"><li>указать уровень важности регистрируемых событий для выбранных компонентов программы;</li><li>указать параметры хранения журналов выполнения задач.</li></ul>
Уведомления о событиях	<p>В блоке <b>Уведомления о событиях</b> по кнопке <b>Настройка</b> вы можете настроить следующие параметры:</p> <ul style="list-style-type: none"><li>указать параметры уведомления пользователя для события <i>Обнаружен объект</i>;</li><li>указать параметры уведомления администратора для любого выбранного события из списка событий в блоке <b>Настройка уведомлений</b>.</li></ul>

<b>Взаимодействие с Сервером администрирования</b>	В блоке <b>Взаимодействие с Сервером администрирования</b> по кнопке <b>Настройка</b> вы можете выбрать типы объектов, информацию о которых Kaspersky Embedded Systems Security 2.1 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 вы можете 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 2.1 будет выполнять обновления баз и модулей программы, а также запускать все локальные системные задачи проверки по требованию в соответствии с параметрами расписания по умолчанию.

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

- задач проверки по требованию: Проверка важных областей, Проверка объектов на карантине, Проверка при старте операционной системы, Проверка целостности модулей программы;
- задач 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 2.1, 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 2.1 на компьютерах группы, выберите команду **Свойства**.
3. В окне **Свойства: <Имя политики>** откройте раздел **Свойства программы**. В блоке **Запуск системных задач** нажмите на 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.

Действие флажка **Разрешить запуск задач проверки по требованию** распространяется на запуск групповых задач автоматической генерации правил. Генерация правил контроля запуска программ и правил контроля устройств будет осуществляться в соответствии с расписанием запуска, указанным для задач проверки по требованию.

4. Убедитесь, что настраиваемая политика активна и действует в группе администрирования (см. раздел "О политиках" на стр. [136](#)).

5. Нажмите на кнопку **ОК**.

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 2.1, их создании, настройке параметров выполнения, запуске и остановке.

## В этом разделе

О создании задач в Kaspersky Security Center .....	<a href="#">151</a>
Настройка локальных задач в окне Параметры программы в Kaspersky Security Center .....	<a href="#">159</a>
Настройка групповых задач в Kaspersky Security Center .....	<a href="#">161</a>
Настройка параметров диагностики сбоев в Kaspersky Security Center .....	<a href="#">183</a>
Работа с расписанием задач .....	<a href="#">186</a>

## 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;
- генерация правил контроля запуска программ;
- генерация правил контроля устройств.

Вы можете создать локальные и групповые задачи следующими способами:

- для одного 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 вы можете отключать действие расписания локальных системных задач обновления и проверки по требованию на всех защищаемых компьютерах, принадлежащих к одной группе администрирования. (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. [148](#))

Общая информация о задачах в Kaspersky Security Center содержится в *Справочной системе Kaspersky Security Center*.

## Создание задачи в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

► 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, 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 имя задачи (не более 100 символов, не может содержать символы **| \* < > ? \ / | : ;**). Рекомендуется включить в имя задачи ее тип (например, "Проверка по требованию папок общего доступа").
3. В окне **Выбор типа задачи** под заголовком **Kaspersky Embedded Systems Security 2.1** выберите тип создаваемой задачи.
4. Если вы выбрали любой тип задачи, кроме типа Откат обновлений баз или Активация программы, откроется окно **Настройка**. В зависимости от типа создаваемой задачи выполните одно из следующих действий:
  - *Если вы создаете задачу проверки по требованию:*

а. 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 предопределенные 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 предопределенную область, диск, папку, сетевой объект или файл, нажмите правой клавишей мыши в таблице **Область проверки** и выберите **Добавить область**. В окне **Добавление в область проверки** выберите предопределенную область в списке **Предопределенная область**, укажите диск компьютера, папку, сетевой объект или файл на защищаемом 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 **Настроить**, затем в окне **Уровень безопасности** нажмите на кнопку **Настройка** и в окне **Настройка проверки по требованию** на закладке **Общие** снимите флажок **Вложенные папки (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 предустановленных уровней безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры безопасности вручную. Настройка выполняется так же, как в Консоли Kaspersky Embedded Systems Security 2.1.
- Чтобы исключить из добавленной области проверки вложенные объекты, откройте контекстное меню в таблице **Область проверки**, выберите **Добавить исключение** и укажите объекты, которые вы хотите исключить: выберите предопределенную область в списке **Предопределенная область**, укажите диск компьютера, папку, сетевой объект или файл на защищаемом компьютере или другом компьютере в сети, а затем нажмите на кнопку **ОК**.

Области, являющиеся исключениями из проверки, отображаются в таблице помеченными значком .

а. 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 2.1.

Если вы планируете использовать создаваемую задачу в качестве задачи проверки важных областей компьютера, в окне **Параметры** установите флажок **Считать выполнение задачи проверкой важных областей**. Программа Kaspersky Security Center будет оценивать состояние безопасности компьютера (компьютеров) по результатам выполнения задач со статусом *Задача 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 (Low)**, в окне **Параметры** установите флажок **Выполнять задачу в фоновом режиме**. По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Embedded Systems Security 2.1, имеют приоритет **Средний (Normal)**. 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:

а. Выберите источник обновлений в окне **Источник обновлений**.

б. Нажмите на кнопку **Настройка параметров локальной сети**. Откроется окно **Настройка параметров соединения**.

с. На закладке **Настройка параметров 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 (компьютеров), 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, копировать и устанавливать критические обновления программных модулей или только проверять их наличие.
  - b. Если вы выбрали **Копировать и устанавливать критические обновления модулей программы**: для применения установленных программных модулей может потребоваться перезагрузка компьютера. Чтобы Kaspersky Embedded Systems Security 2.1 автоматически запускал перезагрузку компьютера после завершения задачи, установите флажок **Разрешать перезагрузку операционной системы**. Чтобы отменить автоматическую перезагрузку после завершения задачи, снимите флажок **Разрешать перезагрузку операционной системы**.
  - c. Если вы хотите получать информацию о выходе плановых обновлений модулей Kaspersky Embedded Systems Security 2.1, 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". Вы можете настроить уведомление администратора о событии **Доступны плановые обновления модулей Kaspersky Embedded Systems Security 2.1**, в котором будет содержаться адрес страницы на нашем веб-сайте, откуда вы сможете загружать плановые 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 *Генерация правил контроля устройств или задачу Генерация правил контроля запуска программ*, в окне **Настройка** укажите параметры, на основе которых будет сформирован список разрешающих правил:
    - а. Укажите префикс для названий правил (только для задачи генерации правил контроля запуска программ).
    - б. Настройте параметры области применения разрешающих правил (только для задачи генерации правил контроля запуска программ). Нажмите на кнопку **Далее**.
    - с. Укажите действия, которые задача будет выполнять во время формирования разрешающих правил (только для задачи генерации правил контроля запуска программ) и по завершении.
5. Настройте параметры расписания задачи (вы можете настраивать расписание задач всех типов кроме задачи Откат обновления баз). В окне **Расписание** выполните следующие действия:
- а. Чтобы включить расписание, установите флажок **Запускать задачу по расписанию**;
  - б. Укажите частоту запуска задачи: в списке **Частота запуска** выберите одно из следующих значений: **Ежечасно**, **Ежесуточно**, **Еженедельно**, **При запуске программы**, **После обновления баз программы** (в групповых задачах Обновление баз программы, 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);
- с. В поле **Время запуска** укажите время первого запуска задачи; в поле **Начать с** укажите дату начала действия расписания.
- д. 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 группе **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 группе **Параметры остановки задачи** введите начальное и конечное значение промежутка в поле **Приостановить с ... 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 распределение времени запуска: установите флажок **Распределять время запуска задач в интервале** и укажите значение параметра в минутах.
- е. Нажмите на кнопку **ОК**.
6. Если создаваемая задача является задачей для произвольного набора компьютеров, выберите компьютеры сети (группы), на которых она будет выполняться.

7. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, с правами которой вы хотите выполнять задачу.
8. В окне **Завершение создания задачи** установите флажок **Запустить задачу после завершения работы мастера**, если хотите, чтобы задача была запущена по созданию. 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 одного компьютера в окне **Параметры программы**, выполните следующие действия:
1. В дереве Сервера 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;
    - откройте контекстное меню на имени защищаемого компьютера и выберите пункт **Свойства**.
  4. В окне **Свойства: <Имя компьютера>** в разделе **Программы** откройте окно **Параметры программы** одним из следующих способов:
    - 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 к программе применяется политика Kaspersky Security Center и в этой политике наложен запрет на изменение параметров программы, эти параметры недоступны для изменения через окно **Параметры программы**.

5. Выполните одно из следующих действий:

- Чтобы настроить параметры локальной задачи:
  - a. Перейдите в раздел **Задачи**.
  - b. В списке задач выберите локальную задачу, параметры которой вы хотите настроить.
  - c. Затем выберите пункт **Свойства** в контекстном меню выбранной задачи.
- Чтобы настроить параметры программы:
  - a. Перейдите в раздел **Программы** → **Kaspersky Embedded Systems Security 2.1**.
  - b. Нажмите на кнопку **Настройка** в блоке параметров, которые вы хотите настроить.

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.



# Настройка групповых задач в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

- Чтобы настроить групповую задачу для нескольких компьютеров, 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 задач.
  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: <Имя задачи>** одним из следующих способов:
    - двойным щелчком мыши на имени задачи в списке созданных задач;
    - выделите имя задачи в списке созданных задач и перейдите по ссылке **Изменить параметры задачи**;
    - откройте контекстное меню на имени 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 *Справочной системе 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 **Настройка** сформируйте 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 **Источник обновлений** настройте параметры источника обновлений и оптимизацию использования дисковой подсистемы.
    - b. По кнопке **Настройка параметров соединения** настройте общие параметры соединения и параметры соединения с источником обновлений.
  - Если вы настраиваете 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.
  - Если вы настраиваете задачу Копирование обновлений, в разделе **Настройка параметров копирования обновлений** укажите состав обновлений и папку локального источника обновлений, в которую обновления будут сохранены.
  - Если вы настраиваете задачу Активация программы, в разделе **Параметры активации** примените файл ключа или код активации, с помощью которых 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.
  - Если вы настраиваете одну из задач автоматического формирования разрешающих правил контроля компьютера, в разделе **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 *Справочной системе 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 *Справочной системе Kaspersky Security Center*.

9. В окне **Свойства <Имя задачи>** нажмите на кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

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

Таблица 25. Параметры групповых задач Kaspersky Embedded Systems Security 2.1

Тип задачи	Раздел в окне Свойства: <Имя задачи>	Параметры задачи
Автоматическая генерация правил (задача Генерация правил контроля запуска программ и задача Генерация правил контроля устройств).	<b>Настройка</b>	При настройке параметров задачи Генерация правил контроля запуска программ вы можете: <ul style="list-style-type: none"><li>• изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых разрешен автоматически сформированными правилами;</li><li>• учитывать или не учитывать запущенные программы.</li></ul>
	<b>Параметры</b>	Вы можете указать действия при формировании разрешающих правил контроля запуска программ: <ul style="list-style-type: none"><li>• <b>Использовать цифровой сертификат;</b> Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В</li></ul>

		<p>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.</p> <p>Этот вариант выбран по умолчанию.</p> <ul style="list-style-type: none"> <li>• <b>Использовать заголовок и отпечаток цифрового сертификата;</b></li> </ul> <p>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.</p> <p>Флажок доступен, если выбран вариант <b>Использовать цифровой сертификат</b>.</p> <p>По умолчанию флажок установлен.</p> <ul style="list-style-type: none"> <li>• <b>Если сертификат отсутствует;</b></li> </ul> <p>Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ для случая, если файл, на основе которого формируется правило, не имеет цифрового сертификата.</p> <ul style="list-style-type: none"> <li>• <b>Хеш SHA256.</b> В качестве критерия разрешающего правила контроля запуска программ устанавливается значение контрольной суммы файла, на основе которого формируется правило. В дальнейшем программа будет разрешать</li> </ul>
--	--	---

		<p>запуск программ, запускаемых файлами с указанной контрольной суммой.</p> <ul style="list-style-type: none"> <li> <b>Путь к файлу.</b> 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 <b>Создавать разрешающие правила для программ из папок.</b> </li> <li> <b>Использовать хеш SHA256;</b> <p>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.</p> <p>Этот вариант рекомендуется применять, если требуется создать максимально надежные правила: контрольная сумма, рассчитанная по алгоритму SHA256, является уникальным идентификатором файла. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.</p> </li> <li> <b>Формировать правила для пользователя или группы пользователей.</b> <p>Поле, в котором отображаются</p> </li> </ul>
--	--	--

		<p>пользователь и / или группа пользователей. Программа будет контролировать запуски программ указанным пользователем и / или группой.</p> <p>По умолчанию выбрана группа <b>Все</b>.</p> <p>Вы можете настроить параметры для конфигурационных файлов со списком сформированных разрешающих правил контроля устройств и контроля запуска программ, которые Kaspersky Embedded Systems Security 2.1 создает по завершении задач.</p>
	<b>Расписание</b>	Вы можете настроить параметры запуска задачи по расписанию.
Активация программы	<b>Параметры активации программы</b>	Вы можете добавить код активации или ключ для активации программы или для продления срока действия лицензии.
	<b>Расписание</b>	Вы можете настроить параметры запуска задачи по расписанию.
Копирование обновлений	<b>Источник обновлений</b>	<p>Вы можете указать сервер администрирования Kaspersky Security Center или Серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы.</p> <p>Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.</p> <p>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.</p>

	<p>Окно <b>Настройка параметров соединения</b></p> <p>► <i>Чтобы открыть окно <b>Настройка параметров соединения</b>,</i></p> <p>нажмите на кнопку <b>Настройка параметров соединения</b> в разделе <b>Источник обновлений</b>.</p>	<p>В блоке <b>Параметры соединения с источниками обновлений</b> вы можете настроить параметры использования прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.</p>
	<p><b>Настройка параметров копирования обновлений</b></p>	<p>Вы можете указать состав обновлений для копирования.</p> <p>В поле <b>Папка для локального хранения скопированных обновлений</b> укажите путь к папке, в которой Kaspersky Embedded Systems Security 2.1 будет сохранять скопированные обновления.</p>
	<p><b>Расписание</b></p>	<p>Вы можете настроить параметры запуска задачи по расписанию.</p>

Тип задачи	Раздел в окне Свойства: <Имя задачи>	Параметры задачи
Обновление баз программы	<b>Источник обновлений</b>	<p>В блоке <b>Источник обновлений</b> 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.</p> <p>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.</p> <p>В блоке <b>Оптимизация использования дисковой подсистемы</b> вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему:</p> <ul style="list-style-type: none"> <li>• <b>Снизить нагрузку на дисковую подсистему за счет оперативной памяти.</b> <p>Флажок включает или выключает функцию оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти.</p> <p>Если флажок установлен, функция активна.</p> <p>По умолчанию флажок снят.</p> </li> <li>• <b>Объем оперативной памяти, используемый для оптимизации (МБ).</b></li> </ul>



Тип задачи	Раздел в окне Свойства: <Имя задачи>	Параметры задачи
<p>Объем оперативной памяти (в мегабайтах), который программа использует для размещения файлов обновлений.</p> <p>По умолчанию установлен объем оперативной памяти 512 МБ.</p>	<p>Окно <b>Настройка параметров соединения</b></p> <p>► Чтобы открыть окно <b>Настройка параметров соединения</b>, нажмите на кнопку <b>Настройка параметров соединения</b> в разделе <b>Источник обновлений</b>.</p>	<p>В блоке <b>Параметры соединения с источниками обновлений</b> вы можете настроить параметры использования прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.</p>
	<p><b>Расписание</b></p>	<p>Вы можете настроить параметры запуска задачи по расписанию.</p>
<p>Обновление модулей программы</p>	<p><b>Источник обновлений</b></p>	<p>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.</p> <p>Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.</p>

	<p>Окно <b>Настройка параметров соединения</b></p> <p>► Чтобы открыть окно <b>Настройка параметров соединения</b>, нажмите на кнопку <b>Настройка параметров соединения</b> в разделе <b>Источник обновлений</b>.</p>	<p>В блоке <b>Параметры соединения с источниками обновлений</b> вы можете настроить параметры использования прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.</p>
	<p><b>Настройка параметров обновления модулей программы</b></p>	<p>Вы можете указать действия, которые Kaspersky Embedded Systems Security 2.1 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.</p>
	<p><b>Расписание</b></p>	<p>Вы можете настроить параметры запуска задачи по расписанию.</p>
Проверка по требованию	<p><b>Настройка</b></p>	<p>Вы можете сформировать область проверки для задачи проверки по требованию, а также перейти к настройке уровня безопасности.</p>
	<p>Окно <b>Настройка проверки по требованию</b></p> <p>► Чтобы открыть окно <b>Настройка</b></p>	<p>Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры пользовательского уровня безопасности вручную.</p>

	<p><b>проверки по требованию,</b></p> <p>нажмите на кнопку <b>Настроить уровень безопасности</b> в разделе <b>Настройка.</b></p>	
	<p><b>Параметры</b></p>	<p>В блоке <b>Эвристический анализатор</b> вы можете включить или выключить применение эвристического анализатора в задаче проверки по требованию и настроить уровень анализа с помощью ползунка.</p> <p>В блоке <b>Дополнительные параметры</b> вы можете настроить следующие параметры:</p> <ul style="list-style-type: none"> <li>• применение доверенной зоны в задаче проверки по требованию;</li> <li>• применение служб KSN в задаче проверки по требованию;</li> <li>• указать приоритет задачи проверки по требованию: выполнять задачу в фоновом режиме (низкий приоритет) или считать выполнение задачи проверкой важных областей.</li> </ul>
	<p><b>Расписание</b></p>	<p>Вы можете настроить параметры запуска задачи по расписанию.</p>
<p>Проверка целостности модулей программы</p>	<p><b>Расписание</b></p>	<p>Вы можете настроить параметры запуска задачи по расписанию.</p>

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 *Справочной системе Kaspersky Security Center*.

## Задачи генерации правил контроля устройств и контроля запуска программ

► Чтобы настроить задачу Генерация правил контроля устройств или задачу Генерация правил контроля запуска программ, 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 задач.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте контекстное меню задачи и выберите пункт **Свойства**.

Откроется окно **Свойства: <Имя задачи>**.

4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе содержится в Справочной системе Kaspersky Security Center.
5. 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.
6. 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.

Этот 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;**

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 рекомендуется применять, если требуется создать максимально надежные правила: контрольная сумма, рассчитанная по алгоритму SHA256, является уникальным идентификатором файла. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Формировать 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 2.1 создает по завершении задач.

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. Подробная информация о настройке параметров в этом разделе содержится в Справочной системе Kaspersky Security Center.
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 Справочной системе Kaspersky Security Center.
10. В окне **Свойства <Имя задачи>** нажмите на кнопку **ОК**.

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**. Разверните группу администрирования, для компьютеров которой вы хотите настроить параметры задач.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте контекстное меню задачи и выберите пункт **Свойства**.

Откроется окно **Свойства: <Имя задачи>**.

4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе содержится в Справочной системе Kaspersky Security Center.
5. 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.
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 Справочной системе 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 Справочной системе Kaspersky Security Center.
9. В окне **Свойства <Имя задачи>** нажмите на кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

## Задачи обновления программы

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**. Разверните группу администрирования, для компьютеров которой вы хотите настроить параметры задач.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.



3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте контекстное меню задачи и выберите пункт **Свойства**.

Откроется окно **Свойства: <Имя задачи>**.

4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе содержится в Справочной системе 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 подсистему за счет оперативной памяти.**

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.

- с. 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 2.1 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 разделе **Настройка параметров копирования обновлений** для задачи Копирование обновлений укажите состав обновлений и папку локального источника обновлений, в которую обновления будут сохранены.
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 Справочной системе 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 Справочной системе Kaspersky Security Center.
9. В окне **Свойства <Имя задачи>** нажмите на кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

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 *Справочной системе Kaspersky Security Center*.

# Задача Проверка по требованию

► Чтобы настроить задачу Проверка по требованию, 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 задач.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте контекстное меню задачи и выберите пункт **Свойства**.

Откроется окно **Свойства: <Имя задачи>**.

4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе содержится в Справочной системе Kaspersky Security Center.
5. В разделе **Настройка** вы можете выполнить следующие действия:
  - а. В блоке **Область проверки** установите флажки напротив тех, файловых ресурсов, которые вы хотите включить в область проверки.
  - б. Нажмите на кнопку **Настроить уровень безопасности** и выберите уровень безопасности.

Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры пользовательского уровня безопасности вручную. Чтобы настроить уровень безопасности вручную, в окне **Настройка проверки по требованию** нажмите на кнопку **Настройка**.

6. В разделе **Параметры** вы можете выполнить следующие действия:
  - а. В блоке **Эвристический анализатор** включить или выключить использование эвристического анализатора и настроить уровень анализа с помощью ползунка.

- b. В блоке **Дополнительные параметры** вы можете настроить следующие параметры:
- применение доверенной зоны в задаче проверки по требованию;
  - применение служб KSN в задаче проверки по требованию;
  - указать приоритет задачи проверки по требованию: выполнять задачу в фоновом режиме (низкий приоритет) или считать выполнение задачи проверкой важных областей.
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. Подробная информация о настройке параметров в этом разделе содержится в Справочной системе Kaspersky Security Center.
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 Справочной системе Kaspersky Security Center.
10. В окне **Свойства <Имя задачи>** нажмите на кнопку **ОК**.

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 указано параметром Kaspersky Embedded Systems Security 2.1 **Порог формирования события Проверка важных областей не проводилась давно**.

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

1. Создайте групповую задачу проверки по требованию. В окне **Параметры** мастера создания задачи установите флажок **Считать выполнение задачи проверкой важных областей компьютера**. Указанные вами параметры задачи – область проверки и параметры безопасности – будут едиными для всех компьютеров группы. Настройте расписание задачи.

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

2. 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. [148](#)).

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 *Задача 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 Kaspersky Embedded Systems Security 2.1 вы можете просмотреть, является ли задача проверки по требованию задачей проверки важных областей компьютера.

В Консоли Kaspersky Embedded Systems Security 2.1 флажок **Считать выполнение задачи проверкой важных областей** отображается в свойствах задач, но он не доступен для редактирования.

# Задача 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**. Разверните группу администрирования, для компьютеров которой вы хотите настроить параметры задач.
2. В панели результатов выбранной группы администрирования откройте закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте контекстное меню задачи и выберите пункт **Свойства**.

Откроется окно **Свойства: <Имя задачи>**.

4. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе содержится в Справочной системе 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. Подробная информация о настройке параметров в этом разделе содержится в Справочной системе 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 Справочной системе Kaspersky Security Center.
9. В окне **Свойства <Имя задачи>** нажмите на кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

# Настройка параметров диагностики сбоев в Kaspersky Security Center

Если в работе Kaspersky Embedded Systems Security 2.1 возникла проблема (например, Kaspersky Embedded Systems Security 2.1 завершается аварийно) и вы хотите диагностировать ее, вы можете включить создание файлов трассировки и файла дампа процессов Kaspersky Embedded Systems Security 2.1 и отправить эти файлы на анализ в Службу технической поддержки "Лаборатории Касперского".

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

► 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. [159](#)).
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 2.1 будет сохранять файлы трассировки.
  - Настройте уровень детализации отладочной информации.

В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки.

Вы можете выбрать один из следующих уровней детализации:

- **Критические события** – Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки только информацию о критических событиях.
- **Ошибки** – Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки информацию о критических событиях и об ошибках.
- **Важные события** – Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки информацию о критических событиях, об ошибках и о важных событиях.
- **Информационные события** – Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки информацию о критических событиях, об ошибках, о важных событиях и об информационных событиях.
- **Вся отладочная информация** – Kaspersky Embedded Systems Security 2.1 сохраняет в файле трассировки всю отладочную информацию.

Уровень детализации, который требуется установить для решения возникшей проблемы, определяет специалист Службы технической поддержки.

По умолчанию установлен уровень детализации **Вся отладочная информация**.

Раскрывающийся список доступен, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Укажите максимальный размер файлов трассировки.
- Укажите отлаживаемые компоненты.

Список кодов подсистем Kaspersky Embedded Systems Security 2.1, о работе которых программа сохраняет отладочную информацию в файле трассировки. Коды подсистем требуется вводить через запятую и с соблюдением регистра (см. таблицу ниже).



Таблица 26. Коды подсистем Kaspersky Embedded Systems Security 2.1

Код подсистемы	Название подсистемы
*	Все компоненты.
gui	Подсистема пользовательского интерфейса, оснастка Kaspersky Embedded Systems Security 2.1 в Microsoft Management Console.
ak_conn	Подсистема интеграции с Агентом администрирования Kaspersky Security Center.
bl	Управляющий процесс, реализует задачи управления Kaspersky Embedded Systems Security 2.1.
wp	Рабочий процесс; реализует задачи антивирусной защиты.
blgate	Процесс удаленного управления Kaspersky Embedded Systems Security 2.1.
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 2.1 (gui) и плагина управления Kaspersky Embedded Systems Security 2.1 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 2.1 применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Embedded Systems Security 2.1 сохраняет отладочную информацию о работе всех подсистем Kaspersky Embedded Systems Security 2.1 (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 2.1 будет сохранять файл дампа.

3. Нажмите на кнопку **ОК**.

Настроенные параметры программы будут применены на защищаемом компьютере.

## Работа с расписанием задач

Вы можете настраивать запуск задач Kaspersky Embedded Systems Security 2.1 по расписанию, а также настраивать параметры запуска по расписанию.

## В этом разделе

Настройка параметров расписания запуска задач.....	<a href="#">187</a>
Включение и выключение запуска по расписанию .....	<a href="#">190</a>

# Настройка параметров расписания запуска задач

В Консоли Kaspersky Embedded Systems Security 2.1 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 Kaspersky Security Center разверните узел Управляемые устройства и выполните следующие действия:
  - Если вы хотите настроить параметры политики, в группе компьютеров выберите **Политики** → **<Имя политики>** → **<Раздел>** → **Настройка** → **Управление задачами**.
  - Если вы хотите настроить параметры задачи для одного компьютера через Kaspersky Security Center, откройте окно Параметры задачи (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)) в Kaspersky Security Center.

Откроется окно **Параметры**.

2. В открывшемся окне на закладке **Расписание** включите запуск задачи по расписанию, установив флажок **Выполнять 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 (см. раздел "Настройка запуска по расписанию локальных системных задач" на стр. [148](#)).

3. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

а. В списке **Частота запуска** выберите одно из следующих значений:

- **Ежечасно**, если хотите, чтобы задача запускалась с периодичностью в заданное вами количество часов, и укажите количество часов в поле **Раз в <количество> ч**;
- **Ежесуточно**, если хотите, чтобы задача запускалась с периодичностью в заданное вами количество дней, и укажите количество дней в поле **Раз в <количество> сут**;
- **Еженедельно**, если хотите, чтобы задача запускалась с периодичностью в 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 2.1;
- **После обновления баз программы**, если хотите, чтобы задача запускалась после каждого обновления баз программы.

б. В поле **Время запуска** укажите время первого запуска задачи.

в. 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. [148](#)).

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 ... до** 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**.

Настроенные параметры расписания запуска выбранной задачи будут сохранены.

# 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 Kaspersky Embedded Systems Security 2.1 откройте контекстное меню названия задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.

Откроется окно **Параметры задачи**.

3. В открывшемся окне на закладке **Расписание** 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 на кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

---

# Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center.

## В этом разделе

О способах управления Kaspersky Embedded Systems Security 2.1 из Kaspersky Security Center .....	<a href="#">191</a>
О настройке общих параметров программы в Kaspersky Security Center .....	<a href="#">193</a>
О настройке дополнительных возможностей программы .....	<a href="#">201</a>
О настройке журналов и уведомлений .....	<a href="#">212</a>

## О способах управления Kaspersky Embedded Systems Security 2.1 из Kaspersky Security Center

Вы можете централизованно управлять несколькими компьютерами с установленным Kaspersky Embedded Systems Security 2.1, включенными в *группу администрирования*, с помощью плагина Kaspersky Security Center. Также вы можете отдельно настраивать параметры работы для каждого компьютера, входящего в группу администрирования, в Kaspersky Security Center.

*Группа администрирования* формируется на стороне Kaspersky Security Center вручную и включает в себя несколько компьютеров с установленным Kaspersky Embedded Systems Security 2.1, для которых вы хотите настроить единые параметры управления и защиты.

Подробная информация об использовании групп администрирования содержится в *Справочной системе Kaspersky Security Center*.

Параметры программы для одного компьютера недоступны для настройки, если работа Kaspersky Embedded Systems Security 2.1 на этом компьютере контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Embedded Systems Security 2.1 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 задач, заданные в активной политике, имеют приоритет над параметрами задач, настроенными локально в Консоли Kaspersky Embedded Systems Security 2.1 или удаленно в окне **Свойства: <Имя компьютера>** Kaspersky Security Center.

С помощью политик вы можете настроить общие параметры работы программы, параметры задач постоянной защиты, параметры задач контроля компьютера, параметры запуска системных задач по расписанию, 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 компьютеров.** Задачи для набора компьютеров позволяют удаленно настроить единые параметры задач, имеющих ограниченный срок выполнения, для компьютеров, которые не включены ни в одну из созданных групп администрирования.
- **С помощью окна настройки параметров одного компьютера.** В окне **Свойства: <Имя компьютера>** вы можете удаленно настроить параметры задачи для одного компьютера, включенного в группу администрирования. Вы можете настроить как общие параметры работы программы, так и параметры работы всех задач Kaspersky



Embedded Systems Security 2.1, 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 одного компьютера.

## О настройке общих параметров программы в Kaspersky Security Center

Вы можете настроить общие параметры Kaspersky Embedded Systems Security 2.1 из Kaspersky Security Center для группы компьютеров или для одного компьютера.

### В этом разделе

Настройка масштабируемости и интерфейса в Kaspersky Security Center .....	<a href="#">193</a>
Настройка параметров безопасности в Kaspersky Security Center .....	<a href="#">196</a>
Настройка параметров соединения в Kaspersky Security Center .....	<a href="#">199</a>

## Настройка масштабируемости и интерфейса в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

► 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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).
  - 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 **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 2.1 рабочих процессов:
    - **Определять параметры масштабируемости автоматически.**  
Kaspersky Embedded Systems Security 2.1 регулирует количество используемых процессов автоматически.  
Это значение установлено по умолчанию.

- **Указать количество рабочих процессов вручную.**

Kaspersky Embedded Systems Security 2.1 регулирует количество активных рабочих процессов в соответствии с указанными значениями.

- **Максимальное количество активных процессов.**

Максимальное количество процессов, которые использует Kaspersky Embedded Systems Security 2.1.

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 Kaspersky Embedded Systems Security 2.1 в области уведомлений панели задач: снимите или установите флажок **Показывать значок программы в панели задач.**

5. Нажмите на кнопку **ОК**.

Настроенные параметры программы будут сохранены.

# Настройка параметров безопасности в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

► Чтобы настроить параметры безопасности, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите 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 программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).
  - 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 2.1 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 2.1 после сбоя в работе программы или аварийного завершения работы программы.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 автоматически восстанавливает задачи Kaspersky Embedded Systems Security 2.1 после сбоя в работе программы или аварийного завершения работы программы.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 не восстанавливает задачи Kaspersky Embedded Systems Security 2.1 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 2.1.

Поле ввода доступно, если установлен флажок **Выполнять восстановление задач**.

- В блоке **Действия при переходе на источник бесперебойного питания** задайте ограничение нагрузки на сервер, создаваемой Kaspersky Embedded Systems Security 2.1 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 2.1 не

запускает задачи проверки по расписанию при переходе на источник бесперебойного питания до восстановления стандартного режима питания.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 запускает задачи проверки по расписанию вне зависимости от режима питания компьютера.

По умолчанию флажок установлен.

- **Остановить выполнение задачи проверки.**

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

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 останавливает выполнение запущенных задач проверки при переходе компьютера на источник бесперебойного питания.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 продолжает выполнение запущенных задач проверки при переходе компьютера на источник бесперебойного питания.

По умолчанию флажок установлен.

- В блоке **Параметры применения пароля** задайте пароль для защиты доступа к функциям Kaspersky Embedded Systems Security 2.1.

5. Нажмите на кнопку **ОК**.

Настроенные параметры безопасности и надежности будут сохранены.

# Настройка параметров соединения в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

Настроенные параметры соединения используются для подключения Kaspersky Embedded Systems Security 2.1 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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).
  - 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 **Параметры соединения** нажмите на кнопку **Настройка**.

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 2.1 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 2.1 автоматически определяет параметры подключения к службам KSN с использованием протокола Web Proxy Auto-Discovery Protocol (WPAD).

Этот вариант выбран по умолчанию.

- **Использовать параметры указанного прокси-сервера.**

Если выбран этот вариант, для соединения с KSN Kaspersky Embedded Systems Security 2.1 использует параметры прокси-сервера, указанные вручную.

- IP-адрес или символьное имя прокси-сервера и номер порта.

- **Не использовать прокси-сервер для указанных адресов.**

Флажок включает или выключает использование прокси-сервера при обращении к компьютерам из сети, к которой принадлежит компьютер с установленным Kaspersky Embedded Systems Security 2.1.

Если флажок установлен, обращение к компьютерам из сети, к которой принадлежит компьютер с установленным Kaspersky Embedded Systems Security 2.1, 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.

В раскрывающемся списке можно выбрать режим проверки подлинности, который используется при доступе к прокси-серверу.
  - **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 **ОК**.

Настроенные параметры соединения будут сохранены.

## О настройке дополнительных возможностей программы

Вы можете настроить дополнительные возможности Kaspersky Embedded Systems Security 2.1 из Kaspersky Security Center для группы компьютеров или для одного компьютера.

## В этом разделе

Настройка параметров доверенной зоны в Kaspersky Security Center.....	<a href="#">202</a>
Проверка съёмных дисков .....	<a href="#">206</a>
Настройка прав доступа в Kaspersky Security Center .....	<a href="#">209</a>
Настройка параметров карантина и резервного хранилища	
Kaspersky Security Center .....	<a href="#">210</a>

# 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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

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** в блоке **Доверенная зона** нажмите на кнопку **Настройка**.

4. В окне **Доверенная зона** на закладке **Исключения** укажите объекты, которые Kaspersky Embedded Systems Security 2.1 пропускает при проверке:

- Если вы хотите добавить 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 2.1 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.**

Имя или маска имени файла, локальный или съемный диск компьютера, локальная или сетевая папка, предопределенная область.

- **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 (<http://www.securelist.ru>).

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает при проверке указанные обнаруживаемые объекты.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

- **Область применения исключения.**

Название задачи Kaspersky Embedded Systems Security 2.1, 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 2.1 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 2.1 пропускает при проверке операции чтения файлов, выполняемые установленными на компьютере средствами резервного копирования.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 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 2.1 пропускает при проверке файловые операции доверенных процессов.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет файловые операции доверенных процессов.

По умолчанию флажок снят.

6. Если требуется, добавьте процессы, для которых вы не хотите проверять файловую активность, выполнив следующие действия:

- а. Нажмите на кнопку **Добавить**.

- b. В открывшемся окне **Добавление доверенного процесса** нажмите на кнопку **Обзор**.

Откроется стандартно окно выбора файла Microsoft Windows.

- c. Выберите исполняемый файл процесса и нажмите на кнопку **ОК**.

Блок **Критерии доверенности** автоматически заполнится данными указанного файла.

- d. Выберите, какие критерии доверенности вы хотите учитывать для данного процесса:

- Папка с файлом на защищаемом компьютере.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 будет использовать полный путь к папке для определения статуса доверенности процесса.

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

По умолчанию флажок установлен.

- Использовать хеш файла для определения доверенности процесса.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 будет использовать хеш выбранного файла для определения статуса доверенности процесса.

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

По умолчанию флажок установлен.

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

- e. Нажмите на кнопку **ОК**.

# Проверка съёмных дисков

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

Kaspersky Embedded Systems Security 2.1 выполняет проверку съёмного диска с помощью задачи Проверка по требованию. Программа автоматически создает новую задачу Проверка по требованию в момент подключения съёмного диска и удаляет созданную задачу по завершении проверки. Созданная задача выполняется с предустановленным уровнем безопасности, указанным для проверки съёмных дисков. Вы не можете настроить параметры временной задачи Проверка по требованию.

Если вы установили Kaspersky Embedded Systems Security 2.1 без антивирусных баз, проверка съёмных дисков будет недоступна.

Kaspersky Embedded Systems Security 2.1 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 съёмного диска, если его подключение было заблокировано задачей Контроль устройств. Программа не выполняет проверку MTP-подключаемых мобильных устройств.

Kaspersky Embedded Systems Security 2.1 не блокирует доступ к съёмному диску на время проверки.

Результаты проверки каждого съёмного диска доступны в журнале выполнения задачи Проверка по требованию, созданной при подключении этого диска.

Вы можете изменять значения параметров компонента Проверка съёмных дисков (см. таблицу ниже).

Таблица 27. Параметры проверки съёмных дисков

Параметр	Значение по умолчанию	Описание
Проверять съёмные диски при их подключении по USB	Флажок снят	Вы можете включать или выключать проверку съёмных дисков при их подключении к защищаемому компьютеру.
Проверять, если объем содержащихся на диске данных не превышает порог (МБ)	1024 МБ	<p>Вы можете уменьшить область срабатывания компонента, указав максимальный объем данных на съёмном диске.</p> <p>Kaspersky Embedded Systems Security 2.1 не будет выполнять проверку съёмного диска, если объем содержащихся на нем данных превышает указанное значение.</p>
Запускать проверку с уровнем безопасности	Максимальная защита	<p>Вы можете настраивать параметры создаваемых задач проверки по требованию, выбирая один из трех уровней безопасности:</p> <ul style="list-style-type: none"> <li>• <b>Максимальная защита;</b></li> <li>• <b>Рекомендуемый;</b></li> <li>• <b>Максимальное быстрое действие.</b></li> </ul> <p>Алгоритм действий при обнаружении зараженных, возможно зараженных и других объектов, а также другие параметры проверки для каждого уровня безопасности соответствуют предустановленным уровням безопасности в задачах проверки по требованию.</p>

Чтобы настроить параметры проверки съёмных дисков при подключении, 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, в Консоли администрирования Kaspersky Security Center в группе компьютеров выберите закладку **Политики**, откройте свойства **<Имя политики>** → **Свойства программы** → **Настройка** в блоке **Проверка съёмных дисков**.
  - Если вы хотите настроить параметры программы для одного компьютера через Kaspersky Security Center, перейдите к параметрам, которые требуется настроить, в окне Параметры программы (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)) в Kaspersky Security Center.

Откроется окно **Проверка съёмных дисков**.

3. В блоке **Параметры проверки при подключении** выполните следующие действия:
  - Установите флажок **Проверять съёмные диски при их подключении по USB**, если вы хотите, чтобы Kaspersky Embedded Systems Security 2.1 автоматически выполнял проверку съёмных дисков при подключении.
  - Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** и укажите максимальное пороговое значение объема данных в поле справа.
  - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съёмных дисков.

4. 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 к управлению службой Kaspersky Security Service в Kaspersky Security Center для группы компьютеров и для одного компьютера.

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

► Чтобы настроить права доступа к управлению программой и службой Kaspersky Security Service, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите 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 программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

- 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 2.1 для пользователей или группы пользователей, в блоке **Права пользователей на управление программой** нажмите на кнопку **Настройка**.
  - Если вы хотите настроить права доступа к управлению службой Kaspersky Security Service для пользователей или группы пользователей, в блоке **Права пользователей на управление службой** нажмите на кнопку **Настройка**.
4. В открывшемся окне настройте права доступа в соответствии с вашими требованиями.

Настроенные параметры будут сохранены.

## Настройка параметров карантина и резервного хранилища в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

► 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 компьютеров которой вы хотите настроить параметры программы.

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

- Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
- Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [159](#)).
- 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** в блоке **Хранилища** нажмите на кнопку **Настройка**.

4. В окне **Параметры хранилищ** на закладке **Резервное хранилище** настройте следующие параметры резервного хранилища:

- Если вы хотите задать папку-местоположение 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 группе параметров **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 ввода **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 ввода **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 вы можете настроить уведомление администратора и пользователей о следующих событиях, связанных с работой Kaspersky Embedded Systems Security 2.1 и состоянием антивирусной защиты защищаемого компьютера:

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

Вы можете настроить уведомления о событиях Kaspersky Embedded Systems Security 2.1 как для одного компьютера в окне **Свойства: <Имя 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 *Справочной системе 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 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

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 и уведомлений в Kaspersky Security Center .....	<a href="#">214</a>
Настройка параметров интеграции с SIEM.....	<a href="#">216</a>
Настройка параметров журналов и уведомлений в Kaspersky Security Center .....	<a href="#">221</a>
Настройка взаимодействия с Сервером администрирования .....	<a href="#">223</a>

# Настройка параметров журналов и уведомлений в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

► *Чтобы настроить параметры журналов Kaspersky Embedded Systems Security 2.1, выполните следующие действия:*

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите 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 программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
- Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [159](#)).

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 **Журналы выполнения задач** нажмите на кнопку **Настройка**.
4. В окне **Параметры журналов** настройте следующие параметры Kaspersky Embedded Systems Security 2.1:
  - Настройте уровень детализации событий в журналах. Для этого выполните следующие действия:
    - а. В списке **Компонент** выберите функциональный компонент Kaspersky Embedded Systems Security 2.1, уровень детализации событий которого вы хотите указать.
    - б. 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.

## 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 агрегации событий (SIEM), выполняющий сбор и анализ полученных событий, а также другие действия по управлению 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 2.1 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 28. 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	UDP	Вы можете настроить подключение к основному и дополнительному syslog-серверам по протоколам UDP или TCP с помощью выпадающего списка.

Параметр	Значение по умолчанию	Описание
Параметры подключения к основному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей.  Вы можете указать значение IP-адреса только в формате IPv4.
<b>Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен</b>	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 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей.  Вы можете указать значение IP-адреса только в формате IPv4.

► 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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.

- Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [159](#)).

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 **Журналы выполнения задач** нажмите на кнопку **Настройка**.

Откроется окно **Параметры журналов**.

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

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 принимающего syslog-сервера** выполните следующие действия:

- 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 параметры подключения к зеркальному syslog-серверу.

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 **ОК**.

Настроенные параметры интеграции с SIEM будут применены.

# Настройка параметров журналов и уведомлений в Kaspersky Security Center

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

► Чтобы настроить параметры журналов Kaspersky Embedded Systems Security 2.1, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите 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 программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

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 2.1 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**.
- На закладке **Пороги формирования событий** укажите интервалы времени, по истечении которых Kaspersky Embedded Systems Security 2.1 регистрирует события *Базы программы устарели, Базы программы сильно устарели, Проверка важных областей компьютера давно не выполнялась*:
  - **Базы устарели (сут).**

Количество дней с момента последнего обновления баз программы.

По умолчанию установлено 7 дней.
  - **Базы сильно устарели (сут).**

Количество дней с момента последнего обновления баз программы.

По умолчанию установлено 14 дней.
  - **Проверка важных областей компьютера давно не выполнялась (сут).**

Количество дней с момента последнего успешного завершения задачи проверки важных областей компьютера.

По умолчанию установлено 30 дней.

5. Нажмите на кнопку **ОК**.

Настроенные параметры уведомлений будут сохранены.

# Настройка взаимодействия с Сервером администрирования

► Чтобы выбрать типы объектов, информацию о которых Kaspersky Embedded Systems Security 2.1 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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

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 открывшемся окне выберите типы объектов, информацию о которых Kaspersky Embedded Systems Security 2.1 будет передавать на Сервер администрирования Kaspersky Security Center:

- Данные об объектах карантина.
- Данные об объектах резервного хранилища.

5. Нажмите на кнопку **ОК**.

Kaspersky Embedded Systems Security 2.1 будет передавать информацию о выбранных типах объектов на Сервер администрирования.



---

# Постоянная защита

Этот раздел содержит информацию о задачах постоянной защиты: задаче Постоянная защита файлов и задаче Использование KSN. Также этот раздел содержит инструкции по настройке параметров задач постоянной защиты и по настройке параметров безопасности защищаемого компьютера.

## В этом разделе

Постоянная защита файлов .....	<a href="#">225</a>
Использование KSN .....	<a href="#">242</a>
Защита от эксплойтов .....	<a href="#">247</a>

# 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 .....	<a href="#">226</a>
Настройка параметров задачи Постоянная защита файлов .....	<a href="#">226</a>
Область защиты в задаче Постоянная защита файлов.....	<a href="#">229</a>

## О задаче Постоянная защита файлов

В ходе выполнения задачи Постоянная защита файлов Kaspersky Embedded Systems Security 2.1 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.

Когда какая-нибудь программа записывает на компьютер или считывает с него файл, Kaspersky Embedded Systems Security 2.1 перехватывает этот файл, проверяет его на наличие угроз компьютерной безопасности и, если находит угрозу, выполняет действия, указанные в параметрах задачи вами или по умолчанию: пытается вылечить файл, перемещает файл на карантин или удаляет его. Kaspersky Embedded Systems Security 2.1 возвращает файл программе, если он не заражен или успешно вылечен.

## Настройка параметров задачи Постоянная защита файлов

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

Таблица 29. 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 <b>Рекомендуемый</b> .	Для выбранных узлов в дереве файловых ресурсов компьютера вы можете:

		<ul style="list-style-type: none"> <li>• применить другой предустановленный уровень безопасности;</li> <li>• вручную изменить уровень безопасности;</li> <li>• сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применить его для любого другого узла.</li> </ul>
Режим защиты объектов	При открытии и изменении.	Вы можете выбрать режим защиты объектов – указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security 2.1 проверяет их.
Эвристический анализатор	Применяется уровень безопасности <b>Средний.</b>	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.
Доверенная зона	Применяется.	Единый список исключений, который вы можете применять в выбранных задачах.
Использование служб KSN	Применяется	Вы можете увеличить эффективность защиты компьютера с помощью использования инфраструктуры облачных служб Kaspersky Security Network.
Расписание запуска задачи	При запуске программы	Вы можете настраивать параметры запуска задачи по расписанию.
Наполнение списка недоверенных компьютеров	Не применяется	Вы можете включить добавление компьютеров, со стороны которых выявлена вредоносная активность, в список недоверенных компьютеров в задаче Блокирование доступа к сетевым файловым ресурсам.

- Чтобы настроить параметры задачи *Постоянная защита файлов*, выполните следующие действия:

1. В дереве Консоли Kaspersky Security Center разверните узел **Управляемые устройства** и выполните следующие действия:

- Если вы хотите настроить параметры политики, в группе компьютеров выберите **Политики** → **<Имя политики>** → **Постоянная защита** → **Настройка** в блоке **Постоянная защита файлов**.
- Если вы хотите настроить параметры задачи для одного компьютера через Kaspersky Security Center, откройте окно **Параметры задачи** в Kaspersky Security Center (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

Откроется окно **Параметры**.

2. Настройте следующие параметры задачи:

- На закладке **Общие**:
  - Режим защиты объектов;
  - Применение эвристического анализатора;
  - Параметры интеграции с другими компонентами Kaspersky Embedded Systems Security 2.1.
- На закладке **Управление задачами**:
  - Параметры запуска задачи по расписанию.

3. Выберите закладку **Область защиты** и выполните следующие действия:

- Нажмите на кнопку **Добавить** или **Изменить**, чтобы отредактировать область защиты.
- В открывшемся окне выберите, что вы хотите включить в область защиты задачи:
  - **Предопределенная область**.
  - **Диск, папка или сетевой объект**.
  - **Файл**.

- Выберите один из предустановленных уровней безопасности или настройте параметры защиты объектов вручную.

Чтобы применить к задаче новые настройки области защиты, необходимо перезапустить задачу Постоянной защиты файлов.

4. В окне **Параметры** нажмите на кнопку **ОК**.

Kaspersky Embedded Systems Security 2.1 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после их изменения будут сохранены в журнале выполнения задачи.

## 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.

### Предопределенные 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 2.1 предусмотрены следующие предопределенные области защиты:

- **Локальные жесткие диски.** Kaspersky Embedded Systems Security 2.1 защищает файлы на жестких дисках компьютера.
- **Съемные диски.** Kaspersky Embedded Systems Security 2.1 защищает файлы на внешних устройствах, например, компакт-дисках или съемных дисках. 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 2.1 защищает файлы, которые записываются в сетевые папки или считываются из них программами, выполняемыми на компьютере. Kaspersky Embedded Systems Security 2.1 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 монтируются на компьютер временно, например, общие диски кластера.

Предопределенные области проверки по умолчанию отображаются в дереве файловых ресурсов компьютера и доступны для добавления в список файловых ресурсов при его формировании в параметрах области защиты.

По умолчанию в область защиты включены все предопределенные области, кроме виртуальных дисков.

Псевдодиски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов компьютера в Консоли Kaspersky Embedded Systems Security 2.1. Чтобы включить в область защиты объекты на псевдодиске, включите в область защиты папку на компьютере, с которой этот псевдодиск связан.

Подключенные сетевые диски также не отображаются в дереве 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 предустановленных уровней безопасности

Для выбранных узлов в списке файловых ресурсов компьютера вы можете применить один из следующих предустановленных уровней безопасности: **Максимальное быстрое действие**, **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, кроме использования Kaspersky Embedded Systems Security 2.1 на компьютерах, принимаются дополнительные меры компьютерной безопасности, например, настроены сетевые экраны и действуют политики безопасности для пользователей сети.

## Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и степени влияния на производительность защищаемых компьютеров. Этот уровень рекомендован специалистами "Лаборатории Касперского", как достаточный для защиты компьютеров в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

## Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если вы предъявляете повышенные требования к компьютерной безопасности в сети организации.

Таблица 30. Предустановленные уровни безопасности и соответствующие им значения параметров

Параметры	Уровень безопасности		
	Максимальное быстродействие	Рекомендуемый	Максимальная защита
Защита объектов	По расширению	По формату	По формату
Оптимизация	Включена	Включена	Выключена
Действие над зараженными и другими обнаруженными объектами	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно	Лечить, удалять, если лечение невозможно
Действие над возможно зараженными объектами	Помещать на карантин	Помещать на карантин	Помещать на карантин
Исключать объекты	Нет	Нет	Нет

Параметры	Уровень безопасности		
	Максимальное быстроедействие	Рекомендуемый	Максимальная защита
Останавливать проверку, если она длится более (сек.)	60 сек.	60 сек.	60 сек.
Не проверять составные объекты размером более (МБ)	8 МБ	8 МБ	Не установлен
Альтернативные потоки NTFS	Да	Да	Да
Загрузочные секторы дисков и MBR	Да	Да	Да
Защита составных объектов	<ul style="list-style-type: none"> <li>Упакованные объекты*</li> <li>Только новые и измененные</li> </ul>	<ul style="list-style-type: none"> <li>SFX-архивы*</li> <li>Упакованные объекты*</li> <li>Вложенные OLE-объекты*</li> <li>Только новые и измененные</li> </ul>	<ul style="list-style-type: none"> <li>SFX-архивы*</li> <li>Упакованные объекты*</li> <li>Вложенные OLE-объекты*</li> <li>*Все объекты</li> </ul>

Параметры **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Применение эвристического анализатора** не входят в набор параметров предустановленных уровней безопасности. Если, выбрав один из предустановленных уровней безопасности, вы измените состояние параметров безопасности **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор**, выбранный вами предустановленный уровень безопасности не изменится.



- Чтобы выбрать один из предустановленных уровней безопасности, выполните следующие действия:

1. В дереве Консоли Kaspersky Security Center разверните узел **Управляемые устройства** и выполните следующие действия:

- Если вы хотите настроить параметры политики, в группе компьютеров выберите **Политики** → **<Имя политики>** → **Постоянная защита** → **Настройка** в блоке **Постоянная защита файлов**.
- Если вы хотите настроить параметры задачи для одного компьютера через Kaspersky Security Center, откройте окно **Параметры задачи** в Kaspersky Security Center (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

Откроется окно **Параметры**.

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

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

3. Выберите требуемый уровень безопасности в раскрывающемся списке:

- **Максимальная защита**
- **Рекомендуемый**
- **Максимальное быстродействие**

4. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Kaspersky Embedded Systems Security 2.1 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи 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. Их значения соответствуют значениям предустановленного уровня безопасности **Рекомендуемый**.

Вы можете изменять значения параметров безопасности по умолчанию, 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 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 Kaspersky Security Center разверните узел **Управляемые устройства** и выполните следующие действия:

- Если вы хотите настроить параметры политики, в группе компьютеров выберите **Политики** → **<Имя политики>** → **Постоянная защита** → **Настройка** в блоке **Постоянная защита файлов**.
- Если вы хотите настроить параметры задачи для одного компьютера через Kaspersky Security Center, откройте окно **Параметры задачи** в Kaspersky Security Center (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

Откроется окно **Параметры**.

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

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

3. Выберите требуемый уровень безопасности в раскрывающемся списке:

- **Максимальная защита**
- **Рекомендуемый**

- **Максимальное быстродействие**
- **Другой**

4. Нажмите на кнопку **Настройка**, чтобы изменить нужные параметры безопасности выбранного узла в соответствии с вашими требованиями. Для этого выполните следующие действия:

- На закладке **Общие**, если требуется, настройте следующие параметры:

В блоке **Защита объектов** укажите объекты, которые вы хотите включить в область защиты:

- **Все объекты.**

Kaspersky Embedded Systems Security 2.1 проверяет все объекты.

- **Объекты, проверяемые по формату.**

Kaspersky Embedded Systems Security 2.1 проверяет только потенциально заражаемые файлы на основании формата файла.

Список форматов составляется специалистами "Лаборатории Касперского" и входит в состав баз Kaspersky Embedded Systems Security 2.1.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах.**

Kaspersky Embedded Systems Security 2.1 проверяет только потенциально заражаемые файлы на основании расширения файла.

Список расширений составляется специалистами "Лаборатории Касперского" и входит в состав баз Kaspersky Embedded Systems Security 2.1.

- **Объекты, проверяемые по указанному списку расширений.**

Kaspersky Embedded Systems Security 2.1 проверяет файлы на основании расширения файла. Список расширения файлов, которые нужно проверять, вы можете задать вручную по кнопке **Изменить** в окне **Список расширений**.

- **Загрузочные секторы дисков MBR.**

Включение защиты загрузочных секторов дисков и главных загрузочных записей.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет загрузочные секторы и загрузочные надписи 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, Kaspersky Embedded Systems Security 2.1 проверяет дополнительные потоки файлов и папок.

По умолчанию флажок установлен.

В блоке **Оптимизация** установите или снимите флажок:

- **Проверка только новых и измененных файлов.**

Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Embedded Systems Security 2.1 новыми или измененными с момента последней проверки.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет и защищает все файлы.

По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**. Если установлен уровень безопасности **Рекомендуемый** или **Максимальная защита**, то флажок снят.

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 2.1 проверяет архивы.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает архивы при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые SFX-архивы.**

Проверка архивов, имеющих в своем составе программный модуль-распаковщик.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет SFX-архивы.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 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 2.1 проверяет файлы почтовых баз.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 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 2.1 проверяет исполняемые файлы, упакованные программами-упаковщиками.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает исполняемые файлы, упакованные программами-упаковщиками, при проверке.

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 2.1 проверяет файлы почтовых форматов.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 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 2.1 проверяет встроенные в файл объекты.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 пропускает встроенные в файл объекты при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

Вы можете выбрать защиту всех или только новых составных объектов, если установлен флажок **Защита только новых и измененных файлов**. Если флажок **Защита только новых и измененных файлов** снят, Kaspersky Embedded Systems Security 2.1 защищает все указанные составные объекты.

- На закладке **Действия**, если требуется, настройте следующие параметры:
  - выберите действие над зараженными и другими обнаруживаемыми объектами;
  - выберите действие над возможно зараженными объектами;
  - настройте действия над объектами в зависимости от типа обнаруженного объекта;
  - выберите действия над неизменяемыми контейнерами: снимите или установите флажок **Форсировать удаление родительского файла-контейнера при обнаружении вложенного зараженного или другого объекта**, если изменение контейнера невозможно.

Флажок включает или выключает форсированное удаление родительского файла-контейнера при обнаружении вложенного вредоносного или другого обнаруживаемого объекта.

Если флажок установлен и в качестве действия над зараженными и возможно зараженными объектами выбрано действие **Удалять**, Kaspersky Embedded Systems Security 2.1 принудительно выполняет удаление всего родительского контейнера при обнаружении вложенного вредоносного или другого обнаруживаемого объекта. Принудительное удаление родительского контейнера со всем его содержимым выполняется в случае, если программа не может удалить только вложенный обнаруженный объект (например, если родительский контейнер неизменяем).

Если флажок снят и в качестве действия над зараженными и возможно зараженными объектами выбрано действие **Удалять**, Kaspersky Embedded Systems Security 2.1 не выполняет указанное действие для родительского контейнера при обнаружении вложенного вредоносного или другого обнаруживаемого объекта в случае, если родительский контейнер неизменяем.

По умолчанию флажок установлен для уровня безопасности **Максимальная защита**. По умолчанию флажок снят для уровней безопасности **Рекомендуемый** и **Максимальное быстрое действие**.

- На закладке **Производительность**, если требуется, настройте следующие параметры:

В блоке **Исключения**:

- **Исключать файлы.**

Исключение файлов из проверки по имени файла или маске имени файла.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет все объекты.

По умолчанию флажок снят.

- **Не обнаруживать.**

Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Вы можете найти список имен обнаруживаемых объектов на сайте Вирусной энциклопедии (<http://www.securelist.ru>).

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает при проверке указанные обнаруживаемые объекты.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

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. По умолчанию установлено значение 8 МБ.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет составные объекты, не учитывая размер.

По умолчанию флажок установлен для уровней безопасности **Рекомендуемый** и **Максимальное быстрое действие**.



- **Использовать технологию iChecker.**

Проверка только новых или измененных с момента последней проверки файлов.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет только новые или изменившиеся с момента последней проверки файлы.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет файлы, не учитывая дату создания и изменения.

По умолчанию флажок установлен.

- **Использовать технологию iSwift.**

Проверка только новых или измененных с момента последней проверки объектов файловой системы NTFS.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 проверяет объекты файловой системы NTFS, не учитывая дату создания и изменения.

По умолчанию флажок установлен.

5. Нажмите на кнопку **ОК**.

6. Настроенные параметры задачи будут сохранены.

# 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 .....	<a href="#">242</a>
Настройка параметров задачи Использование KSN .....	<a href="#">243</a>
Настройка обработки данных .....	<a href="#">247</a>

## 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, интернет-ресурсов и программ. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Embedded Systems Security 2.1 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 2.1 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 подробно о передаче, обработке, хранении и уничтожении информации об использовании программы вы можете прочитать в Положении о KSN в окне передачи данных задачи Использование KSN, а также ознакомившись с [Политикой 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 2.1. 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 2.1:

- Постоянная защита файлов.
- Проверка по требованию.
- Контроль запуска программ.

### Использование Локального KSN

Подробную информацию о том, как настроить Локальный Kaspersky Security Network (также "Kaspersky Private Security Network"), вы можете прочитать 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. [247](#)) задачи Использование KSN вы можете прочитать Положение о KPSN и включить или выключить использование компонента в любой момент с помощью флажка **Я принимаю условия участия в Kaspersky Private Security Network**. Принимая условия, вы соглашаетесь отправлять все типы данных (запросы безопасности, статистические данные), предусмотренные в Положении о KPSN, в службы KSN.

После принятия условий Локального KSN, флажки, регулирующие использование Глобального KSN, недоступны.

Если вы выключаете использование Локального KSN во время работы задачи Использование KSN, происходит ошибка *Нарушение лицензии*, и задача останавливается. Чтобы продолжить защищать компьютер, вам требуется принять Положение о KSN в окне **Обработка данных** и перезапустить задачу.

# Настройка параметров задачи Использование KSN

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

Таблица 31. Параметры по умолчанию задачи Использование KSN

Параметр	Значение по умолчанию	Описание
Действия над объектами, недоверенными в KSN	Удалить	Вы можете указывать действия, которые Kaspersky Embedded Systems Security 2.1 будет выполнять над объектами, имеющими репутацию зараженных в KSN.
Отправка данных	Контрольная сумма файла (хеш MD5) 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 2.1 рассчитывает хеш MD5 для файлов любого размера.
Положение о KSN	Флажок <b>Я принимаю условия участия в Kaspersky Security Network</b> снят.	Вы можете изменять свое решение об использовании KSN в любой момент.
Отправлять статистику Kaspersky Security Network	Флажок установлен (Активно, если принятно Положение о KSN)	Если вы приняли Положение о KSN, статистика будет отправляться автоматически, пока вы не снимите флажок.

Параметр	Значение по умолчанию	Описание
<b>Отправлять данные о проверенных файлах</b>	Флажок установлен (Активно, если принятно Положение о KSN)	Положение о KSN принято, данные о файлах, которые были проверены и проанализированы с момента запуска задачи, отправляются. Снять флажок можно в любой момент.
<b>Использовать Kaspersky Security Center как прокси-сервер KSN</b>	Флажок установлен	По умолчанию все данные отправляются в KSN через Kaspersky Security Center.
Расписание запуска задачи	Следующий запуск не определен.	Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

► Чтобы настроить параметры задачи *Использование KSN*, выполните следующие действия:

- В дереве Консоли Kaspersky Security Center разверните узел **Управляемые устройства** и выполните следующие действия:
  - Если вы хотите изменить параметры компьютера, в группе компьютеров выберите **Политики** → **<Имя политики>** → **Постоянная защита** → **Параметры** (блок **Использование KSN**).
  - Если вы хотите настроить параметры программы для одного компьютера через Kaspersky Security Center, откройте окно "Свойства" в Kaspersky Security Center (см. раздел "Настройка локальных задач в окне параметров программы в Kaspersky Security Center" на стр. 147).

Откроется окно **Параметры**.

- В разделе **Постоянная защита** нажмите кнопку **Настройка** в блоке **Использование KSN**.

Откроется окно **Параметры задачи**.

- На закладке **Общие** настройте следующие параметры задачи:

- В блоке **Действия над объектами, недоверенными в KSN** укажите действие, которое Kaspersky Embedded Systems Security 2.1 необходимо совершить при обнаружении объекта, имеющего репутацию недоверенного в KSN:
  - **Удалить**  
Kaspersky Embedded Systems Security 2.1 удаляет зараженный по данным KSN объект и помещает его копию в резервное хранилище.  
Этот вариант выбран по умолчанию.
  - **Фиксировать информацию в отчете**  
Kaspersky Embedded Systems Security 2.1 фиксирует в журнале выполнения задач информацию об обнаруженном зараженном по данным KSN объекте. Kaspersky Embedded Systems Security 2.1 не удаляет зараженный 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 2.1 не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (МБ).  
Если флажок снят, Kaspersky Embedded Systems Security 2.1 рассчитывает контрольную сумму для файлов любого размера.  
По умолчанию флажок установлен.
  - Если требуется, в поле справа укажите максимальный размер файлов, для которых Kaspersky Embedded Systems Security 2.1 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 отправляются в KSN напрямую (не через Kaspersky Security Center). Активная политика определяет, какой тип данных отправляется в KSN.

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 *Справочной системе Kaspersky Security Center*.

4. Если требуется, настройте расписание запуска задачи на закладке **Управление задачами**. Например, вы можете включить запуск задачи по расписанию и указать частоту запуска задачи **При запуске программы**, если хотите, чтобы задача автоматически запускалась после перезагрузки сервера.

Программа будет запускать задачу Использование KSN по расписанию.

5. Настройте обработку данных (см. раздел "Настройка обработки данных" на стр. [247](#)) перед запуском задачи.
6. Нажмите на кнопку **ОК**.

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 Kaspersky Security Center разверните узел **Управляемые устройства** и выполните следующие действия:
  - Если вы хотите изменить параметры компьютера, в группе компьютеров выберите **Политики** → **<Имя политики>** → **Постоянная защита** → **Параметры** (блок **Использование KSN**).

- Если вы хотите настроить параметры программы для одного компьютера через Kaspersky Security Center, откройте окно **Свойства** в Kaspersky Security Center (см. раздел "Настройка локальных задач в окне параметров программы в Kaspersky Security Center" на стр. 147).

Откроется окно **Параметры**.

2. В разделе **Постоянная защита** нажмите кнопку **Обработка данных** в блоке **Использование KSN**.

Откроется окно **Обработка данных**.

3. Прочитайте Положение о Kaspersky Security Network (или Положение о Kaspersky Private Security Network, если вы используете Локальный KSN).
4. Если вы принимаете условия, упомянутые в Положении о KSN, установите флажок **Я принимаю условия участия в Kaspersky Security Network**.
5. Для повышения уровня защиты следующие флажки установлены по умолчанию:

- **Отправлять данные о проверенных файлах.**

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 отправляет контрольную сумму проверенных файлов в "Лабораторию Касперского". Заключение о безопасности каждого файла основано на репутации, полученной от KSN.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 не отправляет контрольную сумму файлов в KSN.

По умолчанию флажок установлен.

- **Отправлять статистику Kaspersky Security Network.**

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 отправляет дополнительную статистику, включая персональные данные. Данные, полученные "Лабораторией Касперского", используются для улучшения качества программ и повышения скорости обнаружения угроз.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 не отправляет дополнительную статистику.

По умолчанию флажок установлен.

Вы можете снять флажки и прекратить передачу дополнительных данных в любой момент.

6. Нажмите на кнопку **ОК**.



# Защита от эксплойтов

Этот раздел содержит инструкции по настройке параметров защиты памяти процессов от эксплуатации уязвимостей.

## В этом разделе

О защите от эксплойтов .....	<a href="#">249</a>
Настройка параметров защиты памяти процессов .....	<a href="#">251</a>
Добавление защищаемого процесса .....	<a href="#">254</a>
Техники снижения рисков .....	<a href="#">256</a>

## О защите от эксплойтов

Kaspersky Embedded Systems Security 2.1 предоставляет возможность защиты памяти процессов от эксплойтов, которая реализуется 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 2.1, 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. Для выполнения удаления компонента при наличии защищенных процессов в системе может потребоваться перезагрузка защищаемого компьютера.

При обнаружении признаков атаки эксплойта на защищаемый процесс Kaspersky Embedded Systems Security 2.1 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.

Если при удалении Агент внедрен хотя бы в один из защищаемых процессов, требуется перезагрузка защищаемого компьютера.

### **Служба Kaspersky Security Broker Host**

Для максимальной эффективности выполнения функций компоненту Защита от эксплойтов требуется наличие службы Kaspersky Security Broker Host на защищаемом компьютере. Эта служба входит в состав рекомендуемой установки совместно с компонентом Защита от эксплойтов. Во время установки службы на защищаемом компьютере создается и запускается процесс kavfswb, который обеспечивает сообщение информации о защищаемых процессах от компонента к Агенту защиты.

После остановки службы Kaspersky Security Broker Host Kaspersky Embedded Systems Security 2.1 продолжает защищать процессы, которые были добавлены в список защищаемых, а также загружается в новые добавленные процессы и применяет все доступные техники снижения рисков для защиты памяти процессов.

В случае остановки службы Kaspersky Security Broker Host программа не будет получать данные о событиях, происходящих с защищаемыми процессами (в том числе, данные об

атаках эксплойтов, 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 2.1 не выполняет завершение такого процесса, независимо от режима, указанного в параметрах компонента Защита от эксплойтов.

- Только сообщать об эксплойте: 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 2.1 фиксирует 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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

- Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
- Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [159](#)).

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** в блоке **Защита от эксплойтов** нажмите на кнопку **Настройка**.

Откроется окно **Защита процессов**.

4. Выберите закладку **Параметры защиты памяти процессов**.
5. В блоке **Защита памяти процессов** настройте следующие параметры:

- **Защищать память процессов от эксплуатации уязвимостей в режиме.**

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 не защищает процессы на компьютере от эксплуатации уязвимостей.

По умолчанию флажок снят.

- **Завершать скомпрометированные процессы.**

Если выбран данный режим, Kaspersky Embedded Systems Security 2.1 завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника

снижения рисков.

- **Только статистика.**

Если выбран данный режим, Kaspersky Embedded Systems Security 2.1 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 2.1 обнаруживает факт эксплуатации уязвимости критического процесса, компонент принудительно переходит в режим *Только сообщать об эксплойте*.

6. В блоке **Действия по снижению рисков** настройте следующие параметры:

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

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 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 2.1 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 Broker Host.

По умолчанию флажок установлен.

- **Применять защиту от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security.**

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 будет снижать риски эксплуатации уязвимостей уже запущенных процессов не зависимо от статуса выполнения службы Kaspersky Security. Kaspersky Embedded Systems Security 2.1 не будет защищать

процессы, которые были добавлены 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 2.1 не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

По умолчанию флажок установлен.

7. Нажмите на кнопку **ОК**.

## Добавление защищаемого процесса

► 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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

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** в блоке **Защита от эксплойтов** нажмите на кнопку **Настройка**.

Откроется окно **Защита памяти процессов**.

4. Нажмите на кнопку **Обзор**.

Откроется стандартное окно Microsoft Windows **Открыть**.

5. В открывшемся окне выберите процесс, который вы хотите добавить в список.

6. Нажмите на кнопку **Открыть**.

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 снижения рисков**.

9. Выберите один из вариантов применения техник снижения рисков:

- **Применять все доступные техники снижения рисков.**

Если выбран этот вариант, редактирование списка недоступно, все техники применяются по умолчанию.

- **Применять указанные техники снижения рисков.**

Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска:

- а. Установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.
- б. Установите или снимите флажок **Применять технику снижения рисков Attack Surface Reduciton**.

10. Настройте параметры работы для техники снижения рисков **Attack Surface Reduciton**:

- Внесите названия модулей, которые будут запрещены к запуску из защищаемого процесса в поле **Запрещать модули**.
- 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**.

## Техники снижения рисков

Таблица 32. Техники снижения рисков

Техника снижения рисков	Описание
Data Execution Prevention (DEP)	Предотвращение выполнения данных - запрет исполнения произвольного кода в защищенной области памяти.
Address Space Layout Randomization (ASLR)	Изменение расположения структур данных в адресном пространстве процесса.
Structured Exception Handler Overwrite Protection (SEHOP)	Подмена записи в структуре исключений или подмена обработчика исключений.
Null Page Allocation	Предотвращение переориентации нулевого указателя.



LoadLibrary Network Call Check (Anti ROP)	Защита от загрузки динамических библиотек с сетевых путей.
Executable Stack (Anti ROP)	Запрет на несанкционированное исполнение областей стека.
Anti RET Check (Anti ROP)	Проверка безопасного вызова функции через CALL инструкцию.
Anti Stack Pivoting (Anti ROP)	Защита от перемещения указателя стека ESP на эксплуатируемый адрес.
Export Address Table Access Moitor (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
Heapspray Allocation	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	Блокирование запуска уязвимых модулей через защищаемый процесс.

---

# Контроль активности на компьютерах

Этот раздел содержит информацию о функциональности Kaspersky Embedded Systems Security 2.1, которая позволяет контролировать запуски программ, подключения флеш-накопителей и других внешних устройств по USB, а также контролировать работу сетевого экрана Windows.

## В этом разделе

Управление запуском программ из Kaspersky Security Center.....	<a href="#">258</a>
Управление подключением устройств из Kaspersky Security Center .....	<a href="#">284</a>

## 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 .....	<a href="#">259</a>
Настройка параметров задачи Контроль запуска программ.....	<a href="#">261</a>
Настройка контроля распространения программного обеспечения.....	<a href="#">267</a>
О формировании правил контроля запуска программ для всей сети через Kaspersky Security Center .....	<a href="#">274</a>

# 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 добавлены компьютеры разных типов, для контроля запуска программ на каждом из них могут потребоваться индивидуальные списки правил. Для того, чтобы разграничить применение политики к компьютерам внутри одной группы администрирования, вы можете 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 компьютера, так как заданные правила контролируют запуски только тех программ, которые характерны для данного типа компьютера.

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 *Справочной системе 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, входящего в группу администрирования, в соответствии с типом компьютера. Для этого выполните следующие действия:
  - В панели результатов выбранной группы администрирования откройте закладку **устройства** и выберите компьютер, для которого хотите назначить теги. В окне **Свойства: <Имя компьютера>** выбранного компьютера откройте раздел **Теги** и сформируйте список тегов. Нажмите на кнопку **ОК**.
3. Создайте профиль политики и настройте его применение для защиты компьютеров внутри группы 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 **ОК**.
4. Нажмите на кнопку **ОК** в окне **Свойства: <Имя политики>**.

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 33. Параметры задачи Контроль запуска программ по умолчанию

Параметр	Значение по умолчанию	Описание
Режим работы задачи	<b>Только статистика.</b> Задача фиксирует события блокировки и запуска программ в соответствии с заданными правилами в журнале выполнения. Фактическая блокировка запуска программ не выполняется.	Вы можете выбрать режим <b>Применять правила контроля запуска программ</b> для защиты компьютера после того, как будет сформирован окончательный список правил.
Правила	<b>Заменить правилами политики локальные правила.</b>	Вы можете выбрать режим совместного применения правил, заданных в политике, и правил на локальном компьютере.
Область применения правил в задаче	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 программ с помощью пакетов установки	Флажок снят	Вы можете разрешать распространение программного обеспечения с помощью указанных в настройках пакетов установки и программ. По умолчанию разрешено только распространение программ с помощью службы Windows Installer.
Расписание запуска задачи	Первый запуск не определен.	Задача Контроль запуска программ не запускается автоматически при старте Kaspersky Embedded Systems Security 2.1. 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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

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 списке **Режим работы задачи Контроль запуска программ** укажите режим выполнения задачи.

В раскрывающемся списке вы можете выбрать один из режимов работы задачи Контроль запуска программ:

- **Применять правила контроля запуска программ.** Kaspersky Embedded Systems Security 2.1 контролирует запуск программ с помощью заданных правил.
- **Только статистика.** Kaspersky Embedded Systems Security 2.1 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, зафиксированной в журнале выполнения задач.

По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.

- Снимите или установите флажок **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска**.

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

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 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 2.1 проверяет программу при каждом ее последующем запуске заново.

По умолчанию флажок установлен.

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

- Нажмите на кнопку **Список правил**, чтобы добавить разрешающие правила контроля запуска задач.
- Выберите режим применения правил:

- **Заменить правилами политики локальные правила**

Программа применяет список правил, заданный в политике, для централизованного контроля запусков 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 автоматической генерации правил контроля запуска программ.

По умолчанию Kaspersky Embedded Systems Security 2.1 применяет два предопределенных правила, которые разрешают запуск скриптов, пакетов MSI 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 2.1 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 2.1 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 2.1 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 2.1 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 2.1 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 2.1 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:

- **Запрещать запуск программ, недоверенных в KSN.**

Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 запрещает запуск программ, имеющих статус недоверенных в KSN. При этом разрешающие правила контроля запуска программ, под которые попадают недоверенные в KSN программы, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 не учитывает репутацию недоверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые попадают 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 2.1 разрешает запуск программ, имеющих статус доверенных в KSN. При этом запрещающие правила контроля запуска программ, под которые попадают 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 2.1 не учитывает репутацию доверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые попадают 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 распространения программного обеспечения.
  9. На закладках **Расписание** и **Дополнительно** настройте параметры запуска задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. [187](#)).
  10. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Kaspersky Embedded Systems Security 2.1 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 контроля распространения программного обеспечения

Формирование правил контроля запуска программ может значительно усложняться, если вам требуется учитывать распространение программного обеспечения 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 соответствующую подсистему задачи Контроль запуска программ.

Подсистема *Контроль распространения программного обеспечения* реализована в виде дополнительного списка исключений. Вы можете добавлять в этот список доверенные пакеты установки (далее также “*доверенные пакеты*”) – программа будет разрешать распаковку доверенных пакетов и автоматический запуск программного обеспечения, установленного и измененного доверенным пакетом.

Учитывайте, что программа контролирует только полный цикл распространения программного обеспечения. Kaspersky Embedded Systems Security 2.1 не сможет корректно обработать запуски файлов, измененных доверенным пакетом, если при первом запуске такого пакета установки контроль распространения программного обеспечения отключен или не установлен компонент *Контроль запуска программ*.

Контроль распространения программного обеспечения невозможен, если в настройках задачи *Контроль запуска программ* не установлен флажок **Использовать правила для исполняемых файлов**.

### **Кеш контроля распространения программного обеспечения**

Kaspersky Embedded Systems Security 2.1 определяет связь между файлами, созданными при распространении программного обеспечения, и доверенными пакетами с помощью динамического формирования *кеша контроля распространения программного обеспечения* (далее – *кеш распространения*). При первом запуске доверенного пакета, Kaspersky Embedded Systems Security 2.1 обнаруживает все файлы, созданные при распространении программного обеспечения с помощью данного 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 2.1 самостоятельно наполняет его, а также контролирует его актуальность.

Вы можете экспортировать кеш распространения в конфигурационный файл (в формате XML), а также полностью 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 2.1 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.

### **Взаимодействие с основным списком правил контроля запуска программ**

Список доверенных пакетов подсистемы контроля распространения программного обеспечения – 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 распространения программного обеспечения 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 заключения KSN имеют больший приоритет, чем исключение контроля распространения программного обеспечения: распаковка доверенного пакета установки или запуск созданных и измененных им файлов будут заблокированы, если для таких файлов получено недоверенное заключение от KSN.

► 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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

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 с помощью указанных программ и пакетов установки**.

Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью указанных в списке программ и пакетов установки.

Если флажок установлен, программа автоматически разрешает запуск файлов, 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 Windows Installer**.

Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью подсистемы Windows Installer.

Если флажок установлен, программа всегда разрешает запуск файлов, установленных с помощью Windows Installer.

Если флажок снят, использование Windows Installer 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 Windows Installer** рекомендуется снимать только в случае крайней необходимости. Снятие флажка может привести к проблемам при обновлении файлов операционной системы, а также блокированию запуска файлов, дочерних по отношению к доверенным пакетам 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 2.1 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 цикл распространения программного обеспечения от доставки пакета на компьютер до факта установки/обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки системы на компьютере.

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 файл запуска программы или пакет установки.

Блок **Критерии доверенности** автоматически заполнится данными о выбранном файле.

- b. 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.

Этот вариант выбран по умолчанию.

- **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 рекомендуется применять, если требуется создать максимально надежные правила: контрольная сумма, рассчитанная по алгоритму SHA256, является уникальным идентификатором файла. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.

- **Добавить несколько по хешу.**

Вы можете выбрать неограниченное число файлов запуска и пакетов установки и добавить их в список одновременно. Kaspersky Embedded Systems Security 2.1 учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

- **Изменить выбранный.**

Используйте этот вариант, чтобы выбрать другой файл запуска или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла.**

Вы можете импортировать список доверенных пакетов установки из сохраненного конфигурационного файла. Распознаваемый Kaspersky Embedded Systems Security 2.1 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 вложенных файлов будет разрешен.

Чтобы запретить запуск вложенных файлов, полностью удалите программу с защищаемого компьютера или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

9. Нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

## О формировании правил контроля запуска программ для всей сети через Kaspersky Security Center

Вы можете создавать 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 автоматической генерации разрешающих правил по программам, установленным на такой эталонной машине.

Вы можете создавать списки правил контроля запуска программ на стороне Kaspersky Security Center двумя способами:

- С помощью групповой задачи генерации правил контроля запуска программ.

При использовании этого сценария групповая задача формирует для каждого компьютера в сети свой список правил контроля запуска программ и сохраняет эти списки в XML-файл в указанной общей папке сети. Далее вы можете вручную импортировать сформированные списки правил в задачу Контроль запуска программ в политике Kaspersky Security Center. В отличие от задачи на локальном компьютере, в политике на стороне Kaspersky Security Center вы не можете настроить автоматическое добавление созданных правил в список правил контроля запуска программ по завершении групповой задачи генерации правил контроля запуска программ.

Рекомендуется использовать этот сценарий, если необходимо сформировать списки правил контроля запуска программ в короткие сроки. Запуск задачи Генерация 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 устройств сети убедитесь, что для всех защищаемых компьютеров настроен доступ к общей сетевой папке. В случае, если применение общей сетевой папки в работе компьютеров сети не предусматривается политикой организации, рекомендуется запускать задачи автоматического формирования разрешающих правил контроля компьютера на тестовой группе компьютеров или на эталонной машине организации.

- На основе отчета о событиях задачи, сформированного в Kaspersky Security Center по работе задачи Контроль запуска программ в режиме **Только статистика**.

При использовании этого сценария Kaspersky Embedded Systems Security 2.1 не блокирует запуски программ, но фиксирует в разделе **События** Kaspersky Security Center все запуски и блокировки запусков программ на всех компьютерах сети за

период работы задачи контроля запуска программ в режиме **Только статистика**. Затем Kaspersky Security Center создает на основе журнала выполнения задачи единый список событий блокирования программ.

Вам нужно 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. [259](#)).

- На основе событий о блокировании программ, полученном 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 сети (например, при установке обновлений или переустановке операционной системы). Рекомендуется формировать обновленный список правил с помощью групповой задачи Генерация правил контроля запуска программ или с помощью политики Контроль запуска программ в режиме **Только статистика**, выполняемых на компьютерах тестовой группы администрирования. Тестовая группа администрирования включает компьютеры, необходимые для проверочного 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. [261](#)). В списке правил политики Kaspersky Security Center отображаются только те правила, которые заданы в этой политике, вне зависимости от режима применения правил. В списке правил локального компьютера отображаются все применяющиеся правила - и локальные, и добавленные через политику.

## Создание разрешающих правил из событий Kaspersky Security Center

- Чтобы сформировать разрешающие правила с помощью опции **Создать разрешающие правила программ из событий Kaspersky Security Center** в параметрах политики **Контроль запуска программ**, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для компьютеров которой вы хотите настроить параметры программы.
2. Выберите закладку **Политики**.
3. В контекстном меню выбранной политики выберите пункт **Свойства**.

Откроется окно **Свойства: <Имя политики>**.

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 пункт **Создать разрешающие правила программ из событий Kaspersky Security Center**.
6. 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.

7. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

Список правил в политике Контроль запуска программ будет дополнен новыми правилами, сформированными на основе данных системы компьютера, на котором установлена Консоль администрирования Kaspersky Security Center.

Если список правил контроля запуска программ уже задан в политике, Kaspersky Embedded Systems Security 2.1 добавит выбранные правила из событий блокирования к уже заданным правилам.

## Импорт правил контроля запуска программ из файла формата XML

Вы можете импортировать отчеты, сформированные по результатам выполнения групповой задачи Генерация 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 сети организации. Списки содержат разрешающие правила для запуска файлов и программ, тип которых соответствует параметрам, указанным в групповой задаче автоматического формирования правил.

Процедура настройки параметров функциональных компонентов Kaspersky Embedded Systems Security 2.1 в Kaspersky Security Center аналогична процедуре настройки этих компонентов в локальной Консоли Kaspersky Embedded Systems Security 2.1. Инструкции по настройке параметров задач и функций программы в Консоли Kaspersky Embedded Systems Security 2.1 содержатся в соответствующих разделах *Руководства пользователя Kaspersky Embedded Systems Security 2.1*.

► 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 Генерация правил контроля запуска программ или выберите уже созданную задачу.
2. В свойствах созданной групповой задачи Генерация правил контроля запуска программ или в мастере создания задачи настройте следующие параметры:
  - В разделе **Уведомления** настройте параметры сохранения отчета выполнения задачи.

Подробная инструкция по настройке параметров в этом разделе содержится в *Справочной системе 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 разделе **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 разделе **Расписание** настройте параметры запуска задачи по расписанию.
- В разделе **Учетная запись** укажите учетную запись пользователя, с правами которой будет выполняться задача.

- В разделе **Исключения из области действия задачи** задайте группы компьютеров, которые требуется исключить из области действия задачи.

Kaspersky Embedded Systems Security 2.1 не будет создавать разрешающие правила по программам, запускаемым на исключенных компьютерах.

3. На закладке **Задачи** в панели управления настраиваемой группы компьютеров в списке групповых задач выберите созданную задачу автоматического формирования разрешающих правил 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 сети убедитесь, что для всех защищаемых компьютеров настроен доступ к общей сетевой папке. В случае, если применение общей сетевой папки в работе компьютеров сетине предусматривается политикой организации, рекомендуется запускать задачи автоматического формирования разрешающих правил контроля компьютера на тестовой группе компьютеров или на эталонной машине организации.

4. Добавьте сформированные списки разрешающих правил в задачу контроля запуска программ. Для этого в свойствах настраиваемой политики в параметрах задачи Контроль запуска программ выполните следующие действия:

- а. На закладке **Общие** нажмите на кнопку **Список правил**.

Откроется окно **Правила контроля запуска программ**.

- б. Нажмите на кнопку **Добавить** и в открывшемся списке выберите пункт **Импортировать правила из файла формата XML**.

- в. 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 Генерация 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 **Применять правила контроля запуска программ**.

Разрешающие правила, автоматически сформированные на основе запусков задач на каждом отдельном компьютере, будут применены для всех компьютеров в сети, для которых применяется настраиваемая политика. Для этих компьютеров программа будет разрешать запуски 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 контроля запуска программ, вы можете отследить, запуск каких программ будет блокироваться.

При импорте из отчета данных о заблокированных программах в настройки 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 из Kaspersky Security Center о заблокированных программах, выполните следующие действия:

1. В свойствах политики в параметрах задачи Контроль запуска программ установите режим работы **Только статистика**.
2. В свойствах политики в разделе **События** убедитесь, что:
  - На закладке **Критическое событие** 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 зафиксированные события в файл формата TXT. Для этого в свойствах задачи Контроль запуска программ разверните узел **Отчеты и уведомления** и во вложенном узле **События** создайте выборку событий по характеристике *Запрещен*, чтобы просмотреть, запуск каких программ будет блокироваться задачей Контроля запуска программ. В панели результатов созданной

выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных запусках программ в файл формата TXT.

Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех программах, запуск которых 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:

а. На закладке **Общие** нажмите на кнопку **Список правил**.

Откроется окно **Правила контроля запуска программ**.

б. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать данные о заблокированных программах из отчета Kaspersky Security Center**.

с. 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.

- е. 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 запрещать или разрешать подключение флеш-накопителей и других запоминающих устройств ко всем компьютерам в сети, формируя единые списки правил контроля устройств на стороне Kaspersky Security Center для групп компьютеров.

### В этом разделе

О формировании правил контроля устройств для всей сети через Kaspersky Security Center .....	<a href="#">284</a>
Создание правил на основе данных системы о внешних устройствах, подключавшихся к компьютерам сети.....	<a href="#">287</a>
Импорт правил из файла отчета Kaspersky Security Center о заблокированных устройствах.....	<a href="#">292</a>

## О формировании правил контроля устройств для всей сети через Kaspersky Security Center

Вы можете создавать списки правил контроля устройств с помощью задач и политик 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 Генерация правил контроля устройств.

При использовании этого сценария групповая задача формирует списки правил на основе данных системы каждого компьютера обо всех когда-либо подключавшихся флеш-накопителях и других запоминающих устройствах. Задача также учитывает все запоминающие устройства, подключенные в момент выполнения групповой задачи. По завершении выполнения групповой задачи, Kaspersky Embedded Systems Security 2.1 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 сети убедитесь, что для всех защищаемых компьютеров настроен доступ к общей сетевой папке. В случае, если применение общей сетевой папки в работе компьютеров сетине предусматривается политикой организации, рекомендуется запускать задачи автоматического формирования разрешающих правил контроля компьютера на тестовой группе компьютеров или на эталонной машине организации.

- На основе отчета, сформированного в Kaspersky Security Center, о событиях в работе задачи Контроль устройств в режиме **Только статистика**.

При использовании этого сценария Kaspersky Embedded Systems Security 2.1 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 контроля 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 2.1 формирует разрешающие правила для устройств, подключавшихся ранее или подключенных в текущий момент к компьютеру, на котором установлена консоль управления 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 устройств, подключенных в текущий момент**).

При использовании этого сценария Kaspersky Embedded Systems Security 2.1 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 2.1 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 на основе информации Windows о когда-либо подключавшихся или подключенных в текущий момент запоминающих устройствах тремя способами (см. раздел "О формировании правил контроля устройств для всей сети через Kaspersky Security Center" на стр. [284](#)):

- С помощью групповой задачи Генерация 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 опции **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 опции **Сформировать правила для устройств, подключенных в текущий момент** в параметрах политики Контроль устройств и задачи Генерация правил контроля устройств. Используйте этот способ, если хотите, чтобы при формировании разрешающих правил учитывались данные только об устройствах, подключенных к защищаемому компьютеру в данный момент.

Kaspersky Embedded Systems Security 2.1 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.

## Формирование правил с помощью задачи Генерация правил контроля устройств

► Чтобы задать разрешающие правила запуска программ для группы компьютеров с помощью задачи Генерация правил контроля устройств, выполните следующие действия.

1. На закладке **Задачи** в панели управления настраиваемой группы компьютеров создайте групповую задачу Генерация правил контроля устройств или выберите уже созданную задачу.
2. В свойствах созданной групповой задачи генерации разрешающих правил 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** в панели управления настраиваемой группы компьютеров в списке групповых задач выберите созданную задачу генерации разрешающих правил 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 сети убедитесь, что для всех защищаемых компьютеров настроен доступ к общей сетевой папке. В случае, если применение общей сетевой папки в работе компьютеров сетине предусматривается политикой организации, рекомендуется запускать задачи автоматического формирования разрешающих правил контроля компьютера на тестовой группе компьютеров или на эталонной машине организации.

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 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 Генератор 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 для контроля устройств, в свойствах политики Контроль устройств выберите режим выполнения задачи **Запрещать недоверенные устройства**.

Разрешающие правила, автоматически сформированные на основе данных системы на каждом отдельном компьютере, будут применены для всех компьютеров в сети, для которых применяется настраиваемая политика. Для этих компьютеров программа будет разрешать 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 **Сформировать правила на основе данных системы** в параметрах политики Контроль устройств, выполните следующие действия:

1. Если требуется, подключите к компьютеру с установленным Kaspersky Security Center новое запоминающее устройство, использование которого вы хотите разрешить.
2. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**, разверните группу администрирования, параметры политики которой вы хотите настроить, затем выберите в панели результатов закладку **Политики**. В контекстном меню политики, параметры которой вы хотите настроить, выберите пункт **Свойства**.
3. В свойствах политики откройте окно настройки параметров задачи Контроль устройств и выполните следующие действия:
  - а. На закладке **Общие** нажмите на кнопку **Список правил**.  
  
Откроется окно **Правила контроля устройств**.
  - б. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Создать правила на основе данных системы**.

с. 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.

4. 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 **Сформировать правила для устройств, подключенных в текущий момент** в параметрах политики Контроль устройств, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**,
2. Разверните группу администрирования, параметры политики которой вы хотите настроить и выберите в панели результатов закладку **Политики**.
3. В контекстном меню политики, параметры которой вы хотите настроить, выберите пункт **Свойства**.

4. В разделе Контроль активности на компьютерах нажмите на кнопку Настройка в блоке Контроль устройств.

5. На закладке **Общие** нажмите на кнопку **Список правил**.

Откроется окно **Правила контроля устройств**.

6. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила для устройств, подключенных в текущий момент**.

Откроется окно **Сформировать правила на основе данных системы**.

7. В списке обнаруженных устройств, которые подключены к защищаемому компьютеру, выберите устройства, для которых вы хотите сформировать разрешающие правила.

8. Нажмите на кнопку **Добавить правила для выбранных устройств**.

9. 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 контроля 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 запоминающих устройств для группы компьютеров на основе отчета из Kaspersky Security Center о заблокированных попытках подключения устройств, выполните следующие действия:

1. В свойствах политики в параметрах задачи Контроль устройств установите режим работы **Только статистика**.
2. В свойствах политики в разделе **События** 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 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 зафиксированные события в файл формата TXT. Для этого разверните узел **Отчеты 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:

а. На закладке **Общие** нажмите на кнопку **Список правил**.

Откроется окно **Правила контроля устройств**.

б. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать данные о заблокированных устройствах из отчета Kaspersky Security Center**.

с. 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.

д. В открывшемся стандартном окне Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных устройствах.

е. 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 .....	<a href="#">295</a>
О правилах сетевого экрана .....	<a href="#">297</a>
Активация и деактивация правил сетевого экрана .....	<a href="#">299</a>
Добавление правил сетевого экрана вручную.....	<a href="#">300</a>
Удаление правил сетевого экрана .....	<a href="#">302</a>

## О задаче Управление сетевым экраном

Kaspersky Embedded Systems Security 2.1 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 2.1. В ходе выполнения задачи Управление сетевым экраном Kaspersky Embedded Systems Security 2.1 полностью перенимает управление параметрами и правилами сетевого экрана операционной системы и блокирует любую возможность настройки параметров сетевого экрана другими способами.

В ходе установки программы компонент Управление сетевым экраном считывает и копирует состояние сетевого экрана Windows, а также все заданные правила. Далее изменение набора правил или их параметров, а также остановка или запуск сетевого экрана возможны только через Kaspersky Embedded Systems Security 2.1.

Если при установке Kaspersky Embedded Systems Security 2.1 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, не 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 2.1 обнаруживает несовпадение параметров сетевого экрана Windows и параметров задачи Управление сетевым экраном, программа форсировано сообщает параметры задачи сетевому экрану операционной системы.

При ежеминутном опросе сетевого экрана Windows, Kaspersky Embedded Systems Security 2.1 контролирует следующее:

- статус работы сетевого экрана Windows;
- статус правил, добавленных после установки Kaspersky Embedded Systems Security 2.1 другими программами или инструментами (Например, добавление нового правила программы для порта/приложения с помощью wf.msc).

После сообщения правил сетевому экрану Windows Kaspersky Embedded Systems Security 2.1 создает группу правил Kaspersky Security Group в оснастке **Брандмауэр Windows**. Эта группа объединяет все правила, созданные на стороне Kaspersky Embedded Systems Security



2.1 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 2.1.

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 2.1 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 нового приложения), Kaspersky Embedded Systems Security 2.1 удаляет такое правило;
- если в параметрах сетевого экрана Windows удаляется существующее правило, Kaspersky Embedded Systems Security 2.1 восстанавливает такое правило;
- если в параметрах сетевого экрана Windows изменяются параметры существующего правила, Kaspersky Embedded Systems Security 2.1 отменяет изменения;

- если в параметрах задачи Управление сетевым экраном создается новое правило, Kaspersky Embedded Systems Security 2.1 форсировано сообщает это правило сетевому экрану Windows;
- если в параметрах задачи Управление сетевым экраном удаляется существующее правило, Kaspersky Embedded Systems Security 2.1 форсировано удаляет такое правило в параметрах сетевого экрана Windows;
- если в параметрах задачи Управление сетевым экраном изменяются параметры существующего правила, Kaspersky Embedded Systems Security 2.1 форсировано обновляет такое правило в параметрах сетевого экрана Windows.

Kaspersky Embedded Systems Security 2.1 не работает с запрещающими правилами, а также с правилами, контролирующими исходящий трафик. В момент запуска задачи Управление сетевым экраном Kaspersky Embedded Systems Security 2.1 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 2.1, 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;
- редактировать 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;
- редактировать 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 деактивация правил сетевого экрана

► Чтобы активировать или деактивировать существующее правило фильтрации входящего трафика, выполните следующие действия:

1. В дереве Консоли Kaspersky Security Center разверните узел **Управляемые устройства** и выполните следующие действия:
  - Если вы хотите настроить параметры политики, выберите закладку **Политики** и откройте свойства **<Имя политики>** → **Контроль активности в сети** → **Настройка** в блоке **Сетевой экран** → **Список правил**.

- Если вы хотите настроить параметры задачи для одного компьютера, выберите закладку **Устройства** и откройте свойства выбранного компьютера. В окне **Задачи** выберите **Управление сетевым экраном** → **Свойства** → **Настройка** → **Список правил**.

Откроется окно **Правила сетевого экрана**.

2. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.
3. 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 деактивировано.

4. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные параметры задачи Управление сетевым экраном будут сохранены; новые параметры правил будут сообщены сетевому экрану 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 Kaspersky Security Center разверните узел **Управляемые устройства** и выполните следующие действия:

- Если вы хотите настроить параметры политики, выберите закладку **Политики** и откройте свойства **<Имя политики>** → **Контроль активности в сети** → **Настройка** в блоке **Сетевой экран** → **Список правил**.
- Если вы хотите настроить параметры задачи для одного компьютера, выберите закладку **Устройства** и откройте свойства выбранного компьютера. В окне **Задачи** выберите **Управление сетевым экраном** → **Свойства** → **Настройка** → **Список правил**.

Откроется окно **Правила сетевого экрана**.

2. 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**.

3. 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 выполняться 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 выполняться настраиваемое правило.

Допускается указание IP-адресов только в формате IPv4.

4. В окне **Настроить правило для приложения** или **Настроить правило для порта** нажмите на кнопку **ОК**.
5. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные параметры задачи Управление сетевым экраном будут сохранены; новые параметры правил будут сообщены сетевому экрану 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 Kaspersky Security Center разверните узел **Управляемые устройства** и выполните следующие действия:

- Если вы хотите настроить параметры политики, выберите закладку **Политики** и откройте свойства **<Имя политики>** → **Контроль активности в сети** → **Настройка** в блоке **Сетевой экран** → **Список правил**.
- Если вы хотите настроить параметры задачи для одного компьютера, выберите закладку **Устройства** и откройте свойства выбранного компьютера. В окне **Задачи** выберите **Управление сетевым экраном** → **Свойства** → **Настройка** → **Список правил**.

Откроется окно **Правила сетевого экрана**.

2. В зависимости от типа правила, которое вы хотите удалить, выберите закладку **Приложения** или закладку **Порты**.
3. В списке правил выберите правило, которое вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

Выбранное правило будет удалено.

5. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные параметры задачи **Управление сетевым экраном** будут сохранены; обновленный список правил будет сообщен сетевому экрану 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 .....	<a href="#">304</a>
Анализ журналов .....	<a href="#">318</a>

# Мониторинг файловых операций

Этот раздел содержит информацию о задаче Мониторинг файловых операций и инструкции о том, как настроить параметры этой задачи.

## В этом разделе

О задаче Мониторинг файловых операций .....	<a href="#">304</a>
О правилах мониторинга файловых операций .....	<a href="#">306</a>
Настройка параметров задачи Мониторинг файловых операций .....	<a href="#">310</a>
Настройка правил мониторинга .....	<a href="#">314</a>

# 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 для выявления изменений файлов,



которые могут свидетельствовать о нарушении 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 2.1 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, поддерживающий файловые системы ReFS и NTFS.
- включен USN-журнал Windows, на основе опроса которого 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 задать исключения для области мониторинга. 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 нижеуровневой 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 2.1 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 2.1 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 2.1 не может определить пользователя-инициатора для операций, выполненных 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 2.1 не может получить данные о пользователе вследствие прерывания задачи или сбоя синхронизации данных драйвера и USN-журнала. Если Kaspersky Embedded Systems Security 2.1 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 2.1 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 зафиксировывает 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 2.1 учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см.таблицу ниже).

Таблица 34. Маркеры файловых операций

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
BASIC_INFO_CHANGE	изменены атрибуты или метки времени файла или папки	NTFS, ReFS
COMPRESSION_CHANGE	изменено сжатие файла или папки	NTFS, ReFS
DATA_EXTEND	размер файла или папки увеличен	NTFS, ReFS
DATA_OVERWRITE	перезаписаны данные в файле или папке	NTFS, ReFS
DATA_TRUNCATION	файл или папка усечены	NTFS, ReFS
EA_CHANGE	изменены расширенные атрибуты файла или папки	только NTFS
ENCRYPTION_CHANGE	изменен статус шифрования файла или папки	NTFS, ReFS
FILE_CREATE	файл или папка созданы впервые	NTFS, ReFS
FILE_DELETE	файл или папка удалены	NTFS, ReFS

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
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

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
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

По умолчанию задача Мониторинг файловых операций имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 35. Параметры задачи Мониторинг файловых операций по умолчанию

Параметр	Значение	Как настроить
Области мониторинга	Не задано	Вы можете задать каталоги и файлы, действия над которыми будут отслеживаться. Для каталогов и файлов заданной области будут формироваться события мониторинга.

Параметр	Значение	Как настроить
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 отключать учет файловых операций, которые были выполнены в указанных областях мониторинга в период обрыва мониторинга.
Учитывать исключенные области мониторинга	Не применяется	Вы можете контролировать применение исключений для каталогов, где не требуется выполнять контроль за файловыми операциями. При выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security 2.1 будет пропускать области мониторинга, заданные в качестве исключений.

Параметр	Значение	Как настроить
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 2.1 формирует событие аудита.
Расписание запуска задачи	Следующий запуск не определен	Вы можете настраивать 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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел



"Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

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 открывшемся окне на закладке **Общие** настройте параметры области мониторинга:

- a. Снимите или установите флажок **Восполнять события о файловых операциях, выполненных в 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 2.1 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. [314](#)), которые будут контролироваться задачей.

5. На закладке **Управление задачами** настройте запуск задачи по расписанию.

6. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

# 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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

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>`. При отсутствии указания тома Kaspersky Embedded Systems Security 2.1 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 2.1 считает недоверенными всех пользователей, не указанных в списке доверенных, и формирует для них события с уровнем важности (см. раздел "О правилах мониторинга файловых операций" на стр. [306](#)) *Критическое событие*.

8. Выберите закладку **Маркеры файловых операций**.
9. Если требуется, выберите несколько маркеров файловых операций, выполнив следующие действия:
- Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
  - В открывшемся списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. [306](#)) установите флажки напротив тех операций, которые вы хотите контролировать.

По умолчанию Kaspersky Embedded Systems Security 2.1 контролирует все доступные файловые операции, выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

10. Если вы хотите, чтобы Kaspersky Embedded Systems Security 2.1 рассчитывал контрольную сумму файлов после изменений, выполните следующие действия:
- В блоке **Контрольная сумма** установите флажок **Рассчитывать контрольную сумму измененного файла, если это возможно**.

Если флажок установлен, Kaspersky Embedded Systems Security 2.1 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 2.1 не рассчитывает контрольную сумму измененных файлов.

Kaspersky Embedded Systems Security 2.1 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. [306](#)) 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 контроля**.

Флажок включает или выключает применение исключений для папок, в которых не требуется выполнять контроль над файловыми операциями.

Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security 2.1 будет пропускать области мониторинга, заданные в списке исключений.

Если флажок снят, Kaspersky Embedded Systems Security 2.1 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 кнопку **ОК**.

Указанная папка добавится в список исключенных областей.

13. В окне **Область контроля** 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 настройке параметров задачи.

### В этом разделе

О задаче Анализ журналов.....	<a href="#">318</a>
Настройка эвристического анализатора .....	<a href="#">320</a>
Настройка правил анализа журналов .....	<a href="#">323</a>

## О задаче Анализ журналов

В ходе выполнения задачи Анализ журналов Kaspersky Embedded Systems Security 2.1 выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows. Программа информирует администратора при обнаружении признаков нетипичного поведения в системе, которые могут свидетельствовать о попытках компьютерных атак.

Kaspersky Embedded Systems Security 2.1 считывает данные журналов событий Windows и определяет нарушения в соответствии с правилами заданными пользователем или

параметрами эвристического анализатора, который применяется задачей для анализа журналов.

### **Эвристический анализатор**

Вы можете использовать задачу Анализ журналов для контроля состояния защищаемой системы на основе предзаданных эвристик. Эвристический анализатор определяет наличие аномальной активности на защищаемом компьютере, которая может являться признаком попытки атаки. Шаблоны определения аномальной активности заложены в доступных эвристиках в параметрах эвристического анализатора.

В списке эвристик для задачи Анализ журналов доступно семь эвристик. Вы можете включать и выключать применение любой эвристики. Вы не можете удалять существующие или создавать новые эвристики.

Для каждой эвристики вы можете настраивать следующие критерии срабатывания анализатора:

- 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 2.1 не применяет эвристики для анализа журналов Windows, если эвристический анализатор не используется задачей. По умолчанию эвристический анализатор включен.

При срабатывании эвристического анализатора 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 поджурналжурнала событий Windows. Программа будет выполнять поиск записей с указанными идентификаторами событий только в этом поджурнале. Вы можете выбрать один из стандартных поджурналов (Приложение, Безопасность или Система), а также указать пользовательский поджурнал.

Программа не выполняет проверок на фактическое наличие заданного поджурнала в журнале событий Windows.

При срабатывании правила Kaspersky Embedded Systems Security 2.1 фиксирует событие с уровнем важности *Критическое* в журнале выполнения задачи Анализ журналов.

По умолчанию задача Анализ журналов не учитывает пользовательские правила.

## Настройка эвристического анализатора

► Чтобы настроить параметры работы эвристического анализатора для задачи Анализ журналов, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите 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 программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
- Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "**Настройка локальных задач в окне Параметры программы в Kaspersky Security Center**" на стр. [159](#)).

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 **Анализ журналов** нажмите на кнопку **Настройка**.

Откроется окно **Параметры анализа журналов**.

4. Выберите закладку **Эвристический анализатор**.
5. Снимите или установите флажок **Использовать эвристический анализатор для анализа журналов**.

Если этот флажок установлен, Kaspersky Embedded Systems Security 2.1 применяет эвристический анализатор для обнаружения аномальной активности на защищаемом компьютере.

Если этот флажок не установлен, эвристический анализатор выключен, Kaspersky Embedded Systems Security 2.1 использует предустановленные или пользовательские правила для обнаружения аномальной активности.

Для работы задачи должен быть выбран хотя бы один режим анализа журналов.

По умолчанию флажок установлен.

6. Выберите эвристики, которые вы хотите применять для анализа журналов из списка доступных эвристик:

- Обнаружена возможная попытка взлома пароля.
- 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 Administrators.

7. Чтобы настроить параметры выбранных эвристик, нажмите на кнопку **Указать критерии срабатывания**.

Откроется окно **Параметры анализа журналов**.

8. В блоке **Обработка подбора 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 2.1 расценивает данное действие как аномальную активность.

10. Выберите закладку **Исключения**.

11. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:

- а. Нажмите на кнопку **Обзор**.
- б. Выберите пользователя.
- с. 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 закладках **Расписание и Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. [187](#)).

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 компьютеров которой вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
  - Если вы хотите настроить параметры программы для группы компьютеров, выберите закладку **Политики**. В списке существующих политик выберите политику, с помощью которой вы хотите настроить параметры программы, и в контекстном меню выбранной политики выберите пункт **Свойства**. Откроется окно **Свойства: <Имя политики>**.
  - Если вы хотите настроить параметры программы для одного компьютера, выберите закладку **Устройства** и откройте окно **Параметры программы** (см. раздел "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center" на стр. [159](#)).

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 **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 2.1 применяет пользовательские правила для анализа журналов в соответствии с настроенными параметрами каждого правила. Вы можете добавлять и редактировать правила анализа журналов.

Если флажок снят, вы не можете добавлять или редактировать пользовательские правила. Kaspersky Embedded Systems Security 2.1 применяет параметры правил по умолчанию.

Вы не можете удалять или редактировать предустановленные правила.

По умолчанию флажок снят.

Вы можете контролировать применение предустановленных 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:

- **Имя**
- **Источник**

Выберите журнал, события которого будут использоваться для анализа. Для выбора доступны следующие виды журналов Windows:

- Application
- Security
- System

7. В блоке **Параметры срабатывания** укажите идентификаторы записей, при обнаружении которых будет срабатывать правило:

- Введите числовое значение идентификатора.
- Нажмите на кнопку **Добавить**.

Указанный идентификатор правила добавится в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.

- Нажмите на кнопку **ОК**.

Правило анализа журналов добавится в общий список правил.

---

# Работа с Kaspersky Embedded Systems Security 2.1 из командной строки

Этот раздел содержит описание работы с Kaspersky Embedded Systems Security 2.1 из командной строки.

## В этом разделе

Команды командной строки .....	<a href="#">326</a>
Коды возврата командной строки.....	<a href="#">368</a>

## Команды командной строки

Вы можете выполнять основные команды управления Kaspersky Embedded Systems Security 2.1 из командной строки защищаемого компьютера, если при установке Kaspersky Embedded Systems Security 2.1 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 2.1.

Некоторые из команд Kaspersky Embedded Systems Security 2.1 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 2.1 применяйте следующие правила:

- вводите ключи и команды символами верхнего или нижнего регистра;
- разделяйте ключи символом пробела;
- если имя файла, которое вы указываете в качестве значения ключа, содержит символ пробела, заключите это имя файла (и путь к нему) 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 2.1 (см. таблицу ниже).

Таблица 36. Команды Kaspersky Embedded Systems Security 2.1

Команда	Описание
KAVSHELL APPCONTROL (см. раздел "Наполнение списка правил контроля запуска программ из файла. KAVSHELL APPCONTROL" на стр. <a href="#">348</a> )	Дополняет список сформированных правил контроля запуска программ в соответствии с выбранным принципом добавления.
KAVSHELL APPCONTROL /CONFIG (см. раздел "Управление задачами Контроль запуска программ. KAVSHELL APPCONTROL /CONFIG" на стр. <a href="#">342</a> )	Управляет режимами работы задачи Контроль запуска программ.

Команда	Описание
KAVSHELL APPCONTROL /GENERATE (см. раздел "Генерация правил контроля запуска программ. KAVSHELL APPCONTROL /GENERATE" на стр. <a href="#">344</a> )	Запускает задачу автоматического формирования разрешающих правил контроля запуска программ.
KAVSHELL VACUUM (см. раздел "Дефрагментация файлов журнала Kaspersky Embedded Systems Security 2.1. KAVSHELL VACUUM" на стр. <a href="#">362</a> )	Дефрагментирует файлы журнала выполнения Kaspersky Embedded Systems Security 2.1.
KAVSHELL PASSWORD	Управляет параметрами защиты паролем.
KAVSHELL HELP (см. стр. <a href="#">330</a> )	Вызывает справку о командах Kaspersky Embedded Systems Security 2.1.
KAVSHELL START (см. стр. <a href="#">331</a> )	Запускает службу Kaspersky Embedded Systems Security 2.1.
KAVSHELL STOP (см. стр. <a href="#">331</a> )	Останавливает службу Kaspersky Embedded Systems Security 2.1.
KAVSHELL SCAN (см. стр. <a href="#">331</a> )	Создает и запускает временную задачу проверки по требованию с областью проверки и параметрами безопасности, заданными ключами команды.
KAVSHELL SCANCritical (см. стр. <a href="#">338</a> )	Запускает системную задачу Проверка важных областей.
KAVSHELL TASK (см. стр. <a href="#">340</a> )	Запускает / приостанавливает / возобновляет / останавливает указанную задачу в асинхронном режиме / возвращает текущее состояние задачи / статистику задачи.



Команда	Описание
KAVSHELL RTP (см. стр. <a href="#">341</a> )	Запускает или останавливает все задачи постоянной защиты.
KAVSHELL UPDATE (см. стр. <a href="#">352</a> )	Запускает задачу обновления баз Kaspersky Embedded Systems Security 2.1 с параметрами, указанными с помощью ключей команды.
KAVSHELL ROLLBACK (см. стр. <a href="#">357</a> )	Откатывает базы до предыдущей версии.
KAVSHELL LICENSE (см. стр. <a href="#">358</a> )	Управляет ключами и кодами активации.
KAVSHELL TRACE (см. стр. <a href="#">359</a> )	Включает или выключает запись журнала трассировки, управляет параметрами журнала трассировки.
KAVSHELL DUMP (см. стр. <a href="#">364</a> )	Включает или выключает создание файлов дампов памяти процессов Kaspersky Embedded Systems Security 2.1 при аварийном завершении процессов.
KAVSHELL IMPORT (см. стр. <a href="#">365</a> )	Импортирует общие параметры Kaspersky Embedded Systems Security 2.1, параметры его функций и задач из предварительно созданного конфигурационного файла.
KAVSHELL EXPORT (см. стр. <a href="#">366</a> )	Экспортирует все параметры Kaspersky Embedded Systems Security 2.1 и существующих задач в конфигурационный файл.
KAVSHELL DEVCONTROL (см. раздел "Наполнение списка правил контроля устройств из файла. KAVSHELL DEVCONTROL" на стр. <a href="#">350</a> )	Дополняет список сформированных правил контроля устройств в соответствии с выбранным принципом добавления.

# Вызов справки о командах Kaspersky Embedded Systems Security 2.1. KAVSHELL HELP

Чтобы получить список всех команд Kaspersky Embedded Systems Security 2.1, 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 следующую команду:

```
KAVSHELL HELP SCAN
```

# Запуск и остановка службы Kaspersky Security Service. KAVSHELL START, KAVSHELL STOP

Чтобы запустить службу Kaspersky Security Service, выполните команду

```
KAVSHELL START.
```

По умолчанию при запуске службы Kaspersky Security Service 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 Service, 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 Kaspersky Embedded Systems Security 2.1 только во время ее выполнения (в Консоли Kaspersky Embedded Systems Security 2.1 вы не можете просматривать параметры задачи). Одновременно регистрируется журнал выполнения задачи, который отображается в узле **Журналы выполнения задач** Консоли Kaspersky Embedded Systems Security 2.1. К задачам, созданным и запущенным с помощью команды SCAN, могут применяться политики программы Kaspersky Security Center.

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. стр. [340](#)).

## 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] [/NOCHECKMSSIGN] [/W:<имя файла
журнала выполнения задачи>] [/ANSI] [/ALIAS:<альтернативное имя 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 37. Ключи команды KAVSHELL SCAN

Ключ	Описание
<b>Область проверки.</b> Обязательный ключ.	
<файлы>	<p>Область проверки – список файлов, папок, сетевых путей и предопределенных областей.</p> <p>Указывайте сетевые пути в формате UNC (Universal Naming Convention).</p> <p>В следующем примере папка Folder4 указана без пути к ней – она находится в папке, из которой вы запускаете команду KAVSHELL:</p> <p>KAVSHELL SCAN Folder4</p> <p>Если имя объекта, который вы хотите проверить, содержит пробелы, требуется заключить его в кавычки.</p> <p>Если вы выбрали папку, то Kaspersky Embedded Systems Security 2.1 проверит также все вложенные подпапки для данной папки.</p> <p>Для проверки группы файлов вы можете использовать символы * или ?.</p>
<папки>	
<сетевой путь>	
/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>	<p>Имя файла со списком областей проверки, включая полный путь к файлу.</p> <p>Разделяйте области проверки в файле символом перевода строки. Вы можете указывать predetermined области проверки, как показано в следующем в примере файла со списком областей проверки:</p> <p>C:\</p> <p>D:\Docs\*.doc</p> <p>E:\My Documents</p> <p>/STARTUP</p> <p>/SHARED</p>
<p><b>Проверяемые объекты</b> (File types). Если вы не укажете никаких значений этого ключа, Kaspersky Embedded Systems Security 2.1 будет проверять объекты по формату.</p>	
/FA	Проверять все объекты
/FC	Проверять объекты по формату (по умолчанию). Kaspersky Embedded Systems Security 2.1 проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам.
/FE	Проверять объекты по расширению. Kaspersky Embedded Systems Security 2.1 проверяет только объекты с расширениями, которые входят в список расширений, свойственных заражаемым объектам.
/NEWONLY	<p>Проверять только новые и измененные файлы.</p> <p>Если вы не укажете этот ключ, Kaspersky Embedded Systems Security 2.1 будет проверять все объекты.</p>

Ключ	Описание
/AI: <b>Действия над зараженными и другими обнаруженными объектами.</b> Если вы не зададите никаких значений этого ключа, Kaspersky Embedded Systems Security 2.1 будет выполнять действие <b>Пропускать</b> .	
DISINFECT	Лечить, если невозможно, пропускать
DISINFDEL	Лечить, удалять, если лечение невозможно
DELETE	Удалять  Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Embedded Systems Security 2.1 для обеспечения совместимости с предыдущими версиями. Вы можете использовать эти параметры вместо ключей команд /AI: и /AS:. В этом случае Kaspersky Embedded Systems Security 2.1 не будет обрабатывать возможно зараженные объекты.
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие
/AS: <b>Действия над возможно зараженными объектами (actions).</b> Если вы не зададите никаких значений этого ключа, Kaspersky Embedded Systems Security 2.1 будет выполнять действие <b>Пропускать</b> .	
QUARANTINE	Помещать на карантин
DELETE	Удалять
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие

Ключ	Описание
<b>Исключения (Exclusions)</b>	
/E:ABMSPO	Ключ исключает составные объекты следующих типов:  A – SFX-архивы;  B – почтовые базы;  M – файлы почтовых форматов;  S – архивы (включая SFX-архивы);  P – упакованные объекты;  O – вложенные OLE-объекты.
/EM:<"маски">	Исключать файлы по маске  Вы можете задать несколько масок, например, EM:"*.txt;*.png; C:\Videos\*.avi".
/ET:<количество секунд>	Прекращать обработку объекта, если она продолжается дольше указанного количества секунд.  По умолчанию ограничений в продолжительности проверки нет.
/ES:<размер>	Исключать из проверки составные объекты, размер которых в мегабайтах превышает указанный значением <размер>.  По умолчанию Kaspersky Embedded Systems Security 2.1 проверяет объекты любого размера.
/TZOFF	Отменить исключения доверенной зоны.
<b>Дополнительные параметры (Options)</b>	
/NOICHECKER	Выключить использование технологии iChecker (по умолчанию включено).
/NOISWIFT	Выключить использование технологии iSwift (по умолчанию включено).



Ключ	Описание
/ANALYZERLEVEL:<ур овень анализа>	<p>Включить использование эвристического анализатора, настроить уровень анализа.</p> <p>Сюда входят следующие уровни эвристического анализа:</p> <p>1 – поверхностный;</p> <p>2 – средний;</p> <p>3 – глубокий.</p> <p>Если вы опустите этот ключ, Kaspersky Embedded Systems Security 2.1 не будет использовать эвристический анализатор.</p>
/ALIAS:<альтернативн ое имя задачи>	<p>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 имя задачи должно быть уникальным среди альтернативных имен задач всех функциональных компонентов Kaspersky Embedded Systems Security 2.1.</p> <p>Если этот ключ не задан, задаче присваивается альтернативное имя scan_&lt;kavshell_pid&gt;, например, scan_1234. В Консоли Kaspersky Embedded Systems Security 2.1 задаче присваивается имя Scan objects (&lt;дата и время&gt;), например, Scan objects 8/16/2007 5:13:14 PM.</p>
<b>Параметры журналов выполнения задач (Report settings)</b>	
/W:<имя файла журнала выполнения задачи>	<p>Если вы укажете этот ключ, Kaspersky Embedded Systems Security 2.1 сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа.</p> <p>Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней.</p>

	<p>В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий Kaspersky Embedded Systems Security 2.1 в консоли "Просмотр событий".</p> <p>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.</p> <p>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.</p> <p>Вы можете просматривать файл журнала во время выполнения задачи.</p> <p>Журнал отображается в узле <b>Журналы выполнения задач</b> Консоли Kaspersky Embedded Systems Security 2.1.</p> <p>Если Kaspersky Embedded Systems Security 2.1 не удастся создать файл журнала, он не прерывает выполнение команды, но выдает сообщение об ошибке.</p>
/ANSI	<p>Ключ позволяет записывать события в журнал выполнения задач в кодировке ANSI.</p> <p>Ключ ANSI не будет применяться, если не задан ключ W.</p> <p>Если ключ ANSI не указан, то журнал выполнения задач ведется в кодировке UNICODE.</p>

## 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 Kaspersky Embedded Systems Security 2.1.

### 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 38. Синтаксис ключа /W команды KAVSHELL SCANCritical

Ключ	Описание
/W:<имя файла журнала выполнения задачи>	<p>Если вы укажете этот ключ, Kaspersky Embedded Systems Security 2.1 сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа.</p> <p>Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней.</p> <p>В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий программы в консоли "Просмотр событий".</p> <p>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.</p> <p>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.</p> <p>Вы можете просматривать файл журнала во время выполнения задачи.</p> <p>Журнал отображается в узле <b>Журналы выполнения задач</b> Консоли Kaspersky Embedded Systems Security 2.1.</p> <p>Если Kaspersky Embedded Systems Security 2.1 не удастся создать файл журнала, он не прерывает выполнение команды, но выдает сообщение об ошибке.</p>

# 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 имя 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 39. Ключи команды KAVSHELL TASK

Ключ	Описание
Без ключей	Команда возвращает список всех существующих задач Kaspersky Embedded Systems Security 2.1. Список содержит поля: альтернативное имя задачи, категория задачи (системная или пользовательская) и текущее состояние задачи.
<альтернативное имя задачи>	Вместо имени задачи в команде <code>SCAN TASK</code> используйте ее альтернативное имя (Task alias) – дополнительное, краткое имя,

	которое Kaspersky Embedded Systems Security 2.1 присваивает задачам. Чтобы просмотреть альтернативные имена задач Kaspersky Embedded Systems Security 2.1, 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, <b>Выполняется, Завершена, Приостановлена, Остановлена, Завершена с ошибкой, Запускается, Восстанавливается</b> )
/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи по текущий момент.

Коды возврата команды KAVSHELL TASK (на стр. [370](#))

## 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 40. Ключи команды KAVSHELL RTP

Ключ	Описание
/START	Запустить все задачи постоянной защиты: Постоянная защита файлов, 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 Применять правила контроля запуска программ 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 41. Ключи команды KAVSHELL APPCONTROL /CONFIG

Ключ	Описание
/mode:<applyrules statistics>	Режим работы задачи Контроль запуска программ.  Вы можете выбрать один из следующих режимов работы задачи: <ul style="list-style-type: none"><li>• applyrules - Применять правила контроля запуска программ;</li><li>• statistics - Только статистика.</li></ul>
/dll:<no yes>	Выключить или включить контроль загрузки DLL-модулей.
/savetofile:<полный путь к XML файлу>	Экспортировать заданные правила в указанный файл в формате XML.

# Генерация 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 42. Ключи команды KAVSHELL APPCONTROL /GENERATE

Ключ	Описание
<b>Область применения разрешающих правил</b>	
<путь к папке>	Путь к папке, содержащей исполняемые файлы, для которых требуется автоматически создать разрешающие правила.
/source: <путь к файлу со списком папок>	Путь к файлу в формате TXT, содержащий список папок с исполняемыми файлами, для которых требуется автоматически создать разрешающие правила.
/masks: <edms>	<p>Расширения исполняемых файлов, для которых требуется создать разрешающие правила контроля запуска программ.</p> <p>Вы можете включить в область срабатывания создаваемых правил файлы следующих расширений:</p> <ul style="list-style-type: none"> <li>• e - файлы с расширением exe;</li> <li>• d - файлы с расширением dll;</li> <li>• m - файлы с расширением msi;</li> <li>• s - скрипты.</li> </ul>
/runapp	Учитывать при формировании разрешающих правил программы, запущенные на защищаемом компьютере в момент выполнения задачи.

Ключ	Описание
<b>Действия при автоматическом формировании правил</b>	
/rules: <ch cp h>	<p>Указать действия, которые задача совершает во время формирования разрешающих правил контроля запуска программ:</p> <ul style="list-style-type: none"> <li>• ch - использовать цифровой сертификат. Если сертификат отсутствует, использовать хеш SHA256.</li> <li>• cp - использовать цифровой сертификат. Если сертификат отсутствует, использовать значение пути к исполняемому файлу.</li> <li>• h - использовать хеш SHA256.</li> </ul>
/strong	Использовать заголовок и отпечаток цифрового сертификата при автоматическом формировании правил контроля запуска программ. Команда выполняется, если задано значение ключа /rules: <ch cp h>.
/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 указанной группой.
<b>Действия по завершении автоматического формирования правил</b>	
/export: <полный 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>	<p>Импортировать сформированные правила в список заданных правил контроля запуска программ в соответствии с указанным принципом добавления новых правил:</p> <ul style="list-style-type: none"> <li>• <b>а - Добавлять к существующим правилам</b> (одинаковые правила дублируются);</li> <li>• <b>г - Заменять существующие правила</b> (новые правила добавляются вместо заданных правил);</li> <li>• <b>т - Объединять с существующими правилами</b> (добавляются новые правила, параметры которых не совпадают с параметрами уже заданных правил).</li> </ul>
------------------	---

## Поддержка программного обеспечения NCR. KAVSHELL APPCONTROL /PROFILE:NCR

Команда `KAVSHELL APPCONTROL /PROFILE:NCR` позволяет осуществлять поддержку автоматизированного формирования списков исключений на встроенных системах с установленным программным обеспечением NCR. Сформированные списки используются задачами Контроль запуска программ, Постоянная защита файлов и задач проверки по требованию.

### Синтаксис команды `KAVSHELL APPCONTROL /PROFILE:NCR`

`KAVSHELL APPCONTROL /PROFILE:NCR /path:<путь к папке с созданными файлами>`

### Примеры команды `KAVSHELL APPCONTROL /PROFILE:NCR`

► *Чтобы создать списки исключений, выполните команду:*

```
KAVSHELL APPCONTROL /PROFILE:NCR /PATH:C:\Temp
```

Kaspersky Embedded Systems Security 2.1 создаст два xml-файла:

- `ncr_whitelist.xml`: список разрешающих правил для программного обеспечения NCR. Список может быть добавлен к списку правил задачи Контроль запуска программ.
- `ncr_trustedprocesses.xml`: список доверенных процессов для Доверенной зоны.

Если такие файлы уже существуют, программа заменит их на новые файлы, содержащие актуальные списки.

Если программное обеспечение NCR не обнаружено, программа возвращает код -504.

## Наполнение списка правил контроля запуска программ из файла. 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 43. 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 - <b>Добавить к существующим правилам</b> (одинаковые правила дублируются).
/replace <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного файла в формате XML. Принцип добавления - <b>Заменить существующие правила</b> (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 - <b>Объединить правила с существующими</b> (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 44. 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 - <b>Добавить к существующим правилам</b> (одинаковые правила дублируются).
/replace <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного файла в формате XML. Принцип добавления - <b>Заменить существующие правила</b> (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 - <b>Объединить правила с существующими</b> (новые правила не дублируют уже заданные правила).
/clear	Очистить список правил контроля устройств.

# Запуск задачи обновления баз Kaspersky Embedded Systems Security 2.1. KAVSHELL UPDATE

С помощью команды `KAVSHELL UPDATE` вы можете запускать задачу обновления баз Kaspersky Embedded Systems Security 2.1 в синхронном режиме.

Задача обновления баз Kaspersky Embedded Systems Security 2.1, запущенная с помощью команды `KAVSHELL UPDATE`, является временной. Она отображается в Консоли Kaspersky Embedded Systems Security 2.1 только во время ее выполнения. Одновременно регистрируется журнал выполнения задачи; он отображается в узле **Журналы выполнения задач** Консоли Kaspersky Embedded Systems Security 2.1. К задачам обновления, созданным и запущенным с помощью команды `KAVSHELL UPDATE`, как и к задачам обновления, созданным в Консоли Kaspersky Embedded Systems Security 2.1, могут применяться политики программы Kaspersky Security Center. Об управлении Kaspersky Embedded Systems Security 2.1 на компьютерах с помощью программы Kaspersky Security Center читайте в разделе "Управление Kaspersky Embedded Systems Security 2.1 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 имя 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 \product\bases, выполните следующую команду:

```
KAVSHELL UPDATE \\server\bases
```

Чтобы запустить задачу обновления с FTP-сервера <ftp://dnl-ru1.kaspersky-labs.com/>, записать все события задачи в файл журнала c:\update\_report.log, выполните команду:

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

Чтобы получить обновления баз Kaspersky Embedded Systems Security 2.1 с сервера обновлений «Лаборатории Касперского»; соединиться с источником обновлений через прокси-сервер (адрес прокси-сервера: proxy.company.com, порт: 8080); для доступа к компьютеру использовать встроенную проверку подлинности Microsoft Windows (NTLM-authentication) под учетной записью (имя пользователя: inetuser, пароль: 123456), выполните команду:

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

Таблица 45. Ключи команды KAVSHELL UPDATE

Ключ	Описание
<b>Источники обновления</b> (обязательный ключ). Укажите один или несколько источников. Kaspersky Embedded Systems Security 2.1 будет обращаться к источникам в порядке их перечисления. Разделяйте источники символом пробела.	
<путь в формате UNC>	Пользовательский источник обновлений – путь к сетевой папке с обновлениями в формате UNC (Universal Naming Convention).
<URL>	Пользовательский источник обновлений – адрес HTTP- или FTP-сервера, на котором помещается папка с обновлениями.
<Локальная папка>	Пользовательский источник обновлений – папка на защищаемом компьютере.
/AK	Сервер администрирования Kaspersky Security Center в качестве источника обновлений.

Ключ	Описание
/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).
<b>Параметры прокси-сервера</b>	
/PROXY:<адрес>:<порт>	Сетевое имя или IP-адрес прокси-сервера и его порт. Если вы не укажете этот ключ, Kaspersky Embedded Systems Security 2.1 будет автоматически распознавать параметры прокси-сервера, который используется в локальной сети.
/AUTHTYPE:<0-2>	<p>Этот ключ задает метод проверки подлинности для доступа к прокси-серверу. Он может принимать следующие значения:</p> <p><b>0</b> – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Kaspersky Embedded Systems Security 2.1 будет обращаться к прокси-серверу под учетной записью <b>Локальная система (SYSTEM)</b>;</p> <p><b>1</b> – встроенная проверка подлинности Microsoft Windows (NTLM-authentication); Kaspersky Embedded Systems Security 2.1 будет обращаться к прокси-серверу под учетной записью, данные которой описаны ключами /PROXYUSER и /PROXYPWD;</p> <p><b>2</b> – проверка подлинности по имени и паролю пользователя, заданным ключами /PROXYUSER и /PROXYPWD (Basic authentication).</p> <p>Если для доступа к прокси-серверу не требуется проверка подлинности, указывать этот ключ нет необходимости.</p>

Ключ	Описание
/PROXYUSER:<им я 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:<пар оль>	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)
/USEPROXYFORC USTOM	Использовать параметры прокси-сервера для соединения с пользовательскими источниками обновлений (по умолчанию не используются)
/USEPROXYFORL OCAL	Использовать параметры прокси-сервера для соединения с локальными источниками обновлений. Если не указано, применяется значение <b>Не использовать настройки прокси-сервера для соединения с локальными источниками обновления.</b>
<b>Общие параметры FTP- и HTTP-сервера</b>	
/NOFTPPASSIVE	Если вы укажете этот ключ, Kaspersky Embedded Systems Security 2.1 будет использовать активный режим FTP-сервера для соединения с защищаемым компьютером. Если вы не укажете этот ключ, Kaspersky Embedded Systems Security 2.1 будет использовать пассивный режим FTP-сервера, если возможно.

Ключ	Описание
/TIMEOUT:<количество секунд>	Время ожидания при соединении с FTP- или HTTP-сервером. Если вы не укажете этот ключ, Kaspersky Embedded Systems Security 2.1 будет использовать значение по умолчанию: 10 с. В качестве значения ключа вы можете вводить только целые числа.
/REG:<код iso3166>	<p>Ключ "Региональные настройки" используется при получении обновлений с серверов обновлений "Лаборатории Касперского". Kaspersky Embedded Systems Security 2.1 оптимизирует загрузку обновлений на защищаемый компьютер, выбирая ближайший к нему сервер обновлений.</p> <p>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 вы опустите этот ключ или укажете несуществующий код страны, Kaspersky Embedded Systems Security 2.1 будет распознавать местоположение защищаемого компьютера в соответствии с региональными настройками защищаемого компьютера.</p>
/ALIAS:<альтернативное имя задачи>	<p>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 имя задачи должно быть уникальным среди альтернативных имен задач всех функциональных компонентов Kaspersky Embedded Systems Security 2.1.</p> <p>Если этот ключ не задан, задаче присваивается альтернативное имя update_&lt;kavshell_pid&gt;, например, update_1234. В Консоли Kaspersky Embedded Systems Security 2.1 задаче присваивается имя Update-bases (&lt;date time&gt;), например, Update-bases 8/16/2007 5:41:02 PM.</p>
/W:<имя файла журнала выполнения задачи>	Если вы укажете этот ключ, Kaspersky Embedded Systems Security 2.1 сохранит файл журнала выполнения задачи; присвоит файлу имя, заданное значением ключа.

	<p>Файл журнала выполнения задачи содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях в ней.</p> <p>В журнале регистрируются события, заданные параметрами журналов выполнения задач и журнала событий Kaspersky Embedded Systems Security 2.1 в консоли "Просмотр событий".</p> <p>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.</p> <p>Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.</p> <p>Вы можете просматривать файл журнала во время выполнения задачи.</p> <p>Журнал отображается в узле <b>Журналы выполнения задач</b> Консоли Kaspersky Embedded Systems Security 2.1.</p> <p>Если Kaspersky Embedded Systems Security 2.1 не удастся создать файл журнала, он не прерывает выполнение команды и не отображает сообщение об ошибке.</p>
--	---

Коды возврата команды KAVSHELL UPDATE (на стр. [372](#)).

## Откат обновления баз Kaspersky Embedded Systems Security 2.1. KAVSHELL ROLLBACK

С помощью команды KAVSHELL ROLLBACK вы можете выполнить системную задачу Откат обновления баз – откатить базы Kaspersky Embedded Systems Security 2.1 до предыдущих установленных обновлений. Команда выполняется синхронно.

### Синтаксис команды

KAVSHELL ROLLBACK

Коды возврата команды KAVSHELL ROLLBACK (на стр. [373](#))

# Активация программы. KAVSHELL LICENSE

С помощью команды KAVSHELL LICENSE вы можете управлять ключами и кодами активации в Kaspersky Embedded Systems Security 2.1.

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:<номер ключа | номер кода активации>]

## Примеры команды KAVSHELL LICENSE

Чтобы активировать программу, выполните команду:

```
KAVSHELL.EXE LICENSE / ADD: <код активации или номер 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 46. Ключи команды KAVSHELL LICENSE

Ключ	Описание
Без ключей	<p>Команда возвращает следующую информацию о добавленных ключах:</p> <ul style="list-style-type: none"> <li>• Номер ключа.</li> <li>• Тип лицензии (коммерческая или пробная).</li> <li>• Срок действия связанной с ключом лицензии.</li> <li>• Статус ключа (активный или дополнительный). Если указано значение *, ключ добавлен в качестве дополнительного.</li> </ul>
/ADD:<имя файла ключа или код активации>	<p>Добавляет ключ с помощью указанного файла или кода активации.</p> <p>Указывая путь к файлу ключа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.</p>
/R	<p>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.</p>
/DEL:<номер ключа или код активации>	<p>Удаляет ключ с указанным номером или указанный код активации.</p>

Коды возврата команды KAVSHELL LICENSE (на стр. [374](#))

## 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 2.1, а также устанавливать уровень детализации информации в журнале.

Kaspersky Embedded Systems Security 2.1 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 47. Ключи команды KAVSHELL TRACE

Ключ	Описание
/ON	Включить ведение журнала трассировки.
/F:<папка с файлами журнала трассировки>	<p>Этот ключ указывает полный путь к папке, в которой будут сохранены файлы журнала трассировки (обязательный ключ).</p> <p>Если вы укажете путь к несуществующей папке, журнал трассировки не будет создан. Вы можете указывать сетевые пути в формате UNC (Universal Naming Convention), но не можете указывать пути к папкам на сетевых дисках защищаемого компьютера.</p> <p>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".</p> <p>Указывая путь к папке с файлами журнала трассировки, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.</p>



Ключ	Описание
/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 2.1 начнет записывать информацию в новый файл; предыдущий файл журнала сохранится.  Если вы не укажете этот ключ, максимальный размер одного файла журнала составит 50 МБ.
/LVL:debug info warning error critical	Этот ключ устанавливает уровень детализации журнала от максимального ( <b>Отладочная информация</b> ), при котором в журнал записываются все события, до минимального ( <b>Критические события</b> ), при котором в журнал записываются только критические события.  Если вы не укажете этот ключ, в журнал трассировки будут записываться события с уровнем детализации <b>Отладочная информация</b> .
/OFF	Этот ключ выключает ведение журнала трассировки.

### Примеры команды KAVSHELL TRACE

Чтобы включить ведение журнала трассировки с уровнем детализации **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 (на стр. [375](#))

# Дефрагментация файлов журнала Kaspersky Embedded Systems Security 2.1. 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 2.1, 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 2.1 обновляет логическую структуру файлов журнала программы, хранящихся на защищаемом компьютере по указанному пути.

По умолчанию файлы журнала событий работы программы сохраняются по пути `C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.1\Reports`. Если вы вручную указали другой путь для хранения файлов журналов, команда `KAVSHELL VACUUM` выполняет дефрагментацию файлов в папке, указанной в параметрах журналов Kaspersky Embedded Systems Security 2.1.

Большой размер дефрагментируемых файлов журнала событий увеличивает время выполнения команды `KAVSHELL VACUUM`.

Во время выполнения команды `KAVSHELL VACUUM` невозможно выполнение задач постоянной защиты и контроля компьютера. Процедура дефрагментации блокирует доступ к журналам Kaspersky Embedded Systems Security 2.1 и запрещает запись событий в журнал. Во избежание снижения уровня защиты компьютера рекомендуется заранее планировать выполнение команды `KAVSHELL VACUUM` в нерабочее время.

Чтобы выполнить дефрагментацию файлов журналов, созданных по событиям работы Kaspersky Embedded Systems Security 2.1, выполните команду:

```
KAVSHELL VACUUM
```

Выполнение команды доступно при запуске с правами учетной записи локального администратора.

## Очищение базы iSwift. KAVSHELL FBRESET

Kaspersky Embedded Systems Security 2.1 использует технологию iSwift, позволяющую не проверять файл повторно, если с момента последней проверки он не был изменен (**Использовать технологию iSwift**).

В системном каталоге %SYSTEMDRIVE%\System Volume Information Kaspersky Embedded Systems Security 2.1 создает файлы fidbox.dat и fidbox2.dat, которые содержат информацию об уже проверенных незараженных объектах. Чем больше различных файлов проверил Kaspersky Embedded Systems Security 2.1, тем больше размер файла fidbox.dat (fidbox2.dat). В данном файле хранится только актуальная информация о реально существующих в системе файлах: если какой-либо файл в системе удаляется, то Kaspersky Embedded Systems Security 2.1 удаляет информацию о нем из файла fidbox.dat (fidbox2.dat).

Для очищения данного файла используйте команду KAVSHELL FBRESET.

Учитывайте следующие особенности работы команды KAVSHELL FBRESET:

- При очистке файла fidbox.dat с помощью команды KAVSHELL FBRESET Kaspersky Embedded Systems Security 2.1 не приостанавливает защиту (в отличие от удаления файла fidbox.dat вручную).
- После очистки файла fidbox.dat Kaspersky Embedded Systems Security 2.1 может увеличить нагрузку на компьютер. При этом антивирусная программа проверяет все файлы, к которым обращается впервые после очистки файла fidbox.dat. После проверки Kaspersky Embedded Systems Security 2.1 вновь заносит в файл fidbox.dat информацию о проверенном объекте. 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 2.1 при их аварийном завершении (см. таблицу ниже). Кроме этого вы можете в любой момент снять образы памяти выполняющихся процессов Kaspersky Embedded Systems Security 2.1.

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 48. Ключи команды KAVSHELL DUMP

Ключ	Описание
/ON	Включает создание файла дампа процесса при его аварийном завершении.
/F:<папка с файлами дампов>	<p>Обязательный ключ; указывает путь к папке, в которой будет сохранен файл дампа. Если вы укажете путь к несуществующей папке, файл дампа не будет создан. Вы можете использовать сетевые пути в формате UNC (Universal Naming Convention), но не можете указывать пути к папкам на сетевых дисках защищаемого компьютера.</p> <p>Указывая путь к папке с файлом дампа, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.</p>
/SNAPSHOT	Снимает образ памяти указанного выполняющегося процесса Kaspersky Embedded Systems Security 2.1 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 (на стр. [376](#))

## Импорт параметров. KAVSHELL IMPORT

С помощью команды `KAVSHELL IMPORT` вы можете импортировать параметры Kaspersky Embedded Systems Security 2.1, его функций и задач из конфигурационного файла в Kaspersky Embedded Systems Security 2.1 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 49. Ключи команды KAVSHELL IMPORT

Ключ	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, из которого будут импортированы параметры.  Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Коды возврата команды KAVSHELL IMPORT (на стр. [376](#))

# Экспорт параметров. KAVSHELL EXPORT

С помощью команды KAVSHELL EXPORT вы можете экспортировать все параметры Kaspersky Embedded Systems Security 2.1 и существующих задач в конфигурационный файл, чтобы потом импортировать их в Kaspersky Embedded Systems Security 2.1 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 50. Ключи команды KAVSHELL EXPORT

Ключ	Описание
<имя конфигурационного файла и путь к файлу>	<p>Имя конфигурационного файла, в котором будут сохранены параметры.</p> <p>Вы можете присвоить конфигурационному файлу любое расширение.</p> <p>Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.</p>

Коды возврата команды KAVSHELL EXPORT (на стр. [377](#))

# Коды возврата командной строки

## В этом разделе

Коды возврата команд KAVSHELL START и KAVSHELL STOP .....	<a href="#">369</a>
Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCritical .....	<a href="#">369</a>
Коды возврата команды KAVSHELL TASK .....	<a href="#">370</a>
Коды возврата команды DEVCONTROL .....	<a href="#">371</a>
Коды возврата команды KAVSHELL RTP .....	<a href="#">372</a>
Коды возврата команды KAVSHELL UPDATE .....	<a href="#">372</a>
Коды возврата команды KAVSHELL ROLLBACK .....	<a href="#">373</a>
Коды возврата команды KAVSHELL LICENSE .....	<a href="#">374</a>
Коды возврата команды KAVSHELL TRACE .....	<a href="#">375</a>
Коды возврата команды KAVSHELL FBRESET .....	<a href="#">375</a>
Коды возврата команды KAVSHELL DUMP .....	<a href="#">376</a>
Коды возврата команды KAVSHELL IMPORT .....	<a href="#">376</a>
Коды возврата команды KAVSHELL EXPORT .....	<a href="#">377</a>



# Коды возврата команд KAVSHELL START и KAVSHELL STOP

Таблица 51. 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 2.1 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 2.1 работает под учетной записью Локальная система).
-99	Неизвестная ошибка

# Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCritical

Таблица 52. Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCritical

Код возврата	Описание
0	Операция выполнена успешно (Угроз не обнаружено)
1	Операция отменена

Код возврата	Описание
-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	Обнаружены зараженные и другие объекты
-81	Обнаружены возможно зараженные объекты
-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

Таблица 53. Коды возврата команды KAVSHELL TASK

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (задача не найдена)

-5	Неверный синтаксис команды
-6	Неверная операция (например, задача не запущена, уже запущена или не может быть приостановлена)
-99	Неизвестная ошибка
-301	Недействительный ключ
401	Задача не запущена (для ключа /STATE)
402	Задача уже запущена (для ключа /STATE)
403	Задача уже приостановлена (для ключа /STATE)
-404	Ошибка выполнения операции (изменение состояния задачи привело ее к сбою)

## Коды возврата команды DEVCONTROL

Таблица 54. Коды возврата команды KAVSHELL DEVCONTROL

Код возврата	Описание
0	Операция выполнена успешно
-3	Ошибка прав доступа
-4	Объект не найден (задача не найдена)
-5	Неверный синтаксис команды
-6	Неверная операция (например, задача уже запущена или уже остановлена)
-99	Неизвестная ошибка

# Коды возврата команды KAVSHELL RTP

Таблица 55. 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 56. 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

Код возврата	Описание
-5	Неверный синтаксис команды
-99	Неизвестная ошибка
-206	Файлы обновлений отсутствуют в указанном источнике или имеют неизвестный формат
-209	Ошибка подключения к источнику обновлений
-232	Ошибка аутентификации при подключении к прокси-серверу
-234	Ошибка подключения к программе Kaspersky Security Center
-235	Kaspersky Embedded Systems Security 2.1 не прошел проверку подлинности при соединении с источником обновлений
-236	Базы Kaspersky Embedded Systems Security 2.1 повреждены
-301	Недействительный ключ

## Коды возврата команды KAVSHELL ROLLBACK

Таблица 57. 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 58. 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 59. 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 60. Коды возврата команды KAVSHELL FBRESET

Код возврата	Описание
0	Операция выполнена успешно
-99	Неизвестная ошибка

# Коды возврата команды KAVSHELL DUMP

Таблица 61. 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 с 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 62. Коды возврата команды KAVSHELL IMPORT

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден импортируемый конфигурационный файл)
-5	Неверный синтаксис
-99	Неизвестная ошибка



Код возврата	Описание
501	Операция выполнена успешно, однако во время выполнения команды возникла ошибка / замечание, например, Kaspersky Embedded Systems Security 2.1 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 2.1 более поздней или несовместимой версии)

## Коды возврата команды KAVSHELL EXPORT

Таблица 63. 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 2.1 не экспортировал параметры какого-либо из функциональных компонентов

---

# Контроль производительности. Счетчики Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о счетчиках Kaspersky Embedded Systems Security 2.1: счетчиках производительности для программы Системный монитор, счетчиках и ловушках SNMP.

## В этом разделе

Счетчики производительности для программы Системный монитор .....	<a href="#">378</a>
Счетчики и ловушки SNMP Kaspersky Embedded Systems Security 2.1 .....	<a href="#">390</a>

## 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 2.1 во время установки.

## В этом разделе

О счетчиках производительности Kaspersky Embedded Systems Security 2.1 .....	<a href="#">379</a>
Общее количество отвергнутых запросов .....	<a href="#">380</a>
Общее количество пропущенных запросов .....	<a href="#">381</a>
Количество запросов, не обработанных из-за нехватки системных ресурсов .....	<a href="#">383</a>
Количество запросов, отданных на обработку .....	<a href="#">384</a>
Среднее количество потоков диспетчера файловых перехватов .....	<a href="#">385</a>
Максимальное количество потоков диспетчера файловых перехватов .....	<a href="#">386</a>
Количество элементов в очереди зараженных объектов .....	<a href="#">387</a>
Количество объектов, обрабатываемых за секунду .....	<a href="#">388</a>

# О счетчиках производительности Kaspersky Embedded Systems Security 2.1

В состав устанавливаемых компонентов Kaspersky Embedded Systems Security 2.1 по умолчанию включен компонент **Счетчики производительности**. Во время установки Kaspersky Embedded Systems Security 2.1 регистрирует свои счетчики производительности для программы "Системный монитор" Microsoft Windows.

С помощью счетчиков Kaspersky Embedded Systems Security 2.1 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 2.1 и сбои в его работе.

Вы можете просматривать счетчики производительности Kaspersky Embedded Systems Security 2.1, 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 2.1 в случае, если значения счетчиков их превышают.

## Общее количество отвергнутых запросов

Таблица 64. Общее количество отвергнутых запросов

<b>Название</b>	Общее количество отвергнутых запросов (Total number of requests denied)
<b>Определение</b>	<p>Общее количество запросов драйвера файловых перехватов на обработку объектов, которые не были приняты рабочими процессами Kaspersky Embedded Systems Security 2.1; рассчитывается с момента последнего запуска Kaspersky Embedded Systems Security 2.1.</p> <p>Программа пропускает объекты, запросы на обработку которых отвергаются рабочими процессами Kaspersky Embedded Systems Security 2.1.</p>
<b>Назначение</b>	<p>Счетчик позволяет обнаруживать:</p> <ul style="list-style-type: none"> <li>• снижение качества постоянной защиты из-за полной загрузки рабочих процессов Kaspersky Embedded Systems Security 2.1;</li> <li>• прерывание постоянной защиты из-за отказа диспетчера файловых перехватов.</li> </ul>
<b>Нормальное / пороговое значение</b>	0 / 1
<b>Рекомендуемый интервал считывания показаний</b>	1 ч

<p><b>Рекомендации по настройке, если значение превышает пороговое</b></p>	<p>Количество отвергнутых запросов на обработку соответствует количеству пропущенных объектов.</p> <p>Возможны следующие ситуации в зависимости от поведения счетчика:</p> <ul style="list-style-type: none"> <li>• счетчик показывает несколько отвергнутых запросов в течение длительного времени: все рабочие процессы Kaspersky Embedded Systems Security 2.1 были полностью загружены, поэтому Kaspersky Embedded Systems Security 2.1 не удалось проверить объекты.</li> </ul> <p>Чтобы исключить пропуск объектов, увеличьте количество процессов программы для задач постоянной защиты. Вы можете использовать параметры Kaspersky Embedded Systems Security 2.1 <b>Максимальное количество активных процессов</b> и <b>Число процессов для постоянной защиты</b>;</p> <ul style="list-style-type: none"> <li>• количество отвергнутых запросов значительно превышает критический порог и быстро растет: отказал диспетчер файловых перехватов. Kaspersky Embedded Systems Security 2.1 не проверяет объекты при доступе.</li> </ul> <p>Перезапустите Kaspersky Embedded Systems Security 2.1.</p>
--	--

## Общее количество пропущенных запросов

Таблица 65. Общее количество пропущенных запросов

<p><b>Название</b></p>	<p>Общее количество пропущенных запросов (Total number of requests skipped).</p>
<p><b>Определение</b></p>	<p>Общее количество запросов драйвера файловых перехватов на обработку объектов, принятых Kaspersky Embedded Systems Security 2.1, но не отправивших события о завершении обработки; рассчитывается с момента последнего запуска программы.</p> <p>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 <b>Общее</b></p>

	<p><b>количество пропущенных запросов</b> 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 2.1 пропускает такой объект и на 1 увеличивается значение счетчика <b>Общее количество отвергнутых запросов</b>.</p>
<b>Назначение</b>	Счетчик позволяет обнаруживать снижение производительности из-за простоя потоков диспетчера файловых перехватов.
<b>Нормальное / пороговое значение</b>	0 / 1.
<b>Рекомендуемый интервал считывания показаний</b>	1 ч.
<b>Рекомендации по настройке, если значение превышает пороговое</b>	<p>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.</p> <p>Если скорость проверки не удовлетворительна, перезапустите Kaspersky Embedded Systems Security 2.1, чтобы восстановить простаивающие потоки.</p>

# Количество запросов, не обработанных из-за нехватки системных ресурсов

Таблица 66. Количество запросов, не обработанных из-за нехватки системных ресурсов

<b>Название</b>	Количество запросов, не обработанных из-за нехватки системных ресурсов (Number of requests not processed due to lack of resources)
<b>Определение</b>	<p>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 2.1.</p> <p>Kaspersky Embedded Systems Security 2.1 пропускает объекты, запросы на проверку которых не обрабатываются драйвером файловых перехватов.</p>
<b>Назначение</b>	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты, возникающее из-за недостаточности системных ресурсов.
<b>Нормальное / пороговое значение</b>	0 / 1
<b>Рекомендуемый интервал считывания показаний</b>	1 ч
<b>Рекомендации по настройке, если значение превышает пороговое</b>	<p>Если значение счетчика отличается от нулевого, рабочие процессы Kaspersky Embedded Systems Security 2.1 нуждаются в увеличении объема оперативной памяти для обработки запросов.</p> <p>Возможно, активные процессы других программ используют всю доступную оперативную память.</p>

# Количество запросов, отданных на обработку

Таблица 67. Количество запросов, отданных на обработку

<b>Название</b>	Количество запросов, отданных на обработку (Number of requests sent to be processed).
<b>Определение</b>	Количество объектов, ожидающих обработки рабочими процессами.
<b>Назначение</b>	Счетчик позволяет отслеживать загрузку рабочих процессов Kaspersky Embedded Systems Security 2.1 и общий уровень файловой активности на компьютере.
<b>Нормальное / пороговое значение</b>	Значение счетчика может колебаться в зависимости от уровня файловой активности на компьютере.
<b>Рекомендуемый интервал считывания показаний</b>	1 мин.
<b>Рекомендации по настройке, если значение превышает пороговое</b>	нет



# Среднее количество потоков диспетчера файловых перехватов

Таблица 68. Среднее количество потоков диспетчера файловых перехватов

<b>Название</b>	Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams).
<b>Определение</b>	Количество потоков диспетчера файловых перехватов в одном рабочем процессе, среднее по всем процессам, занятым в задачах постоянной защиты в текущий момент.
<b>Назначение</b>	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты из-за полной загрузки процессов Kaspersky Embedded Systems Security 2.1.
<b>Нормальное / пороговое значение</b>	Варьируется / 40.
<b>Рекомендуемый интервал считывания показаний</b>	1 мин.
<b>Рекомендации по настройке, если значение превышает пороговое</b>	<p>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 2.1 пропустит объект.</p> <p>Увеличьте количество процессов Kaspersky Embedded Systems Security 2.1 для задач постоянной защиты. Вы можете использовать параметры Kaspersky Embedded Systems Security 2.1</p> <p><b>Максимальное количество активных процессов Количество процессов для постоянной защиты.</b></p>

# Максимальное количество потоков диспетчера файловых перехватов

Таблица 69. Максимальное количество потоков диспетчера файловых перехватов

Название	Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).
Определение	Количество потоков диспетчера файловых перехватов в одном рабочем процессе, наибольшее из всех процессов, занятых в задачах постоянной защиты в текущий момент.
Назначение	Счетчик позволяет обнаруживать и устранять снижение производительности из-за неравномерного распределения нагрузки в выполняющихся рабочих процессах.
Нормальное / пороговое значение	Варьируется / 40.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	<p>Если значение этого счетчика значительно и продолжительно превышает значение счетчика <b>Среднее количество потоков диспетчера файловых перехватов</b>, Kaspersky Embedded Systems Security 2.1 неравномерно распределяет нагрузку на выполняющиеся процессы.</p> <p>Перезапустите Kaspersky Embedded Systems Security 2.1.</p>

# Количество элементов в очереди зараженных объектов

Таблица 70. Количество элементов в очереди зараженных объектов

<b>Название</b>	Количество элементов в очереди зараженных объектов (Number of items in the infected object queue).
<b>Определение</b>	Количество зараженных объектов, ожидающих обработки (лечения или удаления) в текущий момент.
<b>Назначение</b>	<p>Счетчик позволяет обнаруживать следующие ситуации:</p> <ul style="list-style-type: none"><li>• прерывание постоянной защиты из-за возможного отказа диспетчера файловых перехватов;</li><li>• перегруженность процессора из-за неравномерного распределения процессорного времени между другими работающими программами и Kaspersky Embedded Systems Security 2.1;</li><li>• вирусную эпидемию.</li></ul>
<b>Нормальное / пороговое значение</b>	Значение счетчика может быть отличным от нуля, пока Kaspersky Embedded Systems Security 2.1 обрабатывает обнаруженные зараженные или возможно зараженные объекты, но оно возвращается к нулю вскоре после окончания обработки / Значение счетчика остается ненулевым длительное время.
<b>Рекомендуемый интервал считывания показаний</b>	1 мин.
<b>Рекомендации по настройке, если значение превышает пороговое</b>	<p>Если значение счетчика остается ненулевым длительное время:</p> <ul style="list-style-type: none"><li>• Kaspersky Embedded Systems Security 2.1 не обрабатывает объекты (возможно, отказал диспетчер файловых перехватов); Перезапустите Kaspersky Embedded Systems Security 2.1.</li><li>• Недостаточно процессорного времени для обработки объектов;</li></ul>

	<p>Обеспечьте выделение Kaspersky Embedded Systems Security 2.1 дополнительного процессорного времени, например, снизив нагрузку на компьютер другими программами.</p> <ul style="list-style-type: none"> <li>• Возникла вирусная эпидемия.</li> </ul> <p>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.</p>
--	---

## Количество объектов, обрабатываемых за секунду

Таблица 71. Количество объектов, обрабатываемых за секунду

<b>Название</b>	Количество объектов, обрабатываемых за секунду (Number of objects processed per second).
<b>Определение</b>	Количество обработанных объектов, разделенное на количество времени, в течение которого эти объекты были обработаны; рассчитывается за равные промежутки времени.
<b>Назначение</b>	Счетчик отражает скорость обработки объектов; позволяет обнаружить и устранить снижение производительности компьютера, возникшее из-за недостаточности выделяемого рабочим процессам Kaspersky Embedded Systems Security 2.1 процессорного времени или сбоя в работе Kaspersky Embedded Systems Security 2.1.
<b>Нормальное / пороговое значение</b>	Варьируется / Нет.

<b>Рекомендуемый интервал считывания показаний</b>	1 мин.
<b>Рекомендации по настройке, если значение превышает пороговое</b>	<p>Значения счетчика зависят от установленных значений параметров Kaspersky Embedded Systems Security 2.1 и загрузки компьютера процессами других программ.</p> <p>Наблюдайте средний уровень показаний счетчика в течение продолжительного времени. Если общий уровень показаний счетчика снизился, то могла произойти одна из следующих ситуаций:</p> <ul style="list-style-type: none"> <li>• Рабочим процессам Kaspersky Embedded Systems Security 2.1 не хватает процессорного времени для обработки объектов.</li> </ul> <p>Обеспечьте выделение Kaspersky Embedded Systems Security 2.1 дополнительного процессорного времени, например, снизив нагрузку на компьютер другими программами.</p> <ul style="list-style-type: none"> <li>• Возник сбой в работе Kaspersky Embedded Systems Security 2.1 (простаивает несколько потоков).</li> </ul> <p>Перезапустите Kaspersky Embedded Systems Security 2.1.</p>

# Счетчики и ловушки SNMP Kaspersky Embedded Systems Security 2.1

Этот раздел содержит информацию о счетчиках и ловушках SNMP Kaspersky Embedded Systems Security 2.1.

## В этом разделе

О счетчиках и ловушках SNMP Kaspersky Embedded Systems Security 2.1 .....	<a href="#">390</a>
Счетчики SNMP Kaspersky Embedded Systems Security 2.1 .....	<a href="#">390</a>
Ловушки SNMP .....	<a href="#">395</a>

## О счетчиках и ловушках SNMP Kaspersky Embedded Systems Security 2.1

Если вы включили в состав устанавливаемых компонентов Kaspersky Embedded Systems Security 2.1 компонент **Счетчики и ловушки SNMP**, вы можете просматривать счетчики и ловушки Kaspersky Embedded Systems Security 2.1 по протоколам Simple Network Management Protocol (SNMP).

Чтобы просматривать счетчики и ловушки Kaspersky Embedded Systems Security 2.1 на компьютере-рабочем месте администратора, запустите на защищаемом компьютере Службу SNMP (SNMP Service), а на рабочем месте администратора – Службу SNMP (SNMP Service) и Службу ловушек SNMP (SNMP Trap Service).

## Счетчики SNMP Kaspersky Embedded Systems Security 2.1

Этот раздел содержит таблицы с описанием параметров счетчиков SNMP Kaspersky Embedded Systems Security 2.1.

## В этом разделе

Счетчики производительности .....	<a href="#">391</a>
Общие счетчики.....	<a href="#">392</a>
Счетчик обновления.....	<a href="#">392</a>
Счетчики постоянной защиты.....	<a href="#">393</a>
Счетчики карантина .....	<a href="#">395</a>
Счетчики резервного хранилища .....	<a href="#">395</a>

## Счетчики производительности

Таблица 72. Счетчики производительности

Счетчик	Определение
currentRequestsAmount	Количество запросов, отданных на обработку (см. стр. <a href="#">384</a> )
currentInfectedQueueLength	Количество элементов в очереди зараженных объектов (см. стр. <a href="#">387</a> )
currentObjectProcessingRate	Количество объектов, обрабатываемых за секунду (см. стр. <a href="#">388</a> )
currentWorkProcessesNumber	Количество рабочих процессов Kaspersky Embedded Systems Security 2.1 в текущий момент

## Общие счетчики

Таблица 73. Общие счетчики

Счетчик	Определение
lastCriticalAreasScanAge	Период с момента проведения последней проверки важных областей компьютера (промежуток времени в секундах между датой завершения задачи, имеющей статус <i>Задача проверки важных областей</i> , и текущим моментом)
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 2.1 с момента его последнего запуска, в сотых долях секунды
currentFileMonitorTaskStatus	Состояние задачи Постоянная защита файлов: <b>On</b> – выполняется; <b>Off</b> – остановлена или приостановлена

## Счетчик обновления

Таблица 74. 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 75. *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 2.1 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 2.1 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 2.1 вылечил; рассчитывается с момента последнего запуска задачи Постоянная защита файлов

Счетчик	Определение
totalObjectsNotDisinfected	Общее количество зараженных и других объектов, которые Kaspersky Embedded Systems Security 2.1 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 2.1 удалил; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotDeleted	Общее количество зараженных, возможно зараженных и других объектов, которые Kaspersky Embedded Systems Security 2.1 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 2.1 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 2.1 пытался поместить в резервное хранилище, но это ему не удалось; рассчитывается с момента последнего запуска задачи Постоянная защита файлов

## Счетчики карантина

Таблица 76.   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 77.   Счетчики резервного хранилища

Счетчик	Определение
currentBackupStorageSize	Объем данных в папке резервного хранилища (МБ)

## Ловушки SNMP

Параметры ловушек SNMP Kaspersky Embedded Systems Security 2.1 описаны в таблице ниже.

Таблица 78.   Ловушки SNMP Kaspersky Embedded Systems Security 2.1

Ловушка	Описание	Параметры
eventThreatDetected	Обнаружен объект.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty

eventBackupStorageSizeExceeds	<p>Превышен максимальный размер резервного хранилища. Общий объем данных в папке резервного хранилища превысил значение, указанное параметром <b>Максимальный размер резервного хранилища</b>. Kaspersky Embedded Systems Security 2.1 продолжает резервировать зараженные объекты.</p>	<p>eventDateAndTime</p> <p>eventSeverity</p> <p>eventSource</p>
eventThresholdBackupStorageSizeExceeds	<p>Достигнут порог свободного места в резервном хранилище. Размер свободного пространства в папке резервного хранилища, заданный параметром <b>Порог доступного пространства</b>, уменьшился до указанного значения. Kaspersky Embedded Systems Security 2.1 продолжает резервировать зараженные объекты.</p>	<p>eventDateAndTime</p> <p>eventSeverity</p> <p>eventSource</p>
eventQuarantineStorageSizeExceeds	<p>Превышен максимальный размер карантина. Общий объем данных в папке карантина превысил значение, указанное параметром <b>Максимальный размер карантина</b>. Kaspersky Embedded Systems Security 2.1 продолжает помещать возможно зараженные объекты на карантин.</p>	<p>eventDateAndTime</p> <p>eventSeverity</p> <p>eventSource</p>

Ловушка	Описание	Параметры
eventThresholdQuarantineStorageSizeExceeds	Достигнут порог свободного места в карантине. Размер свободного пространства в папке карантина, заданный параметром <b>Порог свободного места в карантине</b> , уменьшился до указанного значения. Kaspersky Embedded Systems Security 2.1 продолжает помещать возможно зараженные объекты на карантин.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Ошибка помещения объекта на карантин.	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuperd	Ошибка сохранения копии объекта в резервном хранилище.	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason

Ловушка	Описание	Параметры
eventQuarantineInternalError	Ошибка карантина.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Ошибка резервного хранилища.	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	Базы устарели. Рассчитывается количество дней, прошедших с момента последнего завершения задачи обновления баз (локальной, групповой задачей или задачей для наборов компьютеров).	eventSeverity eventDateAndTime eventSource days
eventAVBasesTotallyOutdated	Базы сильно устарели. Рассчитывается количество дней, прошедших с момента последнего завершения задачи обновления баз (локальной, групповой задачей или задачей для наборов компьютеров).	eventSeverity eventDateAndTime eventSource days
eventApplicationStarted	Kaspersky Embedded Systems Security 2.1 запущен.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Embedded Systems Security 2.1 остановлен.	eventSeverity eventDateAndTime eventSource

Ловушка	Описание	Параметры
eventCriticalAreasScanWasntPerformForALongTime	Проверка важных областей не проводилась давно. Рассчитывается количество дней с момента последнего завершения задачи, имеющей статус <i>Задача проверки важных областей</i> .	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	Срок действия лицензии истек.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	Срок действия лицензии скоро истечет. Рассчитывается количество дней, оставшихся до окончания срока действия лицензии.	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	Ошибка выполнения задачи.	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Ошибка выполнения задачи обновления.	eventSeverity eventDateAndTime taskName updaterErrorEvent Reason

В таблице ниже описаны параметры ловушек и возможные значения параметров.

Таблица 79. Значения параметров ловушек SNMP

Параметр	Описание и возможные значения
eventDateAndTime	Время возникновения события.
eventSeverity	<p>Уровень важности события. Параметр принимает следующие значения:</p> <ul style="list-style-type: none"> <li>critical (1) – критический,</li> <li>warning (2) – предупреждение,</li> <li>info (3) – информационный.</li> </ul>
UserName	Имя пользователя (например, пользователя, который пытался получить доступ к зараженному файлу).
computerName	Имя компьютера (например, компьютера, с которого пользователь пытался получить доступ к зараженному файлу).
eventSource	<p>Источник события: функциональный компонент, в работе которого возникло событие. Параметр принимает следующие значения:</p> <ul style="list-style-type: none"> <li>unknown (0) – функциональный компонент не определен;</li> <li>quarantine (1) – Карантин;</li> <li>backup (2) – Резервное хранилище;</li> <li>reporting (3) – Журналы выполнения задач;</li> <li>updates (4) – Обновление;</li> <li>realTimeProtection (5) – Постоянная защита файлов;</li> <li>onDemandScanning (6) – Проверка по требованию;</li> <li>product (7) – событие связано не с работой отдельных компонентов, а с работой Kaspersky Embedded Systems Security 2.1 в целом;</li> <li>systemAudit (8) – Журнал системного аудита.</li> </ul>
eventReason	Причина возникновения события. Параметр принимает следующие значения:



	<ul style="list-style-type: none"> <li>• reasonUnknown (0) – причина не определена,</li> <li>• 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 2.1 будет использовать папку резервного хранилища или папку карантина, установленную по умолчанию.</li> </ul>
objectName	Имя объекта (например, имя файла, в котором обнаружена угроза).
threatName	Имя обнаруженного объекта согласно классификации Вирусной энциклопедии ( <a href="http://www.securelist.ru">http://www.securelist.ru</a> ). Это имя входит в полное название обнаруженного объекта, которое Kaspersky Embedded Systems Security 2.1 возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.
detectType	<p>Тип обнаруженного объекта.</p> <p>Параметр принимает следующие значения:</p> <ul style="list-style-type: none"> <li>• undefined (0) – не определен;</li> <li>• virware – классические вирусы и сетевые черви;</li> <li>• trojware – троянские программы;</li> <li>• malware – прочие вредоносные программы;</li> <li>• adware – рекламные программы;</li> <li>• pornware – порнографические программы;</li> <li>• riskware – легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным.</li> </ul>

Ловушка	Описание
detectCertainty	<p>Степень уверенности обнаружения угрозы. Параметр принимает следующие значения:</p> <ul style="list-style-type: none"> <li>• Suspicion (возможно зараженный) – Kaspersky Embedded Systems Security 2.1 обнаружил частичное совпадение участка кода объекта с известным вредоносным кодом;</li> <li>• Sure (зараженный) – Kaspersky Embedded Systems Security 2.1 обнаружил полное совпадение участка кода объекта с известным вредоносным кодом.</li> </ul>
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	Имя задачи.
updaterErrorEventReason	<p>Причина, по которой обновление не было применено. Параметр принимает следующие значения:</p> <ul style="list-style-type: none"> <li>• reasonUnknown(0) – причина не определена;</li> <li>• reasonAccessDenied – доступ запрещен;</li> <li>• reasonUrlsExhausted – список источников обновлений исчерпан;</li> <li>• reasonInvalidConfig – неправильный файл конфигурации;</li> <li>• reasonInvalidSignature – неверная подпись;</li> <li>• reasonCantCreateFolder – невозможно создать папку;</li> </ul>

	<ul style="list-style-type: none"> <li>• reasonFileOperError – файловая ошибка;</li> <li>• reasonDataCorrupted – объект поврежден;</li> <li>• reasonConnectionReset – сброс соединения;</li> <li>• reasonTimeOut – истекло время ожидания при соединении;</li> <li>• reasonProxyAuthError – ошибка проверки подлинности на прокси-сервере;</li> <li>• reasonServerAuthError – ошибка проверки подлинности на сервере;</li> <li>• reasonHostNotFound – компьютер не найден;</li> <li>• reasonServerBusy – сервер недоступен;</li> <li>• reasonConnectionError – ошибка соединения;</li> <li>• reasonModuleNotFound – объект не найден;</li> <li>• reasonBlstCheckFailed(16) – ошибка проверки черного списка ключей. Возможно, в момент обновления публиковались обновления баз; повторите обновление через несколько минут.</li> </ul>
storageObjectNotAdded EventReason	<p>Причина непомещения объекта в резервное хранилище или на карантин. Параметр принимает следующие значения:</p> <ul style="list-style-type: none"> <li>• reasonUnknown(0) – причина не определена.</li> <li>• reasonStorageInternalError – ошибка базы данных; восстановите Kaspersky Embedded Systems Security 2.1.</li> <li>• reasonStorageReadOnly – база данных доступна только для чтения; восстановите Kaspersky Embedded Systems Security 2.1.</li> <li>• reasonStorageIOError – ошибка ввода-вывода: а) Kaspersky Embedded Systems Security 2.1 поврежден, восстановите Kaspersky Embedded Systems Security 2.1; б) диск, на котором хранятся файлы Kaspersky Embedded Systems Security 2.1, поврежден.</li> </ul>

	<ul style="list-style-type: none"> <li>• reasonStorageCorrupted – хранилище повреждено; восстановите Kaspersky Embedded Systems Security 2.1.</li> <li>• reasonStorageFull – база данных полна; освободите место на диске.</li> <li>• reasonStorageOpenError – не удалось открыть файл базы данных; восстановите Kaspersky Embedded Systems Security 2.1.</li> <li>• reasonStorageOSFeatureError – некоторые особенности операционной системы не отвечают требованиям Kaspersky Embedded Systems Security 2.1.</li> <li>• reasonObjectNotFound – помещаемый в хранилище объект отсутствует на диске.</li> <li>• reasonObjectAccessError – недостаточно прав для использования Backup API: учетная запись, с правами которой выполняется операция, не обладает правами Backup Operator.</li> <li>• reasonDiskOutOfSpace – недостаточно места на диске.</li> </ul>
--	--

---

# Обращение в Службу технической поддержки

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

## В этом разделе

Способы получения технической поддержки.....	<a href="#">405</a>
Техническая поддержка через Kaspersky CompanyAccount.....	<a href="#">406</a>
Использование файла трассировки и скрипта AVZ.....	<a href="#">407</a>

## 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 (<http://support.kaspersky.ru/support/rules>).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (<https://support.kaspersky.ru/b2b>) ;
- 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.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки ([http://support.kaspersky.ru/faq/companyaccount\\_help](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 2.1 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 сохранения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения и отправки сохраняемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

---

# Глоссарий

## О

### OLE-объект

Файл, присоединенный или встроенный в другой файл. Программы "Лаборатории Касперского" позволяют проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel® в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

## А

### 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 в проверяемых объектах вредоносный код. Антивирусные базы формируются 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.



## В

### Возможно зараженный файл

Файл, внутри которого содержится либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный "Лаборатории Касперского". Возможно зараженные файлы обнаруживаются с помощью эвристического анализатора.

## Г

### Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

## Д

### Дополнительный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

## З

### Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

## Зараженный файл

Файл, внутри которого содержится вредоносный код (при проверке файла был обнаружен код известной программы, представляющей угрозу). Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими файлами, поскольку это может привести к заражению вашего компьютера.

## 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.

## М

### Маска файла

Представление названия и расширения файла общими символами.

Для формирования маски файла можно использовать любые символы, допустимые в

названиях файлов, в том числе специальные:

- \* – символ, заменяющий нуль или более нуль любых символов;
- ? – символ, заменяющий любой один символ.

Следует иметь в виду, что название и расширение файла всегда пишутся через точку.

## 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 работы программы, специфичные для каждого типа задач.

### Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

## 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, dll и др. Риск внедрения в такие файлы вредоносного кода достаточно высок.

## Р

### Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий файлов, создаваемых перед их первым лечением или удалением.

## С

### Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского" и управления ими.

## У

### 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 анализ

Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

Файлам, в которых во время эвристического анализа обнаружен вредоносный код, присваивается статус *зараженный*.

### Эвристический анализатор

Модуль Kaspersky Embedded Systems Security 2.1, выполняющий эвристический анализ.

---

# АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 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 программного обеспечения, 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, 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. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского": <http://www.kaspersky.ru>

Вирусная энциклопедия: <https://securelist.ru/>

Вирусная лаборатория: <https://virusdesk.kaspersky.ru/> (для проверки подозрительных файлов и сайтов)

Веб-форум "Лаборатории Касперского": <http://forum.kaspersky.com>

---

# Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в папке установки программы.



---

# Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Intel и Pentium – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Active Directory, Excel, Internet Explorer, Microsoft, Outlook, Windows и Windows Vista – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

---

# Предметный указатель

## Е

EICAR..... 111, 113

## И

iSwift-файлы ..... 387

## К

Kaspersky Embedded Systems Security 2.1

    запуск при старте операционной системы ..... 131, 353

KAVSHELL DUMP ..... 388, 402

KAVSHELL HELP ..... 352

KAVSHELL LICENSE ..... 381, 400

KAVSHELL ROLLBACK ..... 380, 399

KAVSHELL RTP ..... 365, 397

KAVSHELL SCAN ..... 354, 394

KAVSHELL TASK ..... 362, 395

KAVSHELL TRACE ..... 382, 401

KAVSHELL UPDATE ..... 374, 398

## В

Восстановление программы ..... 84

## Г

Группы администрирования .....295, 445

## З

Задача

    добавления ключа ..... 123, 381

Задачи

    групповые ..... 164

## И

Инсталляционный пакет ..... 64, 90, 101, 104

Исключения из проверки.....48, 68

Исполняемый файл.....371

## К

Ключ.....381

    установка ..... 123, 381

Консоль управления .....39, 62, 88

    подключение ..... 74, 76

    удаление .....88

    установка .....72, 104

## Л

Лицензирование программы..... 118, 120

## Лицензия

дата окончания .....	119, 124, 129
Лицензионное соглашение.....	118
продление срока действия.....	129
статус .....	124
удаление .....	130
файл ключа .....	122

## Н

### Настройка

задача .....	171, 173
параметров Kaspersky Embedded Systems Security 2.1 .....	211, 213, 216
параметров установки программы .....	68, 104

## О

### Обновление

откат последнего обновления.....	380
----------------------------------	-----

## П

Папка резервного хранилища.....	228
---------------------------------	-----

### Подготовка

к установке программы.....	62, 64
----------------------------	--------

Политика.....	147
---------------	-----

Полная установка.....	68
-----------------------	----

Постоянная защита .....	243, 244
Правила	
контроль запуска программ.....	295, 299, 302
контроль устройств.....	305, 308, 313
Профиль политики .....	280

## С

Сервер администрирования .....	448
--------------------------------	-----

## У

Установка	
Active Directory .....	107
Kaspersky Security Center .....	99, 100, 101
выбор компонентов .....	34, 68
локальная.....	68
мастер .....	67, 68, 72